50% off Falcon Go, Pro, or Enterprise — for a limited time only Claim my deal

CYBERSECURITY 101: THE FUNDAMENTALS OF CYBERSECURITY

Cybersecurity is becoming increasingly important in today's world. CrowdStrike is providing explanations, examples and best practices on fundamental principles of a variety of cybersecurity topics. If you're looking for information on endpoint protection, cloud security, types of cyber attacks and more, you've come to the right place – welcome to Cybersecurity 101!

Search...

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Z |

FILTER CATEGORY

AI & Machine Learning | Cyberattacks | Cloud Security | Next-Gen SIEM | Endpoint Security & XDR | Observability | Exposure Management | Identity Protection | Data Protection | Platform Security | Application Security | Threat Intelligence & Hunting | Social Engineering | Small Business | Incident Response | IT Automation | Advisory Services | Managed Security

A

AI Anomaly Detection Use Cases Read More >

AI anomaly detection employs the use of AI/ML algorithms and models to identify unusual behaviors, events, or patterns that diverge

GoSecure, Inc.
Exhibit 2045
CrowdStrike v. GoSecure
IPR2025-00070

A

AI Anomaly Detection Use Cases Read More >

AI anomaly detection employs the use of AI/ML algorithms and models to identify unusual behaviors, events, or patterns that diverge from normal or expected baselines and is crucial for maintaining the integrity of critical information and systems.

Application Security Testing Read More >

Application security testing evaluates software to identify vulnerabilities that attackers could exploit.

Attribute-Based Access Control (ABAC) Read More >

Attribute-based access control (ABAC) provides a flexible, context-aware approach to access management that evaluates multiple attributes — such as user identity, device type, location, and time of access — to make real-time access decisions.

AI Social Engineering Read More >

In this post, we'll investigate how AI has advanced social engineering to the next level. We'll look specifically at how emerging technologies, such as deepfakes, have amplified social engineering techniques and increased the potential for fraud.

Agentic AI Read More >

Agentic AI is the evolution of generative AI, defined by its ability to make decisions, take action and learn from its environment without human intervention.

AI SIEM Read More >

AI SIEM represents the cutting edge of cybersecurity, combining the strengths of next-gen SIEM with the power of AI and machine learning.

Access Control Read More >

Access control in SaaS security relates to the methods and policies implemented to regulate user access to the SaaS applications and their associated data.

API Security Read More >

API security involves implementing measures to safeguard data confidentiality, integrity, and availability. These measures include setting up authentication and authorization mechanisms that permit only authorized users and applications to access the API.

Adaptive Authentication Read More >

Adaptive authentication, also called risk-based authentication, is a context-aware security approach that continuously evaluates authentication attempts and adjusts security measures dynamically based on real-time risk signals.

Advanced Persistent Threat (APT) Read More >

An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time.

AI and Cloud Security Read More >

In this article, we'll examine how AI technology impacts multiple areas of cloud security. We'll also discuss CrowdStrike and its contributions to leading AI-native security solutions and tools.

Attack Surface Reduction Read More >

This article explores the core principles of attack surface reduction to help you understand which tools and techniques have proven

contributions to leading AI-native security solutions and tools.

Attack Surface Reduction Read More >

This article explores the core principles of attack surface reduction to help you understand which tools and techniques have proven most effective, and how teams can implement them.

Attack Vectors Read More >

An attack vector is the method or combination of methods that cybercriminals use to breach or infiltrate a victim's network.

AI PC Read More >

In this post, we'll cover AI PC use cases in cybersecurity specifically, and various challenges associated with these new machines.

Active Directory (AD) Auditing Read More >

AD auditing is the process of tracking, logging, and reviewing activities in your Active Directory environment. Whether it's detecting risky environment changes, monitoring privilege escalations, or meeting compliance requirements, auditing your AD setup and activity gives you the insights you need to secure your network. Think of it as the detective work that ensures your AD environment stays clean, compliant, and resilient to threats.

Active Directory Federation Services (AD FS) Read More >

Active Directory Federation Services (AD FS) is a single sign on (SSO) feature developed by Microsoft that provides authenticated access to any domain, device, web application or system within the organization's active directory (AD).

Advanced Endpoint Protection (AEP) Read More >

Advanced endpoint protection (AEP) is a next-generation endpoint security solution that uses AI, machine learning, and other intelligent automation capabilities to provide more comprehensive cybersecurity protection from a variety of modern threats.

AI-Native XDR Read More >

The synergy between XDR and AI introduces a powerhouse solution — AI-native XDR — that offers a myriad of benefits to organizations.

Active Directory Security Read More >

Active Directory is a directory service offered by Microsoft Windows that helps administrators configure permissions and network access.

Application Security Read More >

Application security is a set of measures designed to prevent data or code at the application level from being stolen or manipulated. It involves security during application development and design phases as well as systems and approaches that protect applications after deployment.

API Security Testing Read More >

API security testing helps teams address vulnerabilities early and often throughout the API development process.

Application Vulnerability Scanning Read More >

Application vulnerability scanning attempts to identify security weaknesses that may be present within a software application.

Application Security Posture Management (ASPM) Read More >

ASPM is the process of evaluating, managing, and enhancing the security posture of an organization's custom applications. It ensures

Application vulnerability scanning attempts to identify security weaknesses that may be present within a software application.

Application Security Posture Management (ASPM) Read More >

ASPM is the process of evaluating, managing, and enhancing the security posture of an organization's custom applications. It ensures applications adhere to security standards, resist cyber threats, and remain compliant.

ASPM Best Practices Read More >

Read this post to learn about five ASPM best practices that will help keep your application environments secure from adversaries.

Application Security Posture Management (ASPM) Use Cases Read More >

There are many real-world scenarios where ASPM plays a crucial role in helping organizations fortify their application security.

Application Security Orchestration and Correlation (ASOC) Read More >

By correlating data from multiple sources and analyzing patterns, ASOC tools enable security teams to de-duplicate and prioritize application security findings. Additionally, ASOC tools enable development teams to automate key workflows and streamline security processes, increasing speed and efficiency for vulnerability testing and remediation efforts.

ASOC vs. ASPM Read More >

ASOC and ASPM share common foundations in application security, with ASOC often viewed as a precursor to the broader and more holistic ASPM approach.

Application Risk Scoring Read More >

In this post we'll provide a clearer understanding of risk scoring, discuss the role of Common Vulnerability Scoring System (CVSS) scores (and other scoring standards), and talk about what it means to integrate business and data flow context into your risk assessment.

AWS Migration Read More >

An AWS migration is the strategic process of moving digital assets — such as applications, databases, and IT processes — from on-premises or other cloud services to Amazon Web Services (AWS).

Automated Intelligence Read More >

Learn more about how traditional defense measures have evolved to integrate automated systems that use AI/machine learning (ML) and data analytics and the role and benefits of automated intelligence as a part of a modern cybersecurity arsenal.

Automated Intelligence Read More >

Learn more about how traditional defense measures have evolved to integrate automated systems that use AI/machine learning (ML) and data analytics and the role and benefits of automated intelligence as a part of a modern cybersecurity arsenal.

AI-Native Cybersecurity Read More >

AI-native cybersecurity uses cloud-native data platforms and cutting-edge AI to analyze datasets, identify patterns, and strengthen security posture.

Adversarial AI & ML Read More >

Adversarial AI or adversarial machine learning (ML) seeks to inhibit the performance of AI/ML systems by manipulating or misleading them. These attacks on machine learning systems can occur at multiple stages across the model development life cycle.

Azure Kubernetes Service (AKS) Read More >

Azure Kubernetes Service (AKS) is a managed Kubernetes service from Microsoft Azure that aims to simplify the deployment and

them. These attacks on machine learning systems can occur at multiple stages across the model development life cycle.

Azure Kubernetes Service (AKS) Read More >

Azure Kubernetes Service (AKS) is a managed Kubernetes service from Microsoft Azure that aims to simplify the deployment and management of Kubernetes clusters.

AI-Powered Behavioral Analysis Read More >

AI-powered behavioral analysis leverages artificial intelligence to learn and predict adversarial behavior patterns.

AWS Infrastructure Observability Read More >

In this article, we'll cover the benefits of implementing infrastructure observability on AWS. We will explore a few key observability services from AWS, along with external services that you can integrate with your AWS account to enhance your monitoring capabilities.

Application Security Best Practices Read More >

In this post, we will cover seven best practices that can ensure the resilience of your applications against ever-evolving threats.

Adware Read More >

Adware — or advertising-supported software — is automated, unwanted software designed to monitor online user behavior and bombard them with targeted advertisements, banners and pop-ups.

Application Whitelisting Read More >

Application whitelisting is the approach of restricting the usage of any tools or applications only to those that are already vetted and approved.

Audit Logs Read More >

Audit logs are a collection of records of internal activity relating to an information system. Audit logs differ from application logs and system logs.

AWS Cloud Security Read More >

In this article, we go beyond the generic AWS best practices and offer recommendations to help you scale and enhance your AWS security.

AWS CloudTrail vs. AWS CloudWatch Read More >

Amazon Web Services (AWS) offers various monitoring tools to assist users in monitoring their cloud systems. In this post, we'll compare the AWS CloudTrail and AWS CloudWatch tools, exploring their key features, capabilities, differences, and similarities.

Access Logs Read More >

An access log is a log file that records all events related to client applications and user access to a resource on a computer. Examples can be web server access logs, FTP command logs, or database query logs.

Application Log Read More >

Software applications generate logs when something occurs within (or affects) the application. IT teams typically use application log data to investigate outages, troubleshoot bugs, or analyze security incidents.

Application Monitoring Read More >

Application monitoring is the process of collecting log data in order to help developers track availability, bugs, resource use, and

data to investigate outages, troubleshoot bugs, or analyze security incidents.

Application Monitoring Read More >

Application monitoring is the process of collecting log data in order to help developers track availability, bugs, resource use, and changes to performance in applications that affect the end-user experience (UX).

AWS Misconfigurations Read More >

In this article, we'll explore the most common sets of misconfigurations across the most common services, and give advice on how to stay safe and prevent potential breaches when making any modification to your infrastructure

Attack Surface Read More >

An attack surface is the sum of all possible security risk exposures in an organization's software environment.

Address Resolution Protocol (ARP) Spoofing: What It Is and How to Prevent an ARP Attack Read More >

Address Resolution Protocol (ARP) spoofing or ARP poisoning is a form of spoofing attack that hackers use to intercept data. A hacker commits an ARP spoofing attack by tricking one device into sending messages to the hacker instead of the intended recipient.

Attack Surface Management Read More >

Attack surface management is the continuous discovery, monitoring, evaluation, prioritization and remediation of attack vectors within an organization's IT infrastructure.

B

Business Email Compromise (BEC) Read More >

Business email compromise (BEC) is a cyberattack technique whereby adversaries assume the digital identity of a trusted persona in an attempt to trick employees or customers into taking a desired action, such as making a payment or purchase, sharing data or divulging sensitive information.

Browser Extensions Read More >

Browser extensions—sometimes referred to as plug-ins or add-ons—are small software modules that enhance and personalize the functionality of web browsers, such as Chrome, Firefox, Edge, and Safari.

Behavioral Analytics Read More >

In the context of cybersecurity, behavioral analytics focuses on user behavior within networks and applications, watching for unusual activity that may signify a security threat.

Bring-Your-Own-Device (BYOD) Read More >

Bring Your Own Device (BYOD) refers to a business policy that allows employees to use personally owned devices for work purposes. Common personal devices include smartphones, laptops, tablets, and flash drives.

Backdoor Attacks Read More >

A backdoor attack is a clandestine method of sidestepping normal authentication procedures to gain unauthorized access to a system. It's like a secret entrance that a burglar can use to get into a house — but instead of a house, it's a computer or a network.

Bootkits Read More >

A backdoor attack is a clandestine method of sidestepping normal authentication procedures to gain unauthorized access to a system. It's like a secret entrance that a burglar can use to get into a house — but instead of a house, it's a computer or a network.

