We keep the record straight by preserving government websites, news articles, historical data, and more. If you find our archive useful, please CHIP IN

INTERNET ARCHIVE WayBackMachine http://www.crowdstrike.com/falcon-host/index.html Go OCT NOV JAN 27 2012 2013 2014 About this capture
25 captures
21 Sep 2013 - 7 Dec 2022

Next-Generation Threat Protection

Host-based Detection Sensor

CrowdStrike Falcon Host is the cloud-managed threat protection application running on the CrowdStrike Falcon Platform. Falcon Host is comprised of two core components, the cloud-based application and the on-premise host-based sensor. Falcon Host leverages a lightweight host-based sensor that shadows, captures, and correlates low-level operating system events to instantly identify the adversary tradecraft and activity through our patent-pending Execution Profiling technology. As opposed to focusing on malware signatures, indicators of compromise, exploits, and vulnerabilities, Falcon Host instead identifies mission objectives of the adversary leveraging the Kill Chain model and provides real-time detection by focusing on what the attacker is doing, as opposed to looking for a specific, easily changeable indicator used in an attack.

Without performing intrusive and performance-impacting scans of the system, Falcon Host's highly efficient real-time monitoring of all system activity is the only security solution that provides maximum visibility into all adversary activities, including Adversary-in-Motion: reconnaissance, exploitation, privilege escalation, lateral movement, and exfiltration. In addition to real-time detection, Falcon Host provides retrospective insight into past attack and other execution activity with real-time forensics provided by Endpoint Activity Monitoring technology. The intersection of permanently recorded adversary attack information, which is available for future recall and continuous in-the-cloud retrospective analysis, and next-generation targeted attack identification and attribution is a unique capability not offered by any other security technology.

Endpoint Activity Monitoring, Threat Detection & Response

CrowdStrike Falcon Host solves the main business problems that enterprises face today, to include visibility into targeted threats, detection of zero-day attacks, lack of time to hunt through enterprise activity, and insufficient resources to provide flexible responses.

CrowdStrike Falcon Host addresses these problems by leveraging a redundant, highly scalable, secure cloud architecture that correlates intelligence and security events in real-time. Storing a vast amount of event data in a scalable elastic cloud allows enterprises to pinpoint targeted attacks in real-time. CrowdStrike Falcon Host's Endpoint Activity Monitoring (EAM) saves time and money while reducing risk by avoiding "silent failure". EAM offers real-time forensics by tracking all execution on all hosts at all times, shortening the window between infection and detection while providing users with live forensics.

Answers the following questions with Enterprise Activity Monitoring:

- What suspect programs have been executed?
- What processes have run across my systems with different file names?
- Which programs are listening for network connections?
- Which machines and users were affected?
- Who did this and how long have then been here?
- What were they after?
- What programs attempt to maintain persistence?

CrowdStrike Falcon Host's Threat Detection leverages Execution Profiling to

CrowdStrike Falcon Platform

Request a Technical Demo

About CrowdStrike Technology

Dmitri Alperovitch, Co-Founder & CTO, talks technology

GoSecure, Inc.
Exhibit 2016
CrowdStrike v. GoSecure
IPR2025-00068

We keep the record straight by preserving government websites, news articles, historical data, and more. If you find our archive useful, please CHIP IN

INTERNET ARCHIVE WayBackMachine http://www.crowdstrike.com/falcon-host/index.html Go OCT NOV JAN 27 2012 2013 2014 About this capture
25 captures
21 Sep 2013 - 7 Dec 2022

CrowdStrike Falcon Host addresses these problems by leveraging a redundant, highly scalable, secure cloud architecture that correlates intelligence and security events in real-time. Storing a vast amount of event data in a scalable elastic cloud allows enterprises to pinpoint targeted attacks in real-time. CrowdStrike Falcon Host's Endpoint Activity Monitoring (EAM) saves time and money while reducing risk by avoiding "silent failure". EAM offers real-time forensics by tracking all execution on all hosts at all times, shortening the window between infection and detection while providing users with live forensics.

Answers the following questions with Enterprise Activity Monitoring:

- What suspect programs have been executed?
- What processes have run across my systems with different file names?
- Which programs are listening for network connections?
- Which machines and users were affected?
- Who did this and how long have then been here?
- What were they after?
- What programs attempt to maintain persistence?

CrowdStrike Falcon Host's Threat Detection leverages Execution Profiling to constantly search for a match between activities on your machines and a massive catalog of adversary behaviors. With enhanced visibility of each system, CrowdStrike Falcon is able to focus on the Tactics, Techniques, and Procedures (TTPs) – the malicious behaviors themselves – rather than a specific exploit or piece of malware. An adversary doesn't have to use malware, so long as they exhibit a behavior we recognize as malicious based on our extensive intelligence and understanding of attacker tradecraft. CrowdStrike Falcon Host detects browser exploits, Java, Adobe Acrobat, and Microsoft Office documents (Outlook, Word, Excel, and Powerpoint).

Falcon Host Key Features

- Host-based kernel mode sensor with Activity Flight Recorder (AFR) technology
- Detect adversary activity through Execution Profiling
- Provide real-time damage assessment and detect Adversaries-in-Motion
- Global network of event driven sensors
- Attribution of attacks by targeted adversaries

CrowdStrike Falcon Host supports Microsoft Windows and Mac workstations and servers.

COPYRIGHT © 2013 CROWDSTRIKE INC. ALL RIGHTS RESERVED | PRIVACY