

EXHIBIT 10

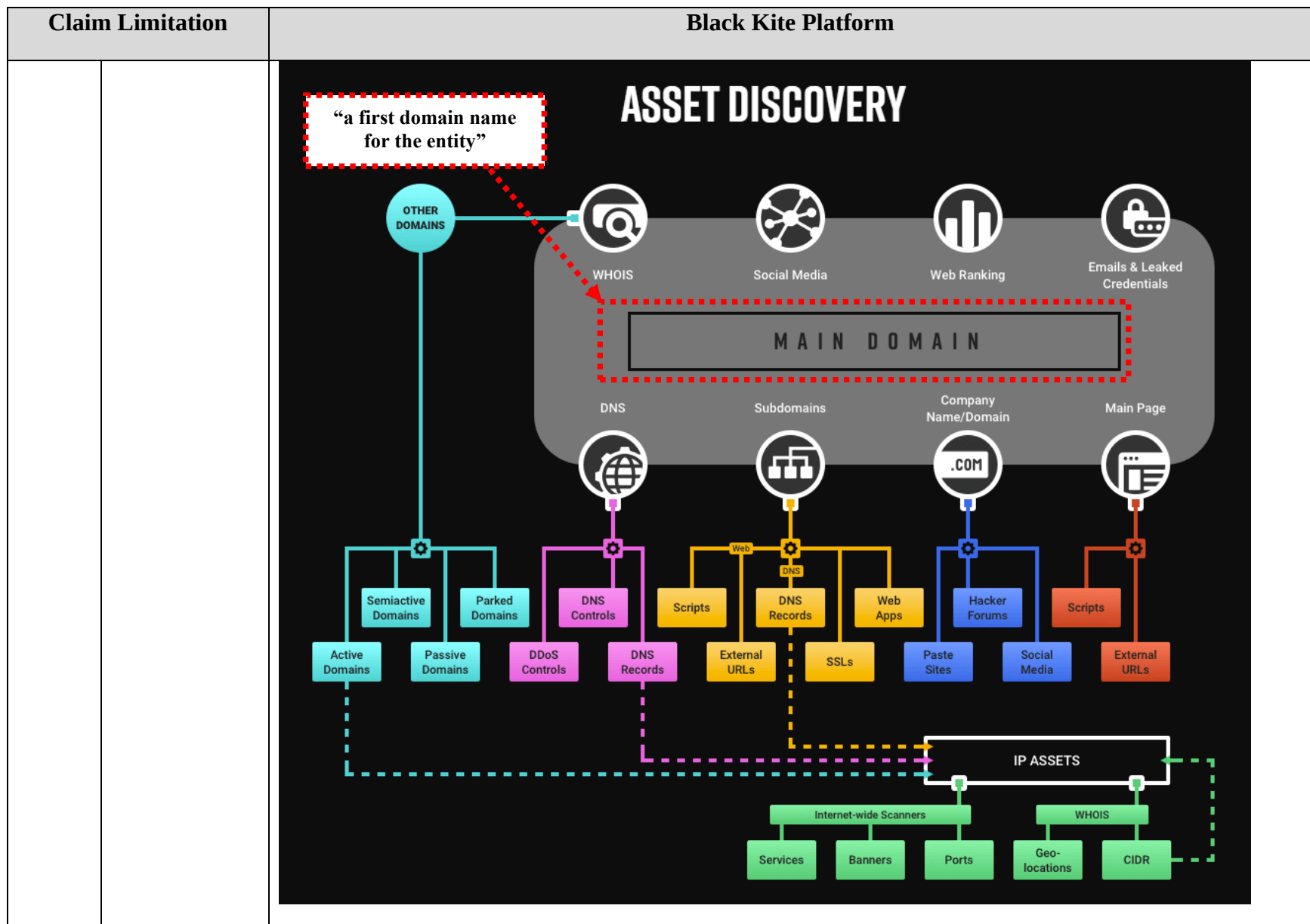
Exhibit 10: U.S. Patent No. 11,652,834 (“834 Patent”)

Claim Limitation		Black Kite Platform
1[pre]	A computer-implemented method for mapping Internet Protocol (IP) addresses to an entity, the method comprising:	To the extent the preamble is limiting, the Black Kite Platform includes a computer-implemented method for mapping Internet Protocol (IP) addresses to an entity, as discussed below.
1[a]	receiving a first domain name for the entity;	The Black Kite Platform receives a first domain name from the entity: “The platform fills a fundamental security gap by making it easy for businesses to non-invasively quantify and monitor cyber risk across thousands of third parties, suppliers, and partners.” https://blackkite.com/blog/cyber-risk-ratings-leader-normshield-rebrands-to-black-kite/ (accessed December 8, 2023).

Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation	Black Kite Platform
	What is our Methodology? Cyber Threat Susceptibility Assessment (CTSA) is a methodology for evaluating the susceptibility of a system to cyberattacks developed by MITRE. CTSA quantitatively assesses a system's inability to resist a cyberattack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). To generate the cyber risk rating, Black Kite only needs the company domain. The engine collects information from VirusTotal, Passive DNS servers, web search engines, and other Internet-wide scanners, as well as Black Kite's proprietary databases, which hold more than 10 billion historic items. The engine searches the databases to find all IP address ranges and domain names that belong to the company. Black Kite uses what is called Open Source Intelligence (OSINT) to gather information. The following map shows how hackers can leverage their attack vectors by using OSINT resources like hacker forums, social networks, Google, leaked database dumps, paste sites, or even legitimate security services like VirusTotal, Censys, Cymon, Shodan, or Google Safe Browsing. Black Kite compiles this data into a simple, understandable report with letter-grade scores to help identify and mitigate potential security risks. The platform identifies the risks (CVE/CWE), the risk score of the corresponding vulnerabilities/weaknesses (CVSS/CWSS) and attack patterns (CAPEC/FIPS-199 impact level). Black Kite also classifies the findings into FISMA Cyber Security Framework Area and Maturity Level, NIST 800-53 Control Family, FIPS-200 Area, and NIST 800-37 Process Step. Black Kite does all of this without scanning or modifying any of the organization's business assets. https://blackkite.com/platform/ (accessed December 8, 2023).