Bootkits Read More >

Bootkit is a type of malware used by a threat actor to attach malicious software to a computer system and can be a critical threat to your business.

Backporting Read More >

Backporting is when a software patch or update is taken from a recent software version and applied to an older version of the same software.

Brute Force Attacks Read More >

A brute force attack is uses a trial-and-error approach to systematically guess login info, credentials, and encryption keys. The attacker submits combinations of usernames and passwords until they finally guess correctly.

Botnet Read More >

A botnet is a network of computers infected with malware that are controlled by a bot herder.

C

Cloud Jacking Read More >

Cloud jacking is a cyberattack where an attacker takes control of a cloud account by compromising credentials or exploiting vulnerabilities.

Cloud Response Read More >

Cloud response is a component of CDR that addresses the challenges of securing cloud environments, focusing on the mitigation and resolution of detected threats.

Cloud SIEM Read More >

Cloud SIEM is stepping in to address the evolving security landscape, offering a more agile and scalable solution than on-premises SIEM tools.

CDR vs Cloud Security Monitoring Read More >

In this article, we'll explore what makes CDR essential for modern organizations and how cloud security monitoring fits into this broader framework.

CWPP vs CSPM Read More >

Together, CWPP and CSPM form the backbone of a solid cloud security strategy, providing the visibility and control necessary to secure ever-expanding cloud environments.

CDR vs XDR Read More >

In this article, we'll explore the differences between CDR and XDR, their functions and benefits, and how combining both approaches can create a more robust protection framework.

Cloud Application Detection and Response (CADR) Read More >

In this article, we'll explore the differences between CDR and XDR, their functions and benefits, and how combining both approaches can create a more robust protection framework.

Cloud Application Detection and Response (CADR) Read More >

CADR gathers and aggregates data from operating system events, containers, workloads, APIs, and applications to provide end-to-end visibility.

Cloud Threat Management Read More >

Cloud threat management refers to the set of practices and technologies employed to safeguard cloud-based systems, SaaS applications, and data from security risks and vulnerabilities.

Continuous Access Evaluation Profile (CAEP) Read More >

CAEP is an Internet Engineering Task Force (IETF) standard developed to enable continuous evaluation of user access in identity and access management (IAM) systems.

Control Plane Read More >

A control plane is a digital component that manages the flow of data across the network. In a cloud environment, it serves as the backbone of the network, overseeing and coordinating cloud infrastructure elements, including provisioning, configuration and management of resources such as VMs, storage, and networking.

Cloud Automation Read More >

Cloud automation handles tasks such as provisioning servers, managing workloads, and applying access control policies.

Cloud Investigation and Response Automation (CIRA) Read More >

CIRA is a cloud security technology designed to automate the collection and analysis of forensics in cloud environments, helping with threat investigation and response.

Cloud Encryption Read More >

Cloud encryption is the process of transforming data from its original plain text format to an unreadable format before it is transferred to and stored in the cloud.

Cloud Workload Protection Platform (CWPP) Read More >

A cloud workload protection platform (CWPP) is a unified cloud security solution that offers continuous threat monitoring and detection for cloud workloads across different types of modern cloud environments.

Cyber Threat Hunting Read More >

Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find malicious actors in your environment that have slipped past your initial endpoint security defenses.

Cloud-Native Application Protection Platform (CNAPP) Read More >

A cloud-native application protection platform (CNAPP) is an all-in-one cloud-native software platform that simplifies mo
detecting, and acting on potential cloud security threats and vulnerabilities.

CDR Use Cases Read More >

In this article, we'll explore five real-world use cases where CDR plays a critical role. Let's dig in.

Cloud Forensics Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

In this article, we'll explore five real-world use cases where CDR plays a critical role. Let's dig in.

Cloud Forensics Read More >

Cloud forensics is a highly specialized branch of digital forensics, capable of conducting investigations in cloud environments during and after a breach. Due to organizations' growing dependence on cloud platforms, cloud forensics is quickly becoming a vital pillar of cybersecurity.

Cloud Threat Hunting Read More >

Cloud threat hunting is the proactive process of identifying potential cyber threats within cloud environments before they evolve into full-blown security breaches

Cloud Data Loss Prevention (DLP) Read More >

Cloud DLP combines tools and practices to safeguard data in the cloud from unauthorized access and transfer. It is essential for cloud data security, risk management, and regulatory compliance.

Cookie Logging Read More >

Cookie logging is the process of collecting cookies from a user's site session.

Continuous Threat Exposure Management (CTEM) Read More >

Continuous threat exposure management (CTEM) is a framework for proactively managing and mitigating threat exposure through an iterative approach that emphasizes building structured organizational processes in addition to leveraging security tools.

Cyber Espionage Read More >

Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

Conditional Access Read More >

Conditional access (CA) is about control — deciding who gets access to which resources, when, and under what conditions. It's a security strategy for organizations that tailors access based on real-time signals like user identity, device health, location, risk, and behavior patterns.

Cybersecurity Read More >

Cybersecurity is the act of defending digital assets, including networks, systems, computers and data, from cyberattacks.

Cyberattacks on Small Businesses Read More >

Many small businesses may still fall into the trap of thinking that their organization isn't large enough or high-profile enough to be the target for attackers. But the fact of the matter is that they have become an easy mark since many do not have advanced tools to defend the business, but they do have what hackers are after: data.

Cloud Access Security Broker (CASB) Read More >

A cloud access security broker (CASB) is a security intermediary between cloud users and cloud-based applications.

Cloud Security Read More >

Cloud security refers to a broad set of strategies and technologies designed to protect data, applications, and infrastructure hosted in the cloud.

Containerization Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Cloud security refers to a broad set of strategies and technologies designed to protect data, applications, and infrastructure hosted in the cloud.

Containerization Read More >

Containerization is a software deployment technology that allows developers to package software and applications in code and run them in isolated compute environments as immutable executable images containing all the necessary files, configurations, libraries, and binaries needed to run that specific application.

Cloud Vulnerabilities Read More >

Cloud vulnerabilities are weaknesses, oversights, or gaps in cloud infrastructure that attackers can exploit to gain unauthorized access and cause harm.

CNAPP vs CWPP Read More >

Read this article to learn what the differences between CNAPP and CWPP and how they work together to improve cloud security.

Cloud Security Assessment Read More >

A cloud security assessment is an evaluation that tests and analyzes an organization's cloud infrastructure to ensure the organization is protected from a variety of security risks and threats.

Cyber Asset Attack Surface Management (CAASM) Read More >

Cloud Detection Read More >

Cloud detection identifies threats, vulnerabilities, and malicious activities within an organization's cloud infrastructure.

Cloud Firewall Read More >

A cloud firewall acts as a barrier between cloud servers and incoming requests by enforcing strict authorization, filtering requests, and blocking any potentially malicious requests from unauthorized clients.

Cloud Detection and Response (CDR) Read More >

CDR is a security approach specifically designed for cloud environments that focuses on threat detection, immediate incident response, and service integrations.

Cloud Native Security Read More >

Cloud native security is a collection of technologies and practices that comprehensively address the dynamic and complex needs of the modern cloud environment.

CDR vs CNAPP Read More >

Cloud Compliance Read More >

Cloud compliance refers to the process of adhering to regulatory standards, international laws and mandates, and indus
practices (frameworks, benchmarks) in the context of cloud computing.

Cloud Migration Read More >

Cloud migration refers to moving everything a business does — from data to applications — into a cloud computing envi

Cloud Infrastructure Read More >

Cloud infrastructure is a collective term used to refer to the various components that enable cloud computing and the delivery of

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Cloud Infrastructure Read More >

Cloud infrastructure is a collective term used to refer to the various components that enable cloud computing and the delivery of cloud services to the customer. This includes hardware, software, network devices, data storage and an abstraction layer that allows users to access virtualized resources.

Continuous Integration and Continuous Delivery (CI/CD) Pipeline Read More >

CI/CD combines the practices of continuous integration (CI) and Continuous Delivery (CD) to allow DevOps teams to deliver code updates frequently, reliably, and quickly.

Common Vulnerability Scoring System (CVSS) Read More >

Cloud Security Best Practices Read More >

In this blog, we'll look at 20 recommended cloud security best practices organizations can implement throughout their cloud adoption process to keep their environments secure from cyberattacks.

Code Security Read More >

Code security is the practice of writing and maintaining secure code. It means taking a proactive approach to dealing with potential vulnerabilities so more are addressed earlier in development and fewer reach live environments.

Cloud Security Strategy Read More >

A cloud security strategy is a framework of tools, policies, and procedures for keeping your data, applications, and infrastructure in the cloud safe and protected from security risks.

Container Security Read More >

Container Security is the continuous process of using security tools to protect containers from cyber threats and vulnerabilities throughout the CI/CD pipeline, deployment infrastructure, and the supply chain.

Cloud Security Issues Read More >

The reasons behind cloud breaches run the gamut, but can be broadly classified into four cloud security challenges: human errors, runtime threats, shadow IT and poor strategic planning.

Cybersecurity Risk Assessment Read More >

A cybersecurity risk assessment is a systematic process aimed at identifying vulnerabilities and threats within an organization's IT environment, assessing the likelihood of a security event, and determining the potential impact of such occurrences.

Cloud Infrastructure Entitlement Management (CIEM) Read More >

Cloud infrastructure entitlement management (CIEM) is a security process that helps security teams analyze and manage identities, access rights, privileges, and permissions in cloud environments.

Cybersecurity Advisory Services Read More >

Cybersecurity advisory services encompass high-level guidance and strategic planning to ensure that an organization's cybersecurity measures are comprehensive, current, and effective.

Cloud Security Policy Read More >

A cloud security policy is a framework with rules and guidelines designed to safeguard your cloud-based systems and data.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Cloud Security Policy Read More >

A cloud security policy is a framework with rules and guidelines designed to safeguard your cloud-based systems and data.

Counter Adversary Operations (CAO) Read More >

Counter Adversary Operations unites intelligence and threat hunting teams to disrupt modern adversaries and raise their cost of doing business.

Cyber Big Game Hunting Read More >

Cyber big game hunting is a type of cyberattack that usually leverages ransomware to target large, high-value organizations or high-profile entities.

Cyber Insurance Read More >

Cyber insurance, sometimes referred to as cyber liability insurance or cyber risk insurance, is a type of insurance that limits a policy holder's liability and manages recovery costs in the event of a cyberattack, data breach or act of cyberterrorism.

Cloud Security Frameworks Read More >

Cloud security frameworks are sets of guidelines, best practices, and controls organizations use to approach the security of their data, applications, and infrastructure in cloud computing environments.

Container Lifecycle Management Read More >

Container lifecycle management is a critical process of overseeing the creation, deployment, and operation of a container until its eventual decommissioning.

CIS Benchmarks Read More >

A CIS Benchmark is a meticulously crafted, comprehensive set of security configuration guidelines for a specific technology. Developed by the Center for Internet Security (CIS), these Benchmarks are key to enhancing an organization's ability to prevent, detect, and respond to cyber threats.

Cybersecurity Transformation Read More >

Cybersecurity transformation is the implementation of a comprehensive cybersecurity strategy that encompasses various components, including risk management, threat intelligence, security governance, incident response readiness, regulatory compliance, and more.

Cloud Workload Protection (CWP) Read More >

Cloud Workload Protection platforms offer organizations a solution to continuously monitor for, and remove threats from their cloud workloads and containers.

Cloud Computing Read More >

Cloud computing, commonly referred to as "the cloud", provides easy online access to a shared pool of configurable cor
resources such as servers, storage, applications, and services.

Cloud Compromise Assessment Read More >

A cloud compromise assessment is an in-depth evaluation of an organization's cloud infrastructure to identify, analyze, a
potential security risks. Performing a regular assessment uncovers vulnerabilities and threats early. Assessments are crucial for
maintaining a strong security posture. The main goal of the assessment is to uncover any signs of compromise before they can escalate into full-blown security incidents.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

potential security risks. Performing a regular assessment uncovers vulnerabilities and threats early. Assessments are crucial for maintaining a strong security posture. The main goal of the assessment is to uncover any signs of compromise before they can escalate into full-blown security incidents.

Credential Stuffing Read More >

Credential stuffing is a cyberattack where cybercriminals use stolen login credentials from one system to attempt to access an unrelated system.

Cybersquatting Read More >

Cybersquatting is the abusive practice of registering and using an internet domain name that is identical or similar to trademarks, service marks, personal names or company names with the bad faith intent of hijacking traffic for financial profit, delivering malware payloads or stealing intellectual property.

Cloud Sprawl Read More >

Cloud sprawl is the uncontrolled proliferation of an organization's cloud services, instances, and resources. It is the unintended but often encountered byproduct of the rapid growth of an organization's cloud services and resources.

Container Scanning Read More >

Container scanning is the process of analyzing components within containers to uncover potential security threats. It is integral to ensuring that your software remains secure as it progresses through the application life cycle.

Crypto-Malware Read More >

Crypto-malware is a type of malicious software, or malware, designed to carry out long-term cryptojacking cyberattacks.

Cybersecurity Sandboxing Read More >

Cybersecurity sandboxing is the use of an isolated, safe space to study potentially harmful code. This practice is an essential tool for security-conscious enterprises and is instrumental in preventing the spread of malicious software across a network.

Cybersecurity Platform Consolidation Best Practices Read More >

Cybersecurity platform consolidation is the strategic integration of diverse security tools into a single, cohesive system, or, the concept of simplification through unification applied to your cybersecurity toolbox.

Computer Worm Read More >

A computer worm is a type of malware that can automatically propagate or self-replicate without human interaction, enabling its spread to other computers across a network.

Cyber Resilience Read More >

Cyber resilience is the concept that describes an organization's ability to minimize the impact of an adverse cyber event and restore their operational systems to maintain business continuity.

Command and Control (C&C) Attacks Read More >

C&C (also known as C2) is a method that cybercriminals use to communicate with compromised devices within a target network.

Credential Harvesting Read More >

Credential harvesting is a cyberattack technique where cybercriminals gather user credentials — such as user IDs, email addresses, passwords, and other login information — en masse.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Credential Harvesting Read More >

Credential harvesting is a cyberattack technique where cybercriminals gather user credentials — such as user IDs, email addresses, passwords, and other login information — en masse.

Cybersecurity Platform Consolidation Read More >

Cybersecurity platform consolidation is the strategic integration of diverse security tools into a single, cohesive system.

Cybersecurity Platform Consolidation Read More >

Cybersecurity platform consolidation is the strategic integration of diverse security tools into a single, cohesive system.

Compromise Assessments Read More >

Compromise assessments are high-level investigations where skilled teams utilize advanced tools to dig more deeply into their environment to identify ongoing or past attacker activity in addition to identifying existing weaknesses in controls and practices. The intent of the comprehensive assessment is to answer the critical question: "Has my organization been breached?"

Cloud Incident Response Read More >

Cloud Incident Response (Cloud IR) is the process you follow when a cybersecurity incident occurs in your cloud environment.

Cloud Security Architecture Read More >

Cloud security architecture is the umbrella term used to describe all hardware, software and infrastructure that protects the cloud environment and its components, such as data, workloads, containers, virtual machines and APIs.

Cloud Application Security Read More >

Cloud application security is the process of securing cloud-based software applications throughout the development lifecycle.

Cloud Data Security Read More >

Cloud data security refers to the technologies, policies, services and security controls that protect any type of data in the cloud from loss, leakage or misuse through breaches, exfiltration and unauthorized access.

Cross Site Scripting (XSS) Read More >

Cross Site Scripting (XSS) is a code injection attack in which an adversary inserts malicious code within a legitimate website.

Cyber Hygiene Read More >

Cyber hygiene refers to the practices computer users adopt to maintain the safety and security of their systems in an online environment.

Container-as-a-Service (CaaS) Read More >

This guide will explore containerization's key role in modern application development and deployment. It will also discuss how containers as a service (CaaS) fits into the broader cloud service landscape, helping you stay ahead of the curve in this e field.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Cloud Security Posture Management (CSPM) Read More >

Cloud security posture management (CSPM) automates the identification and remediation of risks across cloud infrastr

Cyber Risk Read More >

Cyber risk measures the likelihood (probability) that an attacker may exploit a cyber threat, as well as considers the potential impact of

Cloud security posture management (CSPM) automates the identification and remediation of risks across cloud infrastructures.

Cyber Risk Read More >

Cyber risk measures the likelihood (probability) that an attacker may exploit a cyber threat, as well as considers the potential impact of that bad event, such as the loss of confidentiality, integrity and availability of an organization's information.

Cloud Monitoring Read More >

Cloud monitoring is the practice of measuring, evaluating, monitoring, and managing workloads inside cloud tenancies against specific metrics and thresholds. It can use either manual or automated tools to verify the cloud is fully available and operating properly.

Cloud Governance Read More >

Cloud governance is a set of policies and rules used by companies who build or work in the cloud. This framework is designed to ensure data security, system integration and the deployment of cloud computing are properly managed.

Common Cloud Threats: Exploitation of Misconfigured Image Containers Read More >

Developers sometimes use base images from an external registry to build their images. Unfortunately, these images can contain malware or vulnerable libraries.

Cloud Service Provider Abuse Read More >

Adversaries leverage cloud service providers to abuse provider trust relationships and gain access to additional targets through lateral movement.

Cloud Vulnerability Exploitation Read More >

The fast adoption of the cloud has expanded the attack surface businesses must monitor and protect to avoid cloud vulnerability exploitation.

Credential Theft Read More >

Credential theft is the act of stealing personal information such as usernames, passwords and financial information in order to gain access to an online account or system.

CRUD vs REST Explained Read More >

In this article, we will introduce CRUD and REST, explain their similarities and differences, and then consider how to best monitor their performance.

CRUD Read More >

CRUD is the acronym for CREATE, READ, UPDATE and DELETE. These terms describe the four essential operations for creating and managing persistent data elements, mainly in relational and NoSQL databases.

Continuous Monitoring Read More >

Continuous monitoring is an approach where an organization constantly monitors its IT systems and networks to detect threats, performance issues, or non-compliance problems in an automated manner.

Common Vulnerabilities & Exposures (CVE) Read More >

Common Vulnerabilities and Exposures (CVEs) is a framework and international effort to maintain updated registry of all computer security vulnerabilities and exposures.

Container Security Best Practices Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Common Vulnerabilities and Exposures (CVEs) is a framework and international effort to maintain updated registry of all known computer security vulnerabilities and exposures.

Container Security Best Practices Read More >

This article discusses the concept of container security and its main challenges, as well as best practices for developing secure containerized applications.

Cyber Kill Chain Read More >

The cyber kill chain is an adaptation of the military's kill chain, which is a step-by-step approach that identifies and stops enemy activity.

Cryptojacking Read More >

Cryptojacking is the unauthorized use of a person's or organization's computing resources to mine cryptocurrency.

Cloud Analytics Read More >

Cloud analytics is an umbrella term encompassing data analytics operations that are carried out on a cloud platform to produce actionable business insights.

Centralized Logging Read More >

Centralized logging is the process of collecting logs from networks, infrastructure, and applications into a single location for storage and analysis.

Cyberattacks Read More >

A cyberattack is an attempt by cybercriminals, hackers or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying or exposing information.

Cyber Vulnerabilities Read More >

In this article, we review the 7 most common types of vulnerabilities, including: misconfigurations, unsecured APIs, zero days, unauthorized access, and unpatched software.

D

Data Leaks vs Data Breaches Read More >

Learn the differences between data leaks and data breaches, their common causes, and proactive ways to prevent such threats from occurring.

DLP Best Practices Read More >

In this article, we'll review actionable DLP best practices that help organizations reduce data-related risk and strengthen posture.

Dora SaaS Security Read More >

DORA was created by the EU to strengthen the operational resilience of its financial entities. The EU recognized that the transformation taking place in the financial services industry placed an unprecedented reliance on technology.

Dynamic Application Security Testing (DAST) Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

DORA was created by the EU to strengthen the operational resilience of its financial entities. The EU recognized that the digital transformation taking place in the financial services industry placed an unprecedented reliance on technology.

Dynamic Application Security Testing (DAST) Read More >

Dynamic application security testing (DAST) is a method that evaluates an application's security by testing it at runtime without access to its underlying source code.

Dark Web Monitoring Read More >

Dark web monitoring is the process of searching for, and tracking, your organization's information on the dark web.

Decentralized Identity Read More >

Decentralized identity (DCI) often uses distributed ledger technologies (DLT) like blockchain for authentication and can help address challenges related to centralized identity management.

Data Loss Prevention (DLP) Read More >

Data loss prevention (DLP) is a set of tools and procedures that forms part of a company's overall security strategy and focuses on detecting and preventing the loss, leakage, or misuse of data through breaches, exfiltration transmissions, and unauthorized use.

Digital Risk Protection Read More >

Digital risk protection (DRP) involves monitoring and mitigating threats to an organization's digital assets across public, deep, and dark web channels.

DevOps Monitoring Read More >

DevOps monitoring is the practice of tracking and measuring the performance and health of systems and applications in order to identify and correct issues early.

Detection Engineering Read More >

Detection engineering is the process of identifying threats before they can do significant damage.

Digital Forensics and Incident Response (DFIR) Read More >

Digital Forensics and Incident Response (DFIR) is a field within cybersecurity that focuses on the identification, investigation, and remediation of cyberattacks.

Deep Web vs Dark Web Read More >

"Deep web" and "dark web" are NOT interchangeable terms. The deep web is any part of the Net that is not indexed by search engines. The dark web uses encryption software to provide even greater security.

Data Compliance Read More >

Data compliance is the practice of ensuring that sensitive and protected data is organized and managed in a way that en es organizations and government entities to meet relevant legal and government regulations.

Data Theft Prevention Read More >

Understand data theft — what it is, how it works, and the extent of its impact and look into the principles and best practic theft prevention.

Dark AI Read More >

Dark AI refers to the application of AI technologies — and notably, recent innovations in generative AI (GenAI) — for the purposes of accelerating or enabling cyberattacks.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Dark AI Read More >

Dark AI refers to the application of AI technologies — and notably, recent innovations in generative AI (GenAI) — for the purposes of accelerating or enabling cyberattacks.

Disinformation Campaign Read More >

In this post, we'll explore the mechanics of disinformation campaigns, deliberate efforts to spread false information.

Deepfake Attack Read More >

Deepfakes are AI-generated forgeries — false images, audio, or video — that appear convincingly genuine.

Data Classification Read More >

Data Flow Mapping Read More >

Data Onboarding Read More >

Digital Forensics Read More >

Digital forensics is a subset of forensic science that examines system data, endpoint data, user activity, and other pieces of digital evidence to help organizations identify, respond to, and prevent security incidents, breaches, and internal threats.

DevOps Read More >

DevOps is a mindset and set of practices meant to effectively integrate development and operations into a cohesive whole in the modern product development life cycle. DevOps breaks down the divide between creating a product and maintaining it to allow for higher-paced service and application delivery.

DevOps vs. DevSecOps Read More >

DevOps and DevSecOps share cultural similarities but address different business goals. Knowing when to use each practice or transition from DevOps to DevSecOps can improve your business.

DevSecOps Read More >

DevSecOps is a philosophical framework that combines aspects of software development, security, and operations into a cohesive whole. With DevSecOps, developers are more aware of and responsible for maintaining security best practices within their code. It also means operations and security teams implement tools and policies that provide regular security checks throughout the continuous integration/continuous delivery (CI/CD) pipeline.

Data Portability Read More >

Data portability is the ability of users to easily transfer their personal data from one service provider to another.

Data Security Posture Management (DSPM) Read More >

DSPM helps organizations manage their data across the cloud, monitor for risks, enforce security policies, and ensure re
compliance.