Exhibit 10: U.S. Patent No. 11,652,834

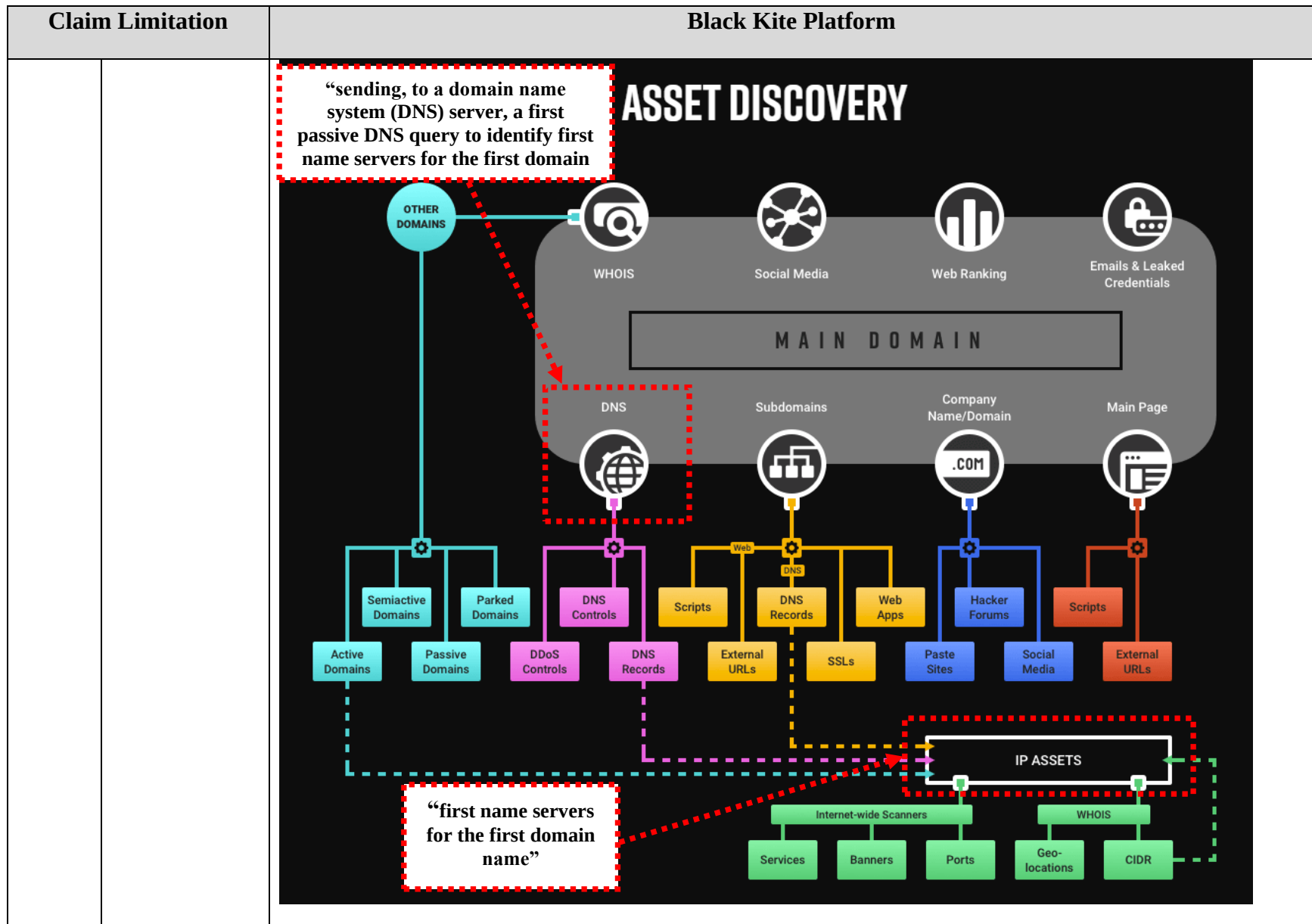


Black Kite Ex. 1027, Page 5 of 28

Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation		Black Kite Platform													
	for the first domain name;	TECHNICAL DEPTH <table><thead><tr><th></th><th>BITSIGHT</th><th>SECURITYSCORECARD</th><th>RISKRECON</th><th>BLACK KITE</th></tr></thead><tbody><tr><td>Passive DNS</td><td>✓✓✓</td><td>✓✓✓</td><td>✓✓✓</td><td>✓✓✓</td></tr></tbody></table>					BITSIGHT	SECURITYSCORECARD	RISKRECON	BLACK KITE	Passive DNS	✓✓✓	✓✓✓	✓✓✓	✓✓✓
			BITSIGHT	SECURITYSCORECARD	RISKRECON	BLACK KITE									
		Passive DNS	✓✓✓	✓✓✓	✓✓✓	✓✓✓									
		https://blackkite.com/platform (accessed December 8, 2023).													
What is our Methodology? Cyber Threat Susceptibility Assessment (CTSA) is a methodology for evaluating the susceptibility of a system to cyberattacks developed by MITRE. CTSA quantitatively assesses a system’s inability to resist a cyberattack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). To generate the cyber risk rating, Black Kite only needs the company domain. The engine collects information from VirusTotal, Passive DNS servers, web search engines, and other Internet-wide scanners, as well as Black Kite’s proprietary databases, which hold more than 10 billion historic items. The engine searches the databases to find all IP address ranges and domain names that belong to the company. Black Kite uses what is called Open Source Intelligence (OSINT) to gather information. The following map shows how hackers can leverage their attack vectors by using OSINT resources like hacker forums, social networks, Google, leaked database dumps, paste sites, or even legitimate security services like VirusTotal, Censys, Cymon, Shodan, or Google Safe Browsing. Black Kite compiles this data into a simple, understandable report with letter-grade scores to help identify and mitigate potential security risks. The platform identifies the risks (CVE/CWE), the risk score of the corresponding vulnerabilities/weaknesses (CVSS/CWSS) and attack patterns (CAPEC/FIPS-199 impact level). Black Kite also classifies the findings into FISMA Cyber Security Framework Area and Maturity Level, NIST 800-53 Control Family, FIPS-200 Area, and NIST 800-37 Process Step. Black Kite does all of this without scanning or modifying any of the organization's business assets.															
https://blackkite.com/platform/ (accessed December 8, 2023).															

Exhibit 10: U.S. Patent No. 11,652,834



<https://blackkite.com/black-kites-methodology/> (accessed December 8, 2023) (annotated).

The Black Kite Platform receives, from the DNS server, a list of the first name servers for the first domain name:

Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation	Black Kite Platform
	What is our Methodology? Cyber Threat Susceptibility Assessment (CTSA) is a methodology for evaluating the susceptibility of a system to cyberattacks developed by MITRE. CTSA quantitatively assesses a system's inability to resist a cyberattack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). To generate the cyber risk rating, Black Kite only needs the company domain. The engine collects information from VirusTotal, Passive DNS servers, web search engines, and other Internet-wide scanners, as well as Black Kite's proprietary databases, which hold more than 10 billion historic items. The engine searches the databases to find all IP address ranges and domain names that belong to the company. Black Kite uses what is called Open Source Intelligence (OSINT) to gather information. The following map shows how hackers can leverage their attack vectors by using OSINT resources like hacker forums, social networks, Google, leaked database dumps, paste sites, or even legitimate security services like VirusTotal, Censys, Cymon, Shodan, or Google Safe Browsing. Black Kite compiles this data into a simple, understandable report with letter-grade scores to help identify and mitigate potential security risks. The platform identifies the risks (CVE/CWE), the risk score of the corresponding vulnerabilities/weaknesses (CVSS/CWSS) and attack patterns (CAPEC/FIPS-199 impact level). Black Kite also classifies the findings into FISMA Cyber Security Framework Area and Maturity Level, NIST 800-53 Control Family, FIPS-200 Area, and NIST 800-37 Process Step. Black Kite does all of this without scanning or modifying any of the organization's business assets. https://blackkite.com/platform/ (accessed December 8, 2023).