Data Poisoning Read More >

Data poisoning is a type of cyberattack in which an adversary intentionally compromises a training dataset used by an A
learning (ML) model to influence or manipulate the operation of that model.

Data Gravity Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Data poisoning is a type of cyberattack in which an adversary intentionally compromises a training dataset used by an AI or machine learning (ML) model to influence or manipulate the operation of that model.

Data Gravity Read More >

Data gravity is a term that captures how large volumes of data attract applications, services, and even more data.

Data Privacy Read More >

Data privacy, also called information privacy, is an area of data protection that addresses the proper storage, access, retention, and security of sensitive data, which helps organizations meet regulatory requirements and protect the confidentiality and immutability of their data.

Data Leakage Read More >

Data leakage refers to the unauthorized transfer of data from inside an organization to an external destination.

Data Protection vs Data Security Read More >

Data protection and data security are often used interchangeably, but they have distinct focuses and objectives. Read this post to learn the difference.

Database Monitoring Read More >

Database monitoring is the continuous tracking of a database's activities and performance. It is crucial in helping optimize and tune database processes for high performance and reliability. Security is also another key factor to consider when it comes to monitoring databases due to the importance of this data.

Data Security Read More >

Data security is the practice of protecting digital data from unauthorized access, use or disclosure in a manner consistent with an organization's risk strategy.

Debug Logging Read More >

Debug logging specifically focuses on providing information to assist in identifying and resolving bugs or defects.

Data Encryption Read More >

Data encryption converts plain text into an encoded format to protect against unauthorized access to data.

Distributed Denial-of-Service (DDoS) Attacks Read More >

DDoS, short for distributed-denial-of-service, is a cyberattack that attempts to interrupt a server or network by flooding it with fake internet traffic, preventing user access and disrupting operations.

Denial-of-Service (DoS) Attacks Read More >

A Denial-of-Service (DoS) attack is a cyberattack that floods a machine or network with false requests in order to disrupt business operations.

Data Obfuscation Read More >

Data obfuscation is the process of disguising confidential or sensitive data to protect it from unauthorized access. Data tactics can include masking, encryption, tokenization, and data reduction.

Downgrade Attacks Read More >

In a downgrade attack, an attacker forces the target system to switch to a low-quality, less secure mode of operation.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

tactics can include masking, encryption, tokenization, and data reduction.

Downgrade Attacks Read More >

In a downgrade attack, an attacker forces the target system to switch to a low-quality, less secure mode of operation.

Data Breach Read More >

A data breach is a security incident where an organization's data is illegally stolen, copied, viewed, or released by an unauthorized individual or group.

Data Logging Read More >

Data logging is the process of capturing, storing and displaying one or more datasets to analyze activity, identify trends and help predict future events.

Domain Spoofing Read More >

Domain spoofing is a form of phishing where an attacker impersonates a known business or person with fake website or email domain to fool people into the trusting them.

Defense in Depth Read More >

Defense in depth provides intensive security measures using a layered approach to protect your company from cyberattacks.

Data Exfiltration Read More >

Data exfiltration is the theft or unauthorized transfer of data from a device or network.

E

Enterprise Browser Read More >

Enterprise browsers have enhanced security features to help organizations mitigate browsing-related cyber threats, enforce compliance policies, and provide better visibility into employee internet activity.

External Authentication Method (EAM) Read More >

Traditional External Authentication Methods (EAM) rely on identity providers to authenticate users. These solutions validate credentials and enforce MFA, but do not assess risk signals in real time. CrowdStrike takes EAM a step further by combining authentication with advanced risk analysis.

Endpoint Data Loss Prevention (DLP) Read More >

Endpoint data loss prevention (DLP) is a set of tools, technologies, and processes designed to protect data on endpoint devices from unauthorized access and data exfiltration.

Extended Detection and Response (XDR) Read More >

XDR (extended detection and response) collects and correlates data from endpoints, cloud workloads, networks and en and prioritizes them, and delivers them to security teams in a normalized format through a single console.

Employee Cybersecurity Awareness Training Program Read More >

CrowdStrike's how-to guide provides SMBs the steps & essentials (with examples) to develop the right training programs for your employees.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Employee Cybersecurity Awareness Training Program Read More >

CrowdStrike's how-to guide provides SMBs the steps & essentials (with examples) to develop the right training programs for your employees.

Entra ID: (formerly Azure Active Directory) Read More >

In this article, we'll explore Entra ID, considering its advantages over traditional identity services. We'll also look at how it integrates with CrowdStrike Falcon® Identity Protection to enhance your cybersecurity posture.

Endpoint Detection and Response (EDR) Read More >

Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response (EDTR), is an endpoint security solution that continuously monitors endpoint devices to detect and mitigate cyber threats.

Endpoint Protection Platforms (EPP) Read More >

An endpoint protection platform (EPP) is a suite of endpoint security technologies such as antivirus, data encryption, and data loss prevention that work together on an endpoint device to detect and prevent security threats like file-based malware attacks and malicious activity.

EDR vs NGAV Read More >

Discover more about two of the most critical elements to every cybersecurity architecture – endpoint detection and response (EDR) and next-generation antivirus (NGAV) – and the points organizations should consider when selecting and integrating these tools

Endpoint Protection Software Read More >

Endpoint protection software offers a centralized management system from which security administrators can monitor, protect, and investigate vulnerabilities across all endpoints, including computers, mobile devices, servers and connected devices.

Endpoints Read More >

An endpoint is any device that can be connected to a network. Common examples of endpoints include computers, laptops, mobile phones, tablets and servers.

EDR vs MDR vs XDR Read More >

Learn the differences between endpoint detection and response (EDR), managed detection and response (MDR) and extended detection and response (XDR).

Endpoint Management Read More >

Endpoint management is an IT and cybersecurity process that consists of two main tasks: evaluating, assigning and overseeing the access rights of all endpoints; and applying security policies and tools that will reduce the risk of an attack or prevent such events.

EPP vs. EDR Read More >

EPP and EDR are two critical and distinct components within a comprehensive cybersecurity strategy.

Extended Internet of Things (XIoT) Read More >

The extended internet of things (XIoT) is an umbrella term that includes all internet of things (IoT) or physical devices co internet. It encompasses IoT, operational technology (OT), internet of medical things (IoMT), industrial IoT (IIoT), and su control and data acquisition (SCADA).

Endpoint Security Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

control and data acquisition (SCADA).

Endpoint Security Read More >

Endpoint security, or endpoint protection, is the cybersecurity approach to defending endpoints – such as desktops, laptops, and mobile devices – from malicious activity.

Endpoint Monitoring Read More >

Endpoint monitoring involves the continuous monitoring and management of devices that connect to a network, such as computers, mobile devices, and servers.

Exposure Management vs. Vulnerability Management Read More >

Exposure management and vulnerability management both play pivotal roles in supporting an organization's security posture. However, they serve different functions in cybersecurity.

External Attack Surface Management (EASM) Read More >

External Attack Surface Management (EASM) refers to the continuous discovery, monitoring, evaluation, prioritization, and remediation of attack vectors of an organization's external attack surface. An External Attack Surface, also known as Digital Attack Surface, is the sum of an organization's internet-facing assets and the associated attack vectors which can be exploited during an attack.

Ethical Hacker Read More >

An ethical hacker, also known as a 'white hat hacker', is employed to legally break into computers and networks to test an organization's overall security. Ethical hackers possess all the skills of a cyber criminal but use their knowledge to improve organizations rather than exploit and damage them.

Exploit Kits Read More >

An exploit kit is a toolkit that cybercriminals use to attack specific vulnerabilities in a system or code.

Error Logs Read More >

An error log is a file that contains detailed records of error conditions a computer software encounters when it's running.

Event Log Read More >

An event is any significant action or occurrence that's recognized by a software system and is then recorded in a special file called the event log.

Email Spoofing Read More >

Email spoofing is a type of cyberattack that targets businesses by using emails with forged sender addresses. Because the recipient trusts the alleged sender, they are more likely to open the email and interact with its contents, such as a malicious link or attachment.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

F

Firewall as a Service (FWaaS) Read More >

Firewall as a service (FWaaS) is a networking solution that deploys firewalls on demand across cloud environments.

Fog Ransomware Read More >

Firewall as a Service (FWaaS) Read More >

Firewall as a service (FWaaS) is a networking solution that deploys firewalls on demand across cloud environments.

Fog Ransomware Read More >

Fog Ransomware is a new ransomware variant that uses compromised virtual private network (VPN) credentials or system vulnerabilities to gain access to an organization's network and rapidly encrypt data in an attempt to earn quick payouts.

Fileless Malware Read More >

Fileless malware is a type of malicious activity that uses native, legitimate tools built into a system to execute a cyberattack. Unlike traditional malware, which typically requires a file to be downloaded and installed, fileless malware operates in memory or manipulates native tools, making it harder to detect and remove.

Free Antivirus vs Paid Antivirus Software Read More >

In this guide, we outline the key differences between free and paid antivirus solutions available to small businesses and help owners decide which option is right for their company.

File Integrity Monitoring Read More >

File integrity monitoring (FIM) is a security process that monitors and analyzes the integrity of critical assets, including file systems, directories, databases, network devices, the operating system (OS), OS components and software applications for signs of tampering or corruption, which may be an indication of a cyberattack.

G

Golden Ticket Attack Read More >

A golden ticket attack is a post-exploitation technique in which a threat actor gains near-unrestricted access to an organization's domain by forging authentication tickets within Microsoft Active Directory (AD).

Google Cloud Migration Read More >

Read this article to learn what a Google Cloud migration entails, its benefits, and the strategic approach needed for a successful transition.

Generative AI (GenAI) in Cybersecurity Read More >

Generative AI (GenAI) is a branch of artificial intelligence that focuses on generating new data based on existing data. This sophisticated technology enables a variety of use cases — such as data retrieval and analysis, content generation, and summarization — across a growing number of applications.

General Data Protection Regulation (GDPR) Read More >

The General Data Protection Regulation (GDPR) is the European Union's (EU) personal data protection law that aims to privacy of EU citizens. Enacted in May 2018, it imposes a unified set of rules on all organizations that process personal d from the EU, regardless of location.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

H

H

Hybrid Cloud Read More >

A hybrid cloud combines elements of a public cloud, private cloud and on-premises infrastructure into a single, common, unified architecture allowing data and applications to be shared between the mixed IT environment.

Healthcare Cybersecurity Read More >

Healthcare cybersecurity refers to the practices and technologies designed to protect healthcare systems, patient data, and medical devices from cyberattacks.

Honeypots Read More >

A honeypot is a cybersecurity mechanism that leverages a manufactured attack target to lure cybercriminals away from legitimate targets and gather intelligence about the identity, methods and motivations of adversaries.

How to choose between outsourced vs in-house cybersecurity Read More >

Learn the benefits and challenges of in-house and outsourced cybersecurity solutions to find the best fit for your business.

Honeytokens Read More >

Honeytokens are digital resources that are purposely designed to be attractive to an attacker, but signify unauthorized use.

How to Build a Zero Trust Strategy Read More >

In this post, we'll outline a framework for a true Zero Trust model that adheres to industry best practices while specifically avoiding the potential pitfalls.

How to Hire a Cybersecurity Expert for Your Small Business Read More >

Cybersecurity specialists play a key role in securing your organization's information systems by monitoring, detecting, investigating and responding to security threats. So how should you go about bringing top cybersecurity talent to your company?

Honey Account Read More >

A honey account is a fabricated user account that triggers alerts for unauthorized activity when accessed. The honey account is part of your system, but it serves no real function other than incident detection.

How to Implement Zero Trust in Stages Read More >

CrowdStrike offers the following recommendations to move Zero Trust along a journey of maturity based on your needs and priorities:

How to Choose the Right Cybersecurity Vendor for Your Business Read More >

Learn the eight factors to use when assessing a cybersecurity vendor to help you choose the right fit for your business r
future.

How to increase your SMB cybersecurity budget Read More >

Sharing helpful thought starters, considerations & tips to help IT leaders make the case for increasing their cybersecurit
Read more!

How to Mitigate Insider Threats for Small Businesses Read More >

In this post, we'll take a closer look at insider threats – what they are, how to identify them, and the steps you can take to better protect

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Read more!

How to Mitigate Insider Threats for Small Businesses Read More >

In this post, we'll take a closer look at insider threats – what they are, how to identify them, and the steps you can take to better protect your business from this serious threat.

How to Spot a Phishing Email Read More >

The most common form of phishing attack is a phishing email. Discover the 7 telltale signs of a phishing email with examples here.

How to Create a Cybersecurity Budget for Your Small Business Read More >

Creating a budget for your evolving cybersecurity needs is critical. Learn tips to develop a budget that covers the protection your small business needs.

Hashing in Cybersecurity Read More >

In the context of cybersecurity, hashing is a way to keep sensitive information and data — including passwords, messages, and documents — secure.

How Does Ransomware Spread Read More >

As ransomware operators continue to evolve their tactics, it's important to understand the 10 most common attack vectors used so that you can effectively defend your organization.

HIPAA Security Rule Read More >

The HIPAA Security Rule specifies security standards for protecting individuals' electronic personal health information (ePHI) that is received, used, maintained, or transmitted by covered entities and their business associates.

Hybrid Cloud Security Read More >

Hybrid cloud security is the protection of data and infrastructure that combines elements of private cloud, public cloud, and on-premises infrastructure into a unified architecture.

Human Intelligence (HUMINT) in Cybersecurity Read More >

Human Intelligence (HUMINT) is a form of "on the ground" information gathering using human sources to collect information.

Hypervisor (VMM) Read More >

A hypervisor, or virtual machine monitor (VMM), is virtualization software that creates and manages multiple virtual machines (VMs) from a single physical host machine.

History of Ransomware Read More >

Ransomware first cropped up around 2005 as just one subcategory of the overall class of scareware. Learn how it's evolved since then.

Hacktivism Read More >

Hacktivism is a combination of the words "hack" and "activism". Hacktivists engage in disruptive or damaging activity on cause, be it political, social or religious in nature.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

I

Interactive Application Security Testing (IAST) Read More >

Interactive Application Security Testing (IAST) is a modern method for ensuring application security by analyzing how code behaves in real time as the application runs.

ISO Compliance Read More >

ISO compliance in SaaS security refers to adherence to the standards and requirements set forth by the International Organization for Standardization (ISO) for information security management systems. ISO has developed various standards, but the most relevant one for SaaS security is ISO 27001.

Identity Security Read More >

Identity security, also known as identity protection, is a comprehensive solution that protects all types of identities within the enterprise

Identity Monitoring Read More >

Identity monitoring is the continuous analysis of authentication activity, access patterns, and privilege changes to detect identity-based threats and prevent unauthorized access.

Identity Theft Prevention Strategies Read More >

Learn how to safeguard personal and corporate identities from identity-based attacks and identity theft.

Identity Threat Detection and Response (ITDR) Read More >

Identity threat detection and response (ITDR) is a security procedure for identifying, reducing, and responding to potential identity-based threats, such as compromised user accounts, leaked passwords, data breaches, and fraudulent activity.

Identity Governance and Administration (IGA) Read More >

IGA is a comprehensive framework that combines identity lifecycle management with access governance to streamline processes and enhance security.

Indicators of Compromise (IOC) Security Read More >

An Indicator of Compromise (IOC) is a piece of digital forensics that suggests that an endpoint or network may have been breached.

Identity Provider (IdP) Security Read More >

An effective IdP security solution goes beyond verifying identities; it enforces stringent access control policies that prev
unauthorized users from slipping through the cracks.

Identity-Based Attacks Read More >

To better understand the identity threat landscape, let's explore seven common identity-based attacks and how they wo

Identity Access Management (IAM) Read More >

Identity and access management (IAM) is a cybersecurity framework in which the IT team controls access to computer systems, cloud applications, networks, and assets based on each user or device's digital identity.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Identity Access Management (IAM) Read More >

Identity and access management (IAM) is a cybersecurity framework in which the IT team controls access to computer systems, cloud applications, networks, and assets based on each user or device's digital identity.

IT Security Read More >

IT security is the overarching term used to describe the collective strategies, methods, solutions and tools used to protect the confidentiality, integrity and availability of the organization's data and digital assets.

Indicators of Attack (IOAs) Read More >

IOAs are telltale signs or activities that signal a potential cybersecurity threat or attack is in progress.

Incident Response (IR) Read More >

Incident response (IR) is the steps used to prepare for, detect, contain, and recover from a data breach.

IT Automation Read More >

IT automation is the use of software to complete time-consuming, repetitive IT tasks without manual intervention.

Identity Security Posture Management (ISPM) Read More >

Identity security posture management (ISPM) is a framework used to strengthen and maintain the security posture of an organization's identity infrastructure to prevent breaches.

Insider Threats Read More >

An insider threat is a cybersecurity risk that comes from within the organization — usually by a current or former employee or other person who has direct access to the company network, sensitive data and intellectual property (IP).

Insider Threat Indicators Read More >

An insider threat refers to the potential for a person to leverage a position of trust to harm the organization through misuse, theft or sabotage of critical assets.

Internet of Things (IoT) Security Read More >

IoT security focuses on protecting, monitoring and remediating threats related to the Internet of Things (IoT) — the network of connected devices equipped to gather, store and share data via the internet.

Identity Segmentation Read More >

Identity segmentation is a method to restrict access to applications/resources based on identities. These identities could be human accounts, service (programmatic accounts), or privileged accounts.

Incident Responder Read More >

An incident responder is a key player on an organization's cyber defense line. When a security breach is detected, incident responders step in immediately.

Infrastructure as Code Security Read More >

Infrastructure as code security is the practice of addressing security configuration issues in the IaC layer rather than sca deployed cloud resources.

IaC Scanning Read More >

IaC scanning is the process of codifying infrastructure setup and configuration to enable organizations to automate and streamline

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

deployed cloud resources.

IaC Scanning Read More >

IaC scanning is the process of codifying infrastructure setup and configuration to enable organizations to automate and streamline their deployments.

Injection Attacks Read More >

Injection attacks occur when attackers exploit vulnerabilities in an application to send malicious code into a system.

IT Asset Discovery Read More >

IT asset discovery is the process an organization uses to identify, catalog, and document all of its IT assets.

IT Asset Management (ITAM) Read More >

IT asset management (ITAM) includes digital, cloud and hardware asset management and is a crucial discipline in cybersecurity.

Infrastructure as Code (IaC) Read More >

Infrastructure as Code (IaC) is the process of dynamically managing and provisioning infrastructure through code instead of a manual process to simplify app development, configuration, and runtime.

Incident Response Plan Read More >

Most IR plans can be summed up in 4 common steps: Preparation, Detection & Analysis, Containment & Eradication, and Post-Incident Activity.

IIS Logs Read More >

IIS creates log files for each website it serves. You can set the log file location for an IIS-hosted website from the "Logging" section of the website.

Infrastructure Monitoring Read More >

Infrastructure Monitoring allows teams to collect operational and performance data from their systems to diagnose, fix, and improve them.

IOA vs IOC Read More >

Indicators of Attack vs Indicators of Compromise: Defining & Understanding the Differences

Infrastructure as a Service (IaaS) Read More >

Infrastructure as a Service (IaaS) is a cloud computing model in which a third-party cloud service provider offers virtualized compute resources such as servers, data storage and network equipment on demand over the internet to clients.

J

Just-in-Time (JIT) Access Read More >

Just-in-time (JIT) access is a dynamic, on-demand approach to access control that grants human and non-human identi permissions to an application or system only when they need them to perform a specific, necessary task and only for the minimal amount of time necessary.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Just-in-time (JIT) access is a dynamic, on-demand approach to access control that grants human and non-human identities permissions to an application or system only when they need them to perform a specific, necessary task and only for the minimal amount of time necessary.

K

Kerberoasting Attacks Read More >

Kerberoasting is a post-exploitation attack technique targeting the Kerberos authentication protocol, enabling adversaries to extract encrypted service account credentials from Active Directory.

Kubernetes Frameworks Read More >

Kubernetes is a container orchestration system used to run various types of workloads, from user-facing web applications to backend processes.

Kubernetes Security Best Practices Read More >

These practices are based on the 4 Cs, which are designed to help organizations achieve optimal security across the primary layers of typical Kubernetes environments.

Kubernetes as a Service (KaaS) Read More >

KaaS is a managed solution offered by cloud providers to streamline the deployment, management, and operation of Kubernetes clusters.

Kubernetes Security Read More >

Kubernetes security is the application of techniques and processes to protect cloud-native applications running on Kubernetes (also known as K8s) from vulnerabilities or malicious actors.

Kubernetes with Admission Controllers Read More >

In this article, we'll take a deep dive into the world of Kubernetes admission controllers by discussing their importance, internal mechanisms, image scanning capabilities, and significance in the security posture of Kubernetes clusters.

Kubernetes vs Docker Read More >

Docker is a versatile platform responsible for creating, managing, and sharing containers on a single host, while Kubernetes is a container orchestration tool responsible for the management, deployment, and monitoring of clusters of containers across multiple nodes.

Keyloggers Read More >

Keyloggers, or keystroke loggers, are tools that record what a person types on a device. While there are legitimate and legal uses for keyloggers, many uses for keyloggers are malicious.

Kubernetes vs. Mesos Read More >

Container orchestration engines (COEs) make managing containerized workloads easier by automating operational tas
Kubernetes and Apache Mesos are two of the most popular COEs.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Kubernetes and Apache Mesos are two of the most popular COEs.

L

Logj Vulnerability Read More >

Log4Shell is a critical zero-day vulnerability (CVE-2021-44228) in Log4j that allows attackers to execute arbitrary code remotely on affected systems.

Lateral Movement Read More >

Lateral movement refers to the techniques that a cyberattacker uses, after gaining initial access, to move deeper into a network in search of sensitive data and other high-value assets.

Low-Code Application Platform Read More >

In this post, we'll examine the low-code application platform — and its near cousin, the low-code application platform — consider its benefits and limitations, and look specifically at the role it can play in cybersecurity.

Log Streaming Read More >

Log streaming in cybersecurity refers to the real-time transfer and analysis of log data to enable immediate threat detection and response.

Log Retention Read More >

Log retention refers to how organizations store log files relating to security and for how long. It is a significant part of log management, and it's integral to your cybersecurity.

Logging vs Monitoring Read More >

In this article, we'll explore logging and monitoring processes, looking at why they're important for managing applications. We'll also cover best practices to integrate logging with monitoring to obtain robust visibility and accessibility over an entire application.

Logging Best Practices Read More >

This article considers some logging best practices that can lay the groundwork for a robust and scalable logging infrastructure.

Living off the Land (LOTL) Attacks Read More >

Living off the land (LOTL) is a fileless malware cyberattack technique where the cybercriminal uses native, legitimate tools within the victim's system to sustain and advance an attack.

Log Analysis Read More >

Log analysis is the process of reviewing computer-generated event logs to proactively identify bugs, security threats, factors affecting system or application performance, or other risks.

Logging Levels Read More >

Setting up meaningful log levels is an important step in the log management process. Logging levels allow team member accessing and reading logs to understand the significance of the message they see in the log or observability tools bein

Log File Formats Read More >

A log format defines how the contents of a log file should be interpreted. Typically, a format specifies the data structure and type of

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

accessing and reading logs to understand the significance of the message they see in the log or observability tools being used.

Log File Formats Read More >

A log format defines how the contents of a log file should be interpreted. Typically, a format specifies the data structure and type of encoding.

Log Files Explained Read More >

A log file is an event that took place at a certain time and might have metadata that contextualizes it.

Logging as a Service (LaaS) Read More >

Logging as a service (LaaS) is a solution that centralizes the collection, analysis, monitoring and management of logs. In this article, you'll learn what LaaS is and why it's important. You'll also discover the differences between LaaS and traditional log monitoring solutions, and how to choose a LaaS provider.