Exhibit 10: U.S. Patent No. 11,652,834

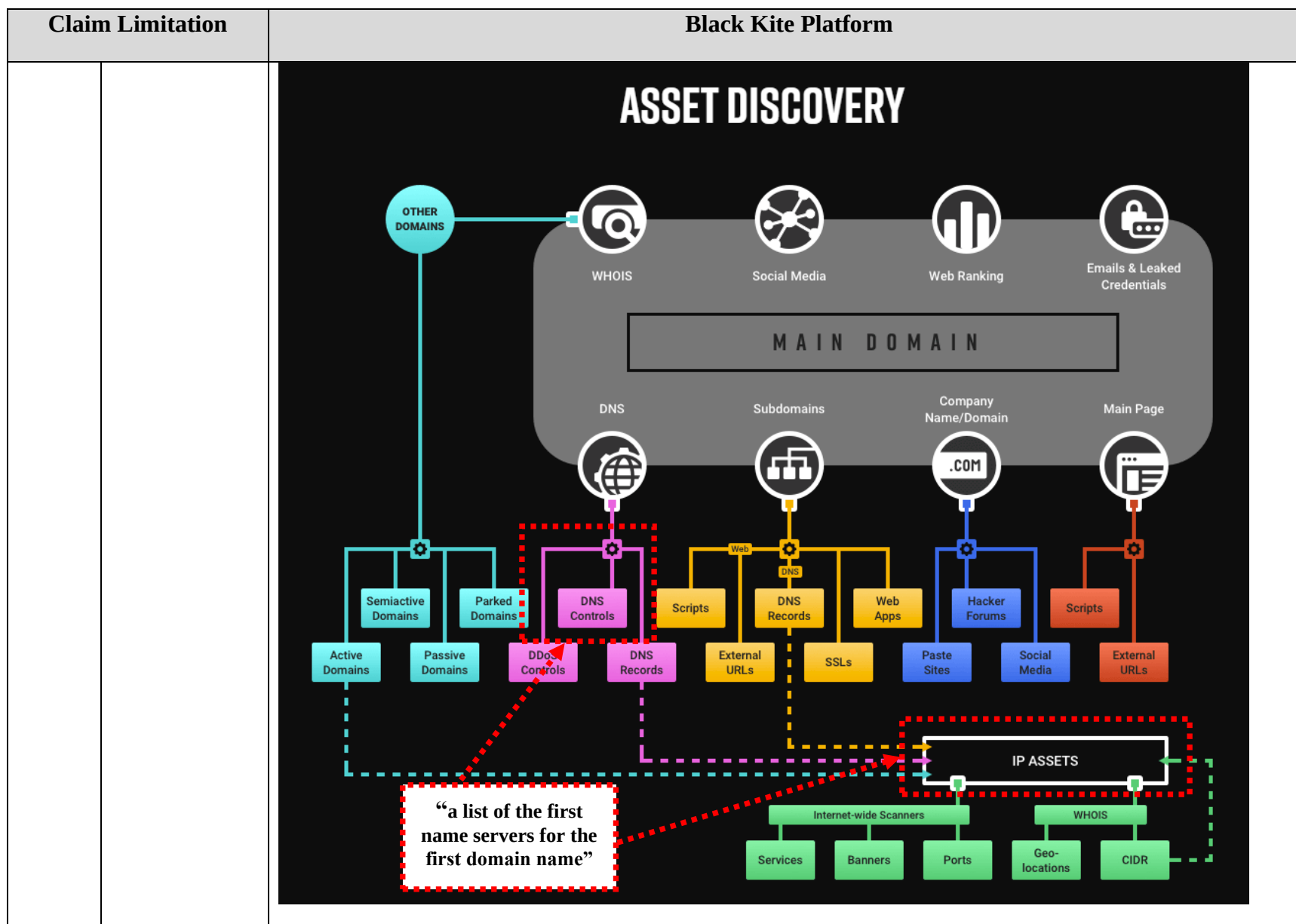


Exhibit 10: U.S. Patent No. 11,652,834

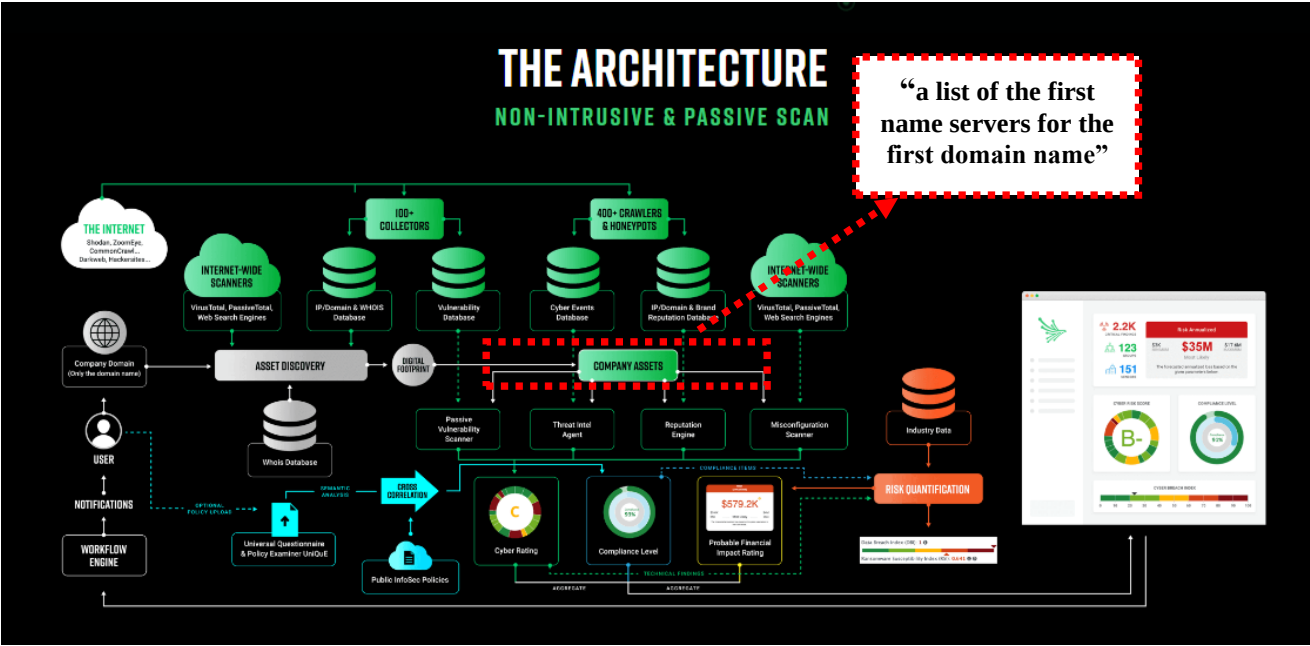
Claim Limitation	Black Kite Platform
	https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).  https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).
1[d] sending, for each of the first name servers, a second passive DNS query to identify second domain names	The Black Kite Platform sends, for each of the first name servers, a second passive DNS query to identify second domain names for which the first name server is authoritative:

Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation	Black Kite Platform
for which the first name server is authoritative;	What is our Methodology? Cyber Threat Susceptibility Assessment (CTSA) is a methodology for evaluating the susceptibility of a system to cyberattacks developed by MITRE. CTSA quantitatively assesses a system's inability to resist a cyberattack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). To generate the cyber risk rating, Black Kite only needs the company domain. The engine collects information from VirusTotal, Passive DNS servers, web search engines, and other Internet-wide scanners, as well as Black Kite's proprietary databases, which hold more than 10 billion historic items. The engine searches the databases to find all IP address ranges and domain names that belong to the company. Black Kite uses what is called Open Source Intelligence (OSINT) to gather information. The following map shows how hackers can leverage their attack vectors by using OSINT resources like hacker forums, social networks, Google, leaked database dumps, paste sites, or even legitimate security services like VirusTotal, Censys, Cymon, Shodan, or Google Safe Browsing. Black Kite compiles this data into a simple, understandable report with letter-grade scores to help identify and mitigate potential security risks. The platform identifies the risks (CVE/CWE), the risk score of the corresponding vulnerabilities/weaknesses (CVSS/CWSS) and attack patterns (CAPEC/FIPS-199 impact level). Black Kite also classifies the findings into FISMA Cyber Security Framework Area and Maturity Level, NIST 800-53 Control Family, FIPS-200 Area, and NIST 800-37 Process Step. Black Kite does all of this without scanning or modifying any of the organization's business assets. https://blackkite.com/platform/ (accessed December 8, 2023).