Log Rotation Read More >

Learn about the basics of log rotation—why it's important, and what you can do with your older log files.

Log Aggregation Read More >

Log aggregation is the mechanism for capturing, normalizing, and consolidating logs from different sources to a centralized platform for correlating and analyzing the data.

Log Management Read More >

Log management is the practice of continuously gathering, storing, processing, synthesizing and analyzing data from disparate programs and applications.

Log Parsing Read More >

Log parsing is the process of converting log data into a common format to make them machine-readable.

M

Machine Learning Security Operations (MLSecOps) Read More >

Machine learning security operations (MLSecOps) is an emerging discipline focused on the security of machine learning systems throughout their lifecycle.

Microservices Security Read More >

In this article, we'll look at these security challenges that microservices introduce, along with the key approaches and tools used to address them.

Machine Identity Management (MIM) Read More >

Machine identity management is the process of securing and managing the digital credentials that machines use to recognize and trust each other. Just like humans need IDs and passwords to access systems, machines rely on digital certificates, cryptographic keys, and other credentials to authenticate and communicate securely.

Malware Analysis Read More >

Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL to help detect and mitigate

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

keys, and other credentials to authenticate and communicate securely.

Malware Analysis Read More >

Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL to help detect and mitigate potential threats.

Malware vs Virus Read More >

The term malware describes any program or code created with the intent to do harm to a computer, network or server. A virus is a type of malware limited only to programs or code that self-replicates or copies itself in order to spread to other devices or areas of the network.

Man in the Middle (MITM) Attack Read More >

A man-in-the-middle attack is a type of cyberattack in which an attacker eavesdrops on a conversation between two targets.

Mobile Threat Defense (MTD) Read More >

Mobile threat defense combines real-time threat detection, automated response and remediation, and comprehensive visibility and control. Learn more!

Managed XDR (MXDR) Read More >

Managed XDR (MXDR) is an outsourced security service that provides advanced detection and response capabilities using a combination of digital technologies and human-led expertise.

Multi-factor Authentication (MFA) Read More >

Multi-factor authentication (MFA) is a multi-layered security system that grants users access to a network, system or application only after confirming their identity with more than one credential or authentication factor.

MDR vs SOC Read More >

Cybersecurity tools and services abound, but two standout services are managed detection and response (MDR) and security operations center (SOC) services.

Managed SIEM Read More >

Managed SIEM gives you the functionalities of traditional SIEM but with the benefits of a managed service model. Along with the strengthened security posture that traditional SIEM affords your organization, you can offload the burden of managing complex SIEM technologies in-house.

Machine Learning and AI in Identity Security Read More >

In the domain of identity security, AI presents a promising pathway forward. By harnessing AI-driven identity security solutions, organizations can strengthen their defenses against identity-based attacks.

Managed Service Provider (MSP) Read More >

Managed service providers (MSPs) offer a wide range of IT and cybersecurity services to help organizations manage ar their technology infrastructure.

Managed Security Services (MSS) Read More >

Managed security services (MSS) is an umbrella term used to describe any cybersecurity service or solution offered by a third-party provider or managed security service provider (MSSP).

Multi-Cloud Management Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Managed security services (MSS) is an umbrella term used to describe any cybersecurity service or solution offered by a third-party provider or managed security service provider (MSSP).

Multi-Cloud Management Read More >

Maintaining consistent security across platforms is crucial in a multi-cloud environment. Learn more about challenges and best practices!

Multi-Cloud Security Read More >

It is important to implement multi-cloud security to protect your infrastructure, application, and data across multiple clouds.

Multi-Cloud Vulnerability Management Read More >

Multi-cloud vulnerability management is the continuous process of identifying and remediating security vulnerabilities across all your cloud environments, whether they're public, private, or hybrid.

Managed Detection and Response (MDR) Read More >

Managed detection and response (MDR) is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring, and response.

Managed Detection and Response (MDR) Read More >

Managed detection and response (MDR) is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring, and response.

Machine Learning (ML) Read More >

This article provides an overview of foundational machine learning concepts and explains the growing application of machine learning in the cybersecurity industry, as well as key benefits, top use cases, common misconceptions and CrowdStrike's approach to machine learning.

Mobile Malware Read More >

Mobile malware is malicious software designed to target mobile devices. Click here to read about the different types and distribution methods.

Managed Cloud Security Read More >

Managed cloud security protects an organization's digital assets through advanced cybersecurity measures, performing tasks like constant monitoring and threat detection.

MDR vs MSSP Read More >

In this post, we explore these two services, outline their key differentiators and help organizations decide which option is best for their business.

MITRE ATT&CK Framework Read More >

The MITRE ATTACK Framework is a curated knowledge base that tracks cyber adversary tactics and techniques used l
actors across the entire attack lifecycle.

Malware Spam (Malspam) Read More >

Malspam, short for malicious spam or spam containing malware, is a spam email that delivers malware as the malicious payload.

MSP vs. MSSP Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Malware Spam (Malspam) Read More >

Malspam, short for malicious spam or spam containing malware, is a spam email that delivers malware as the malicious payload.

MSP vs. MSSP Read More >

While both MSPs and MSSPs are third-party providers, the primary difference between the two is the scope of their offerings. Learn more here!

Microservices Architecture Read More >

A microservice-based architecture is a modern approach to software development that breaks down complex applications into smaller components that are independent of each other and more manageable.

Managed Security Service Providers (MSSP) Explained Read More >

A managed security service provider (MSSP) is an external party that provides cybersecurity services to its customers.

Multi-Cloud Read More >

Multi-cloud is when an organization leverages multiple public cloud services. These commonly consist of compute and storage solutions, but there are numerous options from various platforms to build your infrastructure.

Malware Read More >

Malware (malicious software) is an umbrella term used to describe a program or code created to harm a computer, network, or server. Cybercriminals develop malware to infiltrate a computer system discreetly to breach or destroy sensitive data and computer systems.

Malware Hosting Read More >

Malware hosting occurs when cybercriminals use a free or compromised hosting account to host malware while using the hosting provider's reputation as cover.

Malware Detection Techniques Read More >

Malware detection is a set of defensive techniques and technologies required to identify, block and prevent the harmful effects of malware. This protective practice consists of a wide body of tactics, amplified by various tools.

Mean Time to Repair Explained Read More >

Mean time to repair (MTTR) is a key performance indicator (KPI) that represents the average time required to restore a system to functionality after an incident.

Malicious Code Read More >

Malicious code is a term for code designed to cause damage, security breaches, or other threats to application security.

Malvertising Read More >

Malvertising is a relatively new cyberattack technique that injects malicious code within digital ads.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

N

Network Vulnerability Assessment Read More >

A network vulnerability assessment (NVA) is a proactive cybersecurity practice that focuses on identifying, evaluating, and prioritizing vulnerabilities within an organization's network infrastructure

Network Vulnerability Assessment Read More >

A network vulnerability assessment (NVA) is a proactive cybersecurity practice that focuses on identifying, evaluating, and prioritizing vulnerabilities within an organization's network infrastructure.

Next-Gen SIEM Read More >

Next-gen SIEM is the evolution of traditional SIEM in response to digital advancements like cloud computing, big data, and remote work models to extend visibility beyond traditional perimeters.

Network Security Read More >

Network security refers to the tools, technologies and processes that protect an organization's network and critical infrastructure from unauthorized use, cyberattacks, data loss and other security threats.

Non-Human Identities Read More >

Non-human identities (NHIs) are digital identities for applications, services, or devices. Organizations use these identities to execute automatic machine-to-machine operations. Organizations grant NHIs specific permissions, but they often ignore the principle of least privilege (POLP). As a result, NHIs can create security vulnerabilities.

Network Segmentation Read More >

Network segmentation is a strategy used to segregate and isolate segments in the enterprise network to reduce the attack surface.

Next-Generation Antivirus (NGAV) Read More >

Next-Generation Antivirus (NGAV) uses a combination of artificial intelligence, behavioral detection, machine learning algorithms, and exploit mitigation, so known and unknown threats can be anticipated and immediately prevented.

Next Gen SIEM for Small Business Read More >

Network Monitoring Read More >

Network monitoring is an IT process that continuously monitors and evaluates a computer network and its assets.

O

Open Source Intelligence (OSINT) Read More >

Open source intelligence (OSINT) is the act of gathering and analyzing publicly available data for intelligence purposes.

Open XDR Read More >

Open XDR is a type of extended detection and response (XDR) security solution or platform that supports third-party integrations to collect specific forms of telemetry to enable threat detection, hunting and investigation across the different data sources response actions.

Osquery Read More >

osquery uses SQL-like queries to explore operating system data using a unified interface for system security and endpo monitoring.

Open XDR vs. Native XDR Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

osquery uses SQL-like queries to explore operating system data using a unified interface for system security and endpoint device monitoring.

Open XDR vs. Native XDR Read More >

Extended detection and response (XDR) is often broken into two main categories: open XDR and native XDR. Open XDR relies on third party integrations for full coverage of telemetry, while native XDR handles all collection and response tasks from a single vendor platform.

Observability Read More >

Observability is when you infer the internal state of a system only by observing its external outputs. For modern IT infrastructure, a highly observable system exposes enough information for the operators to have a holistic picture of its health.

Observability vs. Monitoring Read More >

Monitoring tells you that something is wrong. Observability uses data collection to tell you what is wrong and why it happened.

P

Personally Identifiable Information (PII) Read More >

Personally identifiable information (PII) is important data in your enterprise, as it enables you to manage digital identities.

Pass-the-Hash Attack Read More >

Pass the hash is a type of cybersecurity attack in which an adversary steals a “hashed” user credential and uses it to create a new user session on the same network.

Principle of Least Privilege (POLP) Read More >

The principle of least privilege (POLP) is a computer security concept and practice that gives users limited access rights based on the tasks necessary to their job.

Password Storage Read More >

Cybersecurity experts strongly recommend using a password manager to safely store account information on all connected devices, including desktops, laptops, tablets and smartphones.

Passwordless Authentication Read More >

Phishing Read More >

Phishing is a type of cyberattack where threat actors masquerade as legitimate companies or individuals to steal sensitive information such as usernames, passwords, credit card numbers, and other personal details.

Privileged Access Management (PAM) Read More >

Privileged access management helps organizations manage and secure access to their most critical systems, applicatio which are typically reserved for privileged accounts.

Policy As Code (PaC) Read More >

Policy as Code is the representation of policies and regulations as code to improve and automate policy enforcement and management.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Policy As Code (PaC) Read More >

Policy as Code is the representation of policies and regulations as code to improve and automate policy enforcement and management.

Patch Management Read More >

Patch management is the process of identifying and deploying software updates, or "patches," to a variety of endpoints, including computers, mobile devices, and servers.

Public Cloud Read More >

A public cloud is a third-party IT management solution that hosts on-demand cloud computing services and physical infrastructure using the public internet.

PCI DSS Compliance Read More >

The Payment Card Industry Data Security Standard (PCI DSS) is a framework developed by the Payment Card Industry Security Standards Council (PCI SSC) to help secure and protect all payment card account data.

Penetration Testing (Pen Testing) Read More >

Penetration testing, or pen testing, is the simulation of real-world attacks in order to test an organization's detection and response capabilities.

Public Cloud vs Private Cloud Read More >

The key difference between public and private cloud computing relates to access. In a public cloud, organizations use shared cloud infrastructure, while in a private cloud, organizations use their own infrastructure.

Purple Teaming Explained Read More >

A purple team is a group of cyber security professionals who simulate malicious attacks and penetration testing in order to identify security vulnerabilities and recommend remediation strategies for an organization's IT infrastructure.

Phishing Attack Awareness Training Read More >

As cybercrime of all kinds, and phishing, in particular, reaches new heights in 2023, it's important for every person in your organization to be able to identify a phishing attack and play an active role in keeping the business and your customers safe.

PostgreSQL vs. MySQL Read More >

In this article, we will learn about the main features of PostgreSQL and MySQL, compare the two database management systems, and learn when to use PostgreSQL vs MySQL.

Platform as a Service (PaaS) Read More >

Platform as a Service (PaaS) is a cloud computing model in which a third-party cloud provider maintains an environment customers on a pay-as-you-go basis to build, develop, run and manage their own applications.

Pretexting Read More >

Pretexting is a form of social engineering in which an attacker gets access to information, a system or a service through means. The attacker will present a false scenario — or pretext — to gain the victim's trust and may pretend to be an expe investor, HR representative, IT specialist or other seemingly legitimate source.

Password Spraying Read More >

A Password spraying attack involve an attacker using a single common password against multiple accounts on the same application

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

investor, HR representative, IT specialist or other seemingly legitimate source.

Password Spraying Read More >

A Password spraying attack involve an attacker using a single common password against multiple accounts on the same application.

Polymorphic Virus Read More >

A polymorphic virus, sometimes referred to as a metamorphic virus, is a type of malware that is programmed to repeatedly mutate its appearance or signature files through new decryption routines.

Privilege Escalation Read More >

A privilege escalation attack is a cyberattack designed to gain unauthorized privileged access into a system.

Q

Questions to Ask Zero Trust Vendors Read More >

R

Ransomware Read More >

Ransomware is a type of malware that encrypts a victim's data until a payment is made to the attacker. If the payment is made, the victim receives a decryption key to restore access to their files. If the ransom payment is not made, the malicious actor publishes the data on data leak sites (DLS) or blocks access to the files in perpetuity.

Role-Based Access Control (RBAC) Read More >

Role-based access control is a mechanism where you allow users to access certain resources based on permissions defined for the roles they are assigned to.

Remote Desktop Protocol (RDP) Read More >

RDP is software that allows users to control a remote desktop as if it were local.

Remote Monitoring and Management (RMM) Read More >

Remote monitoring and management (RMM) is used by IT departments in many organizations to help oversee and administer IT systems from a remote location.

Regulatory Compliance Read More >

In this article, we'll discuss regulatory compliance, exploring the challenges that organizations commonly encounter.

Ransomware Examples Read More >

In this post, we explore 16 recent ransomware examples to outline the adversaries behind them and how they work.

Rootkit Malware Read More >

Rootkit malware is a collection of software designed to give malicious actors control of a computer, network or application.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Rootkit Malware Read More >

Rootkit malware is a collection of software designed to give malicious actors control of a computer, network or application.

Risk Based Vulnerability Management Read More >

Risk-based vulnerability management is a cybersecurity process that aims to identify and remediate vulnerabilities that pose the greatest risk to an organization.

Ransomware Prevention Read More >

The following tips are supported by what CrowdStrike has found to successfully combat and prevent ransomware.

Ransomware Protection Read More >

Businesses of all sizes are vulnerable to cyberattacks like ransomware. To protect against this increasing risk, business owners can invest in endpoint protection solutions and educate themselves about how to prevent and mitigate the impact of ransomware.

Red Teaming Read More >

Red team testing uses ethical hacking by simulating real-world techniques so your team can identify vulnerabilities in your system and practice response methods. Red teaming goes beyond a penetration test, or pen test, because it puts a team of adversaries — the red team — against an organization's security team — the blue team.

Runtime Application Self-Protection (RASP) Read More >

Runtime Application Self-Protection (RASP) is a term coined by Gartner to describe a technology that incorporates security functionality within software applications to prevent malicious attacks while the application is running.

Red Team vs Blue Team Read More >

In a red team/blue team exercise, the red team is made up of offensive security experts who try to attack an organization's cybersecurity defenses. The blue team defends against and responds to the red team attack.

Ransomware as a Service (RaaS) Explained How It Works & Examples Read More >

Ransomware as a Service (RaaS) is a business model used by ransomware developers, in which they lease ransomware variants in the same way that legitimate software developers lease SaaS products.

Ransomware Detection Read More >

Ransomware detection is the first defense against dangerous malware since it finds the infection earlier so that victims can take action to prevent irreversible damage.

Ransomware Recovery Read More >

A ransomware recovery plan is a playbook to address a ransomware attack, which includes an incident response team, communication plan, and step-by-step instructions to recover your data and address the threat.

Real User Monitoring (RUM) Read More >

Real User Monitoring (RUM) monitors application performance by capturing every user interaction on a website or mob
In this article, we'll learn about RUM and why businesses need it. We'll consider its benefits and how you can choose a RU
for your business.

Remote Code Execution (RCE): Principles and Function Read More >

Remote code execution (RCE) refers to a class of cyberattacks in which attackers remotely execute commands to place malware or

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

for your business.

Remote Code Execution (RCE): Principles and Function Read More >

Remote code execution (RCE) refers to a class of cyberattacks in which attackers remotely execute commands to place malware or other malicious code on your computer or network.

S

Security Information and Event Management (SIEM) Read More >

Security information and event management (SIEM) is a tool designed to help organizations detect, respond to, and manage security threats in real time.

Shadow API Read More >

Shadow API refers to any API deployed by developers that is not secured, registered, or monitored by an organization's IT team.

Shift Left vs. Shift Right Read More >

Learn about shift-left and shift-right approaches in detail, comparing the benefits and differences and how each approach can strengthen overall security posture.

SIEM Replacement Read More >

Explore the differences between traditional and next-gen SIEM platforms and how enterprises can upgrade legacy platforms.

Static Application Security Testing (SAST) Read More >

Static application security testing (SAST) is a key technique in proactive cybersecurity that involves automatically scanning source code for vulnerabilities before code execution.

SaaS Misconfigurations Read More >

SaaS (Software as a Service) misconfigurations refer to the incorrect or insecure configurations of SaaS applications and services.

Silver Ticket Attack Read More >

A silver ticket attack is a post-exploitation attack where an adversary forges a Kerberos service ticket (TGS) to access specific services without needing reauthentication by the domain controller.

Synthetic Identity Fraud Read More >

Synthetic identity fraud involves constructing a fabricated identity that is a mash-up of both authentic and fabricated details.

SaaS Security Posture Management (SSPM) Read More >

SaaS security posture management (SSPM) platforms help businesses address SaaS risk. SSPM provides visibility into organization's SaaS applications by continuously monitoring configurations and user activity for compliance with organi policies and industry standards.

Scareware Read More >

Scareware is a type of malware attack that claims to have detected a virus or other issue on a device and directs the user to download or buy malicious software to resolve the problem.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Scareware Read More >

Scareware is a type of malware attack that claims to have detected a virus or other issue on a device and directs the user to download or buy malicious software to resolve the problem.

Serverless Security Read More >

In serverless architectures, security responsibilities are divided between the cloud provider and the customer, according to what is known as the shared responsibility model.

Small Business Cybersecurity Checklist Read More >

Our cybersecurity checklist will help SMBs uncover any risk areas & identify opportunities for improving the security of your operations.

Shift Left Read More >

Shifting left in the context of DevSecOps means implementing testing and security into the earliest phases of the application development process. This process is known as "shift left" because it moves the security or testing component to the left (earlier) in the software development life cycle.

Semi-Structured Data Read More >

Shift Left vs. Shield Right in Kubernetes Read More >

Learn how security teams can combine shift left and shield right concepts throughout the software development lifecycle to achieve stronger Kubernetes security posture.

Software Security Read More >

Software security refers to a set of practices that developers incorporate into the software development life cycle and testing processes to ensure their digital solutions remain secure and are able to function in the event of a malicious attack.

Security as a Service (SECaaS) Read More >

Security as a service (SECaaS) is a comprehensive solution that helps an organization address any security issue without needing its own dedicated security staff.

Software as a Service (SaaS) Read More >

Software as a Service (SaaS) is a cloud-based software delivery model that allows users to access applications through an internet-connected device rather than requiring an upfront purchase and installation of physical software.

SOC-as-a-Service Read More >

SOC-as-a-Service (SOCaaS) is a security model wherein a third-party vendor operates and maintains a fully-managed SOC on a subscription basis via the cloud.

Shadow IT Read More >

Shadow IT is the unauthorized use of any digital service or device that is not formally approved of and supported by the I

Security Operations Center (SOC) Read More >

A security operations center, or SOC, is a central location where security experts monitor, detect, analyze, respond to, a security incidents.

SecOps Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

security incidents.

SecOps Read More >

SecOps is an approach that combines the processes, tools, and highly skilled staff from both security and IT departments into a single, unified team.

SOC Best Practices Read More >

Building a first-class security operations center is no simple feat – maintaining it is even harder. We discuss four security operations center best practices that every organization should strive for.

Security Data Lake Read More >

This innovation represents a pivotal development in cybersecurity, offering a centralized repository capable of efficiently storing, managing, and analyzing diverse security data, thereby addressing the critical challenges posed by the data deluge.

SOC Automation Read More >

Automation significantly boosts the efficiency of SOCs by streamlining processes and handling repetitive, manual tasks. Automation not only accelerates threat detection and mitigation but allows SOC teams to focus on more strategic tasks.

SOC Reports Read More >

A SOC framework acts like a blueprint, defining the systematic approach a SOC ought to employ as it detects, analyzes, and responds to cybersecurity threats.

SOC Frameworks Read More >

SOC reports distill complex security data into actionable intelligence, keeping you ahead of threats.

Security Orchestration, Automation and Response (SOAR) Read More >

Security orchestration, automation and response (SOAR) is a collection of software programs developed to bolster an organization's cybersecurity posture. A SOAR platform enables a security analyst team to monitor security data from a variety of sources, including security information and management systems and threat intelligence platforms.

Software Composition Analysis (SCA) Read More >

Software composition analysis (SCA) is a technique used for examining the software components that make up an application and then identifying and managing any vulnerabilities discovered.

Security as Code (SaC) Read More >

Security as code (SaC) is the integration of automated security measures directly into the software development process, making it an integral part of the software development life cycle (SDLC). SaC introduces proactive rather than reactive security measures, an essential approach given the increasing sophistication of modern cyber threats.

Spear-Phishing Read More >

Spear-phishing is a targeted attack that uses fraudulent emails, texts and phone calls in order to steal a specific person's information.

Supply Chain Attack Read More >

A supply chain attack is a type of cyberattack that targets a trusted third party vendor who offers services or software vital to the supply chain.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Supply Chain Attack Read More >

A supply chain attack is a type of cyberattack that targets a trusted third party vendor who offers services or software vital to the supply chain.

Security Posture Read More >

An organization's security posture is a holistic snapshot of their security strengths and vulnerabilities across hardware, software, data, and user behavior.

Software Development Lifecycle (SDLC) Read More >

The software development life cycle (SDLC) outlines the stages involved in building software applications, from inception to retirement.

Serverless Architecture Read More >

Serverless architecture is a software development approach in which developers can run applications without managing the underlying infrastructure. In the serverless computing model, the cloud provider handles all infrastructure setup, maintenance, and scaling.

SBOM (Software Bill of Materials) Read More >

In this post, we will cover the key parts of an SBOM, the benefits and challenges for an organization adopting SBOMs, and how an organization might integrate the usage of SBOMs within its current suite of security tools.

Serverless Security Best Practices Read More >

Serverless computing involves the dynamic, on-demand allocation and provisioning of application infrastructure, such as computing power or storage resources.

Social Engineering Read More >

Social engineering is an umbrella term that describes a variety of cyberattacks that use psychological tactics to manipulate people into taking a desired action, like giving up confidential information.

SEO Poisoning Read More >

SEO poisoning is a technique used by threat actors to increase the prominence of their malicious websites, making them look more authentic to consumers.

Snort and Snort Rules Explained Read More >

Snort is an open-source network intrusion detection and prevention system (IDS/IPS) that monitors network traffic and identifies potentially malicious activities on Internet Protocol (IP) networks.

Spoofing vs. Phishing Read More >

Spoofing attacks resemble identity theft while phishing attacks attempt to steal sensitive information.

Security Automation Read More >

Security automation is the practice of using technology to perform recurring IT security tasks, such as endpoint scannin response, with limited human intervention.