Exhibit 10: U.S. Patent No. 11,652,834

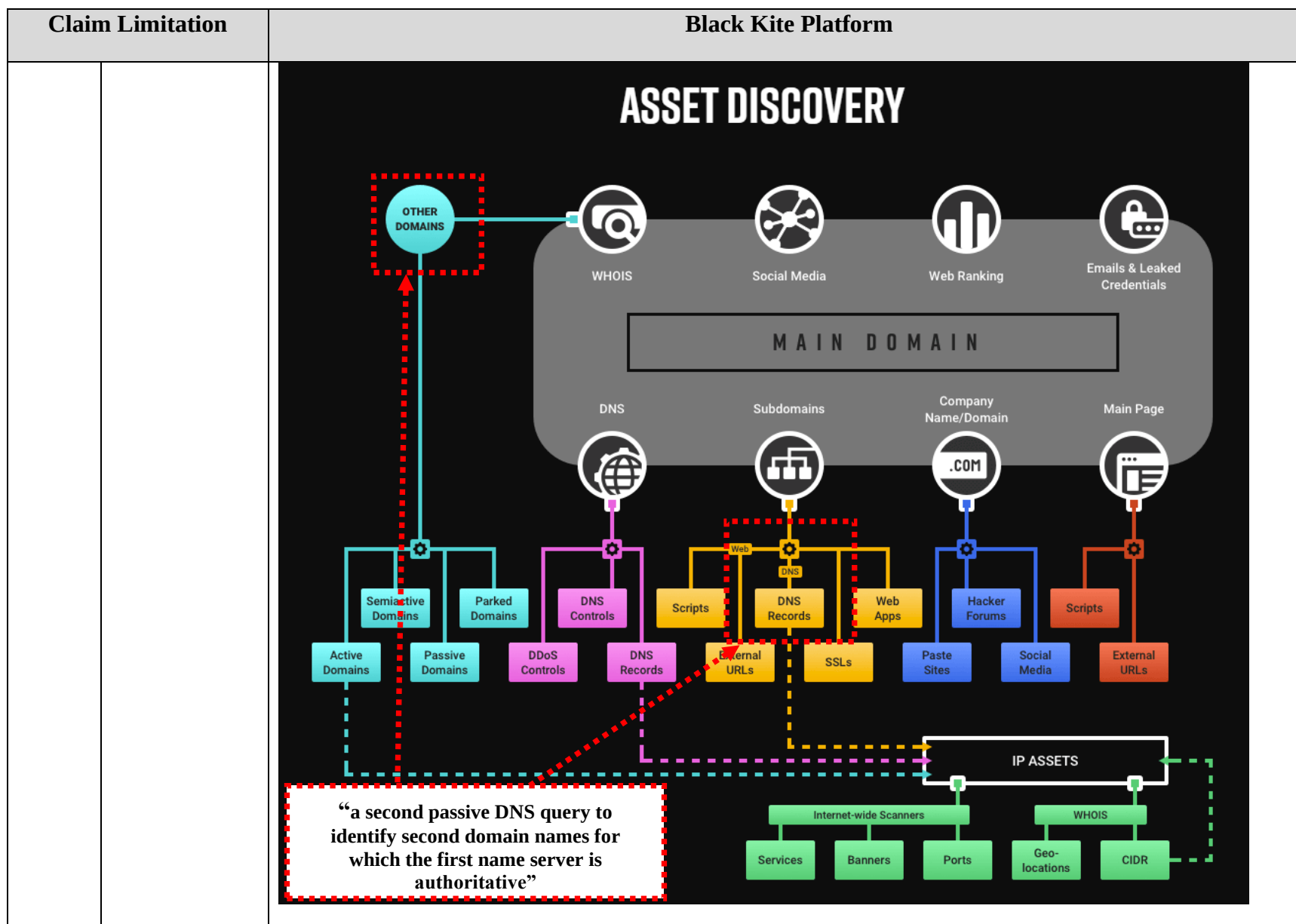


Exhibit 10: U.S. Patent No. 11,652,834

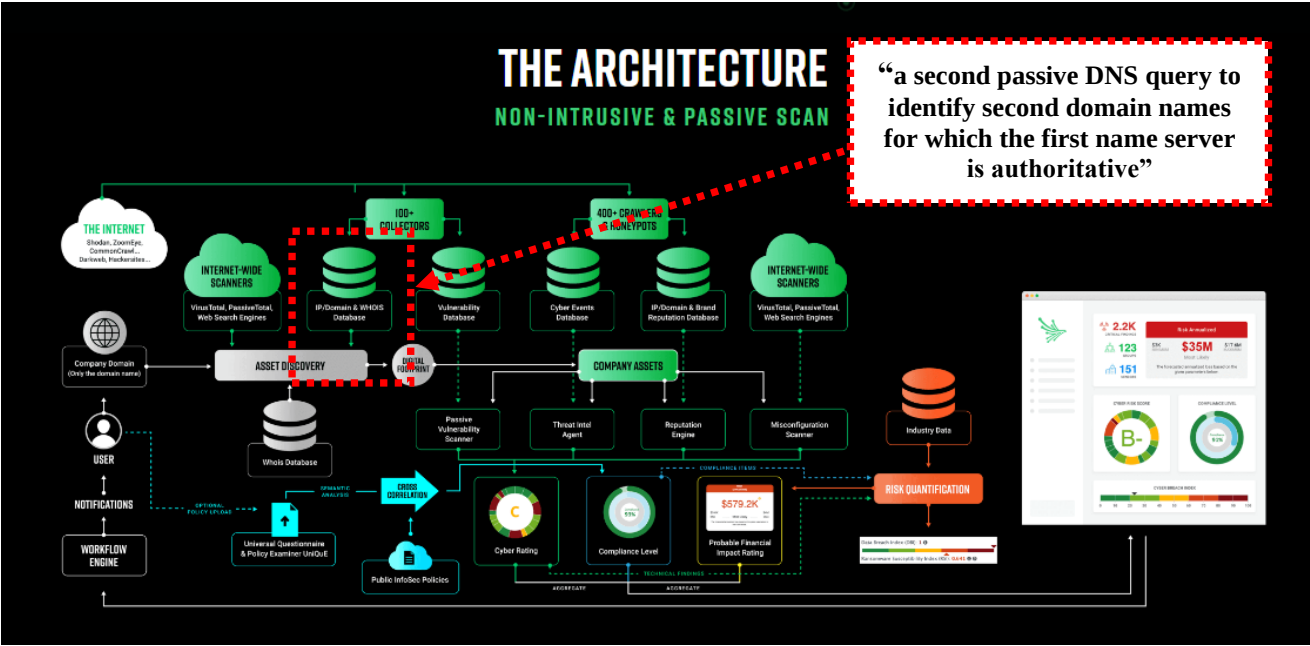
Claim Limitation	Black Kite Platform
	https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).  https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).
1[e] receiving, for each of the first name servers, a list of the second domain names for which the first name	The Black Kite Platform receives, for each of the first name servers, a list of the second domain names for which the first name server is authoritative:

Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation	Black Kite Platform
server is authoritative;	What is our Methodology? Cyber Threat Susceptibility Assessment (CTSA) is a methodology for evaluating the susceptibility of a system to cyberattacks developed by MITRE. CTSA quantitatively assesses a system's inability to resist a cyberattack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). To generate the cyber risk rating, Black Kite only needs the company domain. The engine collects information from VirusTotal, Passive DNS servers, web search engines, and other Internet-wide scanners, as well as Black Kite's proprietary databases, which hold more than 10 billion historic items. The engine searches the databases to find all IP address ranges and domain names that belong to the company. Black Kite uses what is called Open Source Intelligence (OSINT) to gather information. The following map shows how hackers can leverage their attack vectors by using OSINT resources like hacker forums, social networks, Google, leaked database dumps, paste sites, or even legitimate security services like VirusTotal, Censys, Cymon, Shodan, or Google Safe Browsing. Black Kite compiles this data into a simple, understandable report with letter-grade scores to help identify and mitigate potential security risks. The platform identifies the risks (CVE/CWE), the risk score of the corresponding vulnerabilities/weaknesses (CVSS/CWSS) and attack patterns (CAPEC/FIPS-199 impact level). Black Kite also classifies the findings into FISMA Cyber Security Framework Area and Maturity Level, NIST 800-53 Control Family, FIPS-200 Area, and NIST 800-37 Process Step. Black Kite does all of this without scanning or modifying any of the organization's business assets. https://blackkite.com/platform/ (accessed December 8, 2023).