SIEM vs Log Management Read More >

Understand the difference in capabilities, definitions, and costs between a SIEM and a log management solutions (LMS).

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

SIEM vs Log Management Read More >

Understand the difference in capabilities, definitions, and costs between a SIEM and a log management solutions (LMS).

Smishing Read More >

Smishing is the act of sending fraudulent text messages designed to trick individuals into sharing sensitive data such as passwords, usernames and credit card numbers.

Structured, Unstructured and Semi Structured Logging Explained Read More >

Structured, semi structured and unstructured logging falls on a large spectrum each with its own set of benefits and challenges. Unstructured and semi structured logs are easy to read by humans but can be tough for machines to extract while structured logs are easy to parse in your log management system but difficult to use without a log management tool.

Server Monitoring Read More >

Server monitoring provides visibility into network connectivity, available capacity and performance, system health, and much more.

Security Misconfiguration Read More >

Security misconfiguration is any error or vulnerability present in the configuration of code that allows attackers access to sensitive data. There are many types of security misconfiguration, but most present the same danger: vulnerability to data breach and attackers gaining unauthorized access to data.

Security Testing Read More >

Security testing is a type of software testing that identifies potential security risks and vulnerabilities in applications, systems and networks.

Shared Responsibility Model Read More >

The Shared Responsibility Model dictates that a cloud provider must monitor and respond to security threats related to the cloud itself and its underlying infrastructure and end users are responsible for protecting data and other assets they store in any cloud environment.

SQL Injection (SQLi) Read More >

SQL injection (SQLi) is a cyberattack that injects malicious SQL code into an application, allowing the attacker to view or modify a database. Injection attacks, which include SQL injections, were the third most serious web application security risk in 2021.

Spyware Read More >

Spyware is a type of unwanted, malicious software that infects a computer or other device and collects information about a user's web activity without their knowledge or consent.

Spoofing Attack Read More >

Spoofing is when a cybercriminal disguises communication or activity from a malicious source and presents it as a famili
source.

SOA vs Microservices Read More >

As development teams require more flexibility, scalability and speed, traditional monolithic software development mode
become largely obsolete. To meet the needs of the modern landscape, two options have emerged for effectively and efficiently
building and running large-scale, complex applications: service oriented architecture (SOA) and microservices.

Spear Phishing vs. Phishing Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

become largely obsolete. To meet the needs of the modern landscape, two options have emerged for effectively and efficiently building and running large-scale, complex applications: service oriented architecture (SOA) and microservices.

Spear Phishing vs. Phishing Read More >

Spear phishing is a targeted attack on a specific person or organization, whereas general phishing campaigns are sent to a large volume of people.

T

Tailgating and Piggybacking Attacks Read More >

Digital tailgating attacks involve attackers exploiting authorized user access to infiltrate network or computer systems.

Threat Actor Read More >

A threat actor, also known as a malicious actor, is any person or organization that intentionally causes harm in the digital sphere.

Threat Intelligence Read More >

Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors.

Threat Detection and Response (TDR) Read More >

Threat detection and response (TDR) refers to cybersecurity tools that identify threats by analyzing user behaviors.

Types of Ransomware Read More >

The most common types of ransomware are cryptoware, locker ransomware, scareware, leakware, and ransomware-as-a-service.

The Dark Web Read More >

The dark web is the part of the internet where users can access unindexed web content anonymously through special web browsers like TOR.

Threat Detection, Investigation, and Response (TDIR) Read More >

Threat detection, investigation, and response (TDIR) is a cybersecurity process for finding, analyzing, and mitigating threats.

Threat Intelligence Platforms Read More >

A Threat Intelligence Platform automates the collection, aggregation, and reconciliation of external threat data, providing security teams with most recent threat insights to reduce threat risks relevant for their organization.

Tips and Tools to Scale Your Cybersecurity Program Read More >

Get the 9 essential tips and tools that'll help your organization scale its cybersecurity program.

Tabletop Exercise Read More >

Tabletop exercises are a form of cyber defense training in which teams walk through simulated cyberattack scenarios in discussion-based setting.

Types of Cyberattacks Read More >

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Tabletop exercises are a form of cyber defense training in which teams walk through simulated cyberattack scenarios in a structured, discussion-based setting.

Types of Cyberattacks Read More >

Cyberattacks can target a wide range of victims from individual users to enterprises or even governments. When targeting businesses or other organizations, the hacker's goal is usually to access sensitive and valuable company resources, such as intellectual property (IP), customer data or payment details.

The Role of AI in Cybersecurity Read More >

Learn how cybersecurity tools integrate AI, the primary applications of AI, and the benefits of tools that integrate AI.

Types of Social Engineering Attacks Read More >

Explore ten of the most common types of social engineering attacks and how to prevent them.

Three Pillars of Observability Read More >

The three pillars of observability are logs, metrics, and traces. These three data outputs provide different insights into the health and functions of systems in cloud and microservices environments.

TrickBot Malware Read More >

TrickBot malware is a banking Trojan released in 2016 that has since evolved into a modular, multi-phase malware capable of a wide variety of illicit operations.

Threat Intelligence Feed Read More >

A threat intelligence feed is a real-time, continuous data stream that gathers information related to cyber risks or threats.

Types of Malware Read More >

While there are many different variations of malware, there are several types that you are more likely to encounter.

Threat Model Read More >

A threat model evaluates threats and risks to information systems, identifies the likelihood that each threat will succeed and assesses the organization's ability to respond to each identified threat.

Trojan Horse Read More >

A Trojan Horse (Trojan) is a type of malware that disguises itself as legitimate code. Attackers can export files, modify data, and delete files on your device.

U

UEBA vs SIEM Read More >

Compare UEBA and SIEM solutions, unpacking the roles they play in cybersecurity and how they complement one anot

Unified Identity Protection Read More >

Unified identity protection integrates identity management capabilities with real-time threat detection, risk-based authentication, and continuous monitoring across identity, endpoint, and cloud environments.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Unified identity protection integrates identity management capabilities with real-time threat detection, risk-based authentication, and continuous monitoring across identity, endpoint, and cloud environments.

Unified Security Posture Management (USPM) Read More >

USPM is a solution that centralizes security data, providing visibility into both multi-cloud and hybrid environments.

User Authentication Read More >

User authentication is the critical checkpoint that verifies users' identities to protect sensitive data from unauthorized access.

User and Entity Behavior Analytics (UEBA) Read More >

User and entity behavior analytics (UEBA) systems monitor an organization's network, using AI and machine learning (ML) to analyze suspicious activity related to user and endpoint behavior that could indicate a security threat.

V

Virtual Machines (VMs) Read More >

A virtual machine (VM) is a software emulation that splits a single physical computing device into many isolated computing environments to maximize resource optimization and provide independence and isolation for each environment.

Vulnerability Assessment Read More >

Vulnerability assessment is the ongoing, regular process of defining, identifying, classifying and reporting cyber vulnerabilities across endpoints, workloads, and systems.

Vishing Read More >

Vishing, a voice phishing attack, is the fraudulent use of phone calls and voice messages pretending to be from a reputable organization to convince individuals to reveal private information such as bank details and passwords.

Vulnerability Management Read More >

Vulnerability management is the ongoing, regular process of identifying, assessing, reporting on, managing and remediating security risks to keep all systems and assets in a network protected.

Virtualization vs. Containerization Read More >

Learn the differences between containers and virtual machines (VMs), compare and contrast them, and review some use cases showing where one or the other is preferable

Virtual Private Cloud (VPC) Read More >

A VPC is a single compartment within the entirety of the public cloud of a certain provider, essentially a deposit box insid
vault.

Vulnerability Management Lifecycle Read More >

There are five main stages in the vulnerability management lifecycle include: Assess, Prioritize, Act, Reassess, Improve.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

There are five main stages in the vulnerability management lifecycle include: Assess, Prioritize, Act, Reassess, Improve.

W

Workflow Automation Read More >

Workflow automation uses software to execute tasks and processes without human interaction.

What is Synthetic Monitoring? Read More >

Synthetic monitoring is a technique within an application performance monitoring (APM) strategy that simulates user interactions and navigation paths to evaluate the functionality, availability, and performance of applications according to different factors, such as geographic locations or device types.

What is Secure Access Service Edge (SASE)? Read More >

Secure access service edge (SASE) is a cybersecurity and networking framework that enables the integration of networking security functions and wide-area network (WAN) capabilities when architecting networks.

Windows New Technology LAN Manager (NTLM) Read More >

Windows New Technology LAN Manager (NTLM) is a suite of security protocols offered by Microsoft to authenticate users' identity and protect the integrity and confidentiality of their activity.

Web Application Firewall (WAF) Read More >

A Web Application Firewall (WAF) is a security device designed to protect organizations at the application level by filtering, monitoring and analyzing HTTP and HTTPS traffic between the web application and the internet.

Wiper Attacks Read More >

Wiper attacks are malware-based attacks designed to permanently delete or corrupt data on targeted systems.

Whaling Attack Read More >

A whaling attack is a social engineering attack against a specific executive or senior employee with the purpose of stealing money or information, or gaining access to the person's computer in order to execute further attacks.

Web Server Logs Read More >

A web server log is a text document that contains a record of all activity related to a specific web server over a defined period of time.

What Ransomware Allows Hackers to Do Read More >

In a ransomware attack, hackers use malware to encrypt, delete or manipulate data, intellectual property or personal information. This allows attackers to hold the information, device or system digitally hostage until the victim meets the cybercriminal's ransom demands, which usually involve secure, untraceable payment.

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

X

XDR vs SIEM vs SOAR Read More >

XDR, SIEM, and SOAR address similar use cases but take fundamentally different approaches. Learn how they relate and how they

X

XDR vs SIEM vs SOAR Read More >

XDR, SIEM, and SOAR address similar use cases but take fundamentally different approaches. Learn how they relate and how they differ.

Z

Zero Trust Security Read More >

Zero Trust is a security framework that mandates stringent identity verification for every user and device attempting to access resources, regardless of whether they are inside or outside the organization's network.

Zero-Day Exploit Read More >

A Zero-Day Exploit is the technique or attack a malicious actor deploys to leverage an unknown security vulnerability to gain access into a system.

Zero Trust Architecture Read More >

A Zero Trust Architecture refers to the way network devices and services are structured to enable a Zero Trust security model.

Zero Trust vs. SASE Read More >

We will take a closer look at Zero Trust and SASE and answer some common questions that organizations have when incorporating these into their overarching cybersecurity framework.

Zero Trust Network Access (ZTNA) Read More >

Zero Trust network access (ZTNA) is an IT technology solution that requires all users to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

Zeus Trojan Malware Read More >

The two primary goals of the Zeus trojan horse virus are stealing people's financial information and adding machines to a botnet.

Try CrowdStrike free for 15 days

Start free trial → Contact us → View pricing

Welcome to CrowdStrike

What are you looking for today?

CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Zero Trust network access (ZTNA) is an IT technology solution that requires all users to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

Zeus Trojan Malware Read More >

The two primary goals of the Zeus trojan horse virus are stealing people's financial information and adding machines to a botnet.

Try CrowdStrike free for 15 days

Start free trial → Contact us → View pricing

CROWDSTRIKE

Get Started
Pricing Sale
Free Trial Guide
Falcon Flex
Financing
CrowdStrike Marketplace
Cyber Monday Deals

Company
About Us
Executive Leadership
Board of Directors
Newsroom
Investor Relations
CrowdStrike Racing & F1
Sustainability

Partners
Partner Programs
Service Providers
Strategic Technology
Channel & Distributors
Become a Partner

Existing Customers
Support Portal
Developer Portal

Support
Call 1-888-512-8906 (US)
Experienced a Breach?
Contact Us
Schedule a Meeting
FAQs

Welcome to CrowdStrike
What are you looking for today?
CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: Privacy Notice.

Copyright © 2025 Privacy Cookies Your Privacy Choices Terms of Use Accessibility English (US