Exhibit 10: U.S. Patent No. 11,652,834

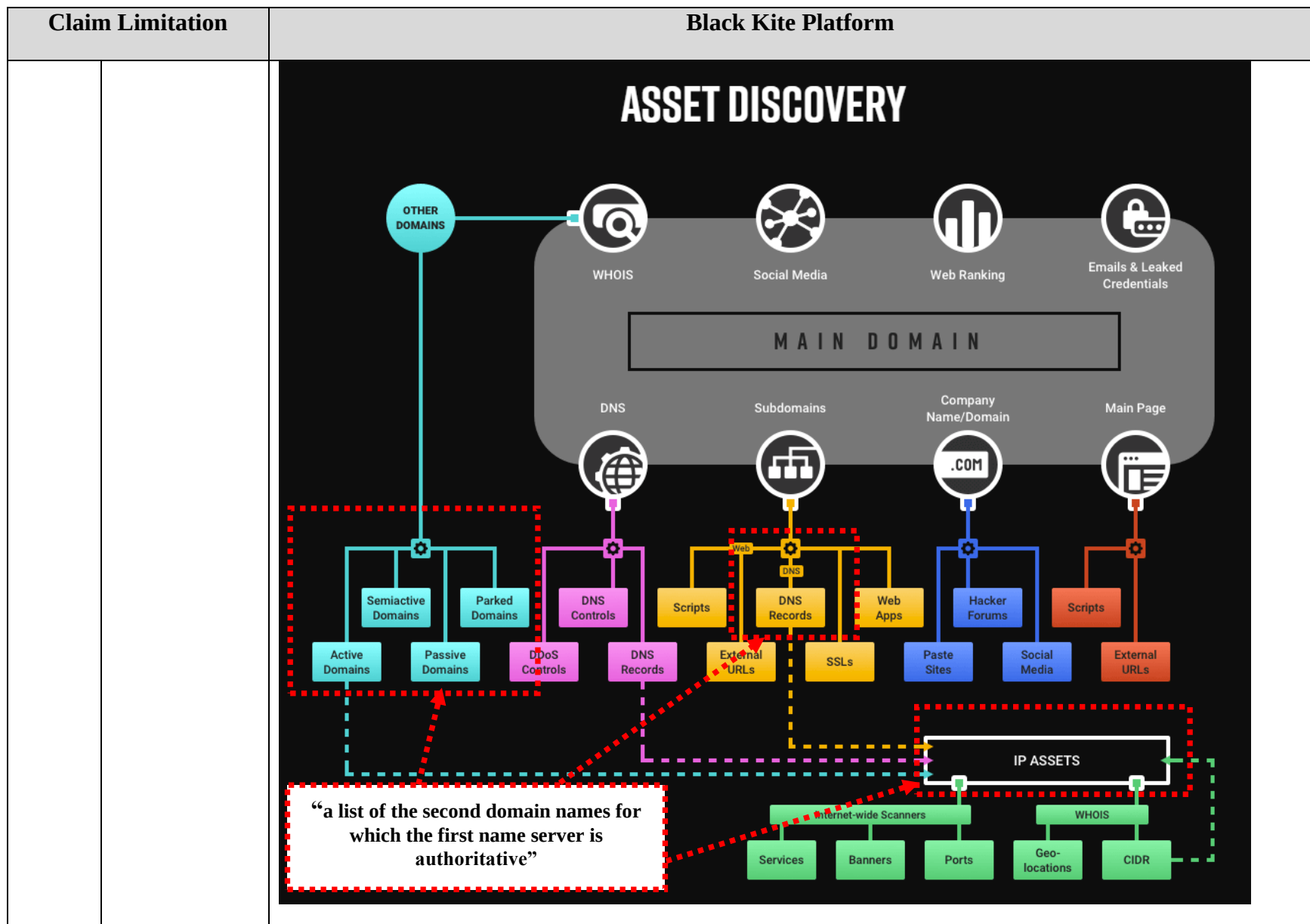


Exhibit 10: U.S. Patent No. 11,652,834

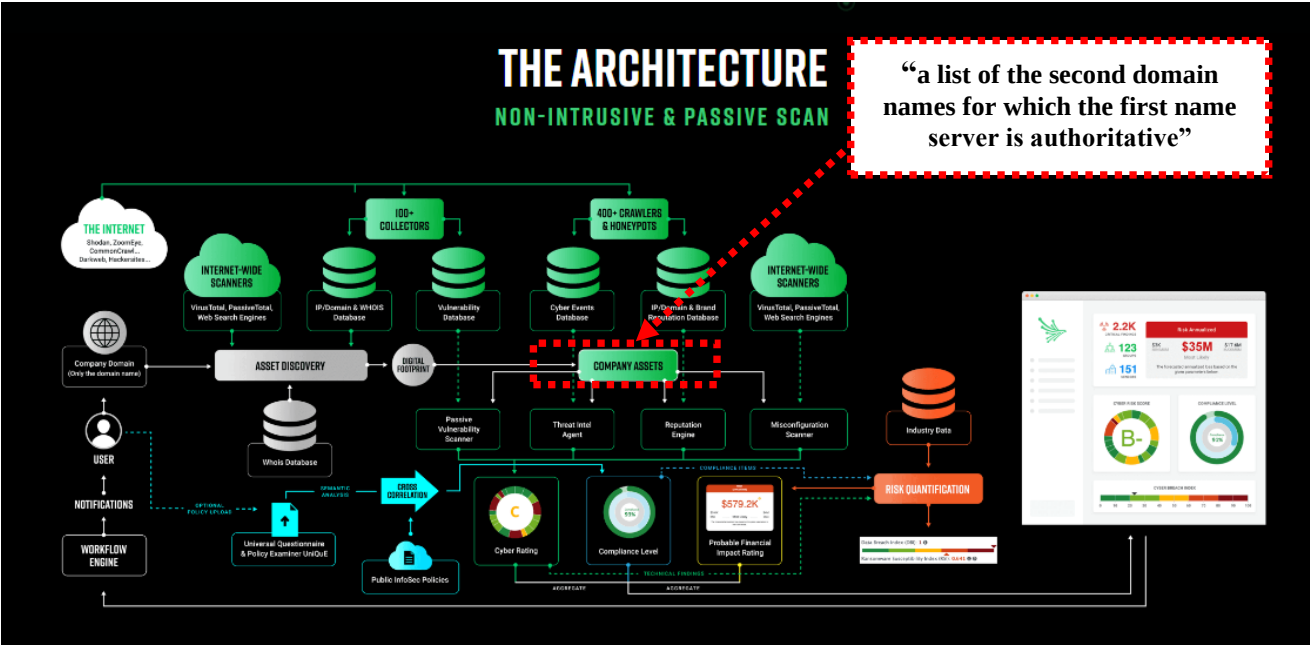
Claim Limitation	Black Kite Platform
	https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).  https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).
1[f] sending, for each of the second domain names, a third passive DNS query to identify host names for the	The Black Kite Platform sends, for each of the second domain names, a third passive DNS query to identify host names for the hosts of the second domain name and IP addresses for the host names:

Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation	Black Kite Platform
hosts of the second domain name and IP addresses for the host names;	What is our Methodology? Cyber Threat Susceptibility Assessment (CTSA) is a methodology for evaluating the susceptibility of a system to cyberattacks developed by MITRE. CTSA quantitatively assesses a system's inability to resist a cyberattack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). To generate the cyber risk rating, Black Kite only needs the company domain. The engine collects information from VirusTotal, Passive DNS servers, web search engines, and other Internet-wide scanners, as well as Black Kite's proprietary databases, which hold more than 10 billion historic items. The engine searches the databases to find all IP address ranges and domain names that belong to the company. Black Kite uses what is called Open Source Intelligence (OSINT) to gather information. The following map shows how hackers can leverage their attack vectors by using OSINT resources like hacker forums, social networks, Google, leaked database dumps, paste sites, or even legitimate security services like VirusTotal, Censys, Cymon, Shodan, or Google Safe Browsing. Black Kite compiles this data into a simple, understandable report with letter-grade scores to help identify and mitigate potential security risks. The platform identifies the risks (CVE/CWE), the risk score of the corresponding vulnerabilities/weaknesses (CVSS/CWSS) and attack patterns (CAPEC/FIPS-199 impact level). Black Kite also classifies the findings into FISMA Cyber Security Framework Area and Maturity Level, NIST 800-53 Control Family, FIPS-200 Area, and NIST 800-37 Process Step. Black Kite does all of this without scanning or modifying any of the organization's business assets. https://blackkite.com/platform/ (accessed December 8, 2023).

Exhibit 10: U.S. Patent No. 11,652,834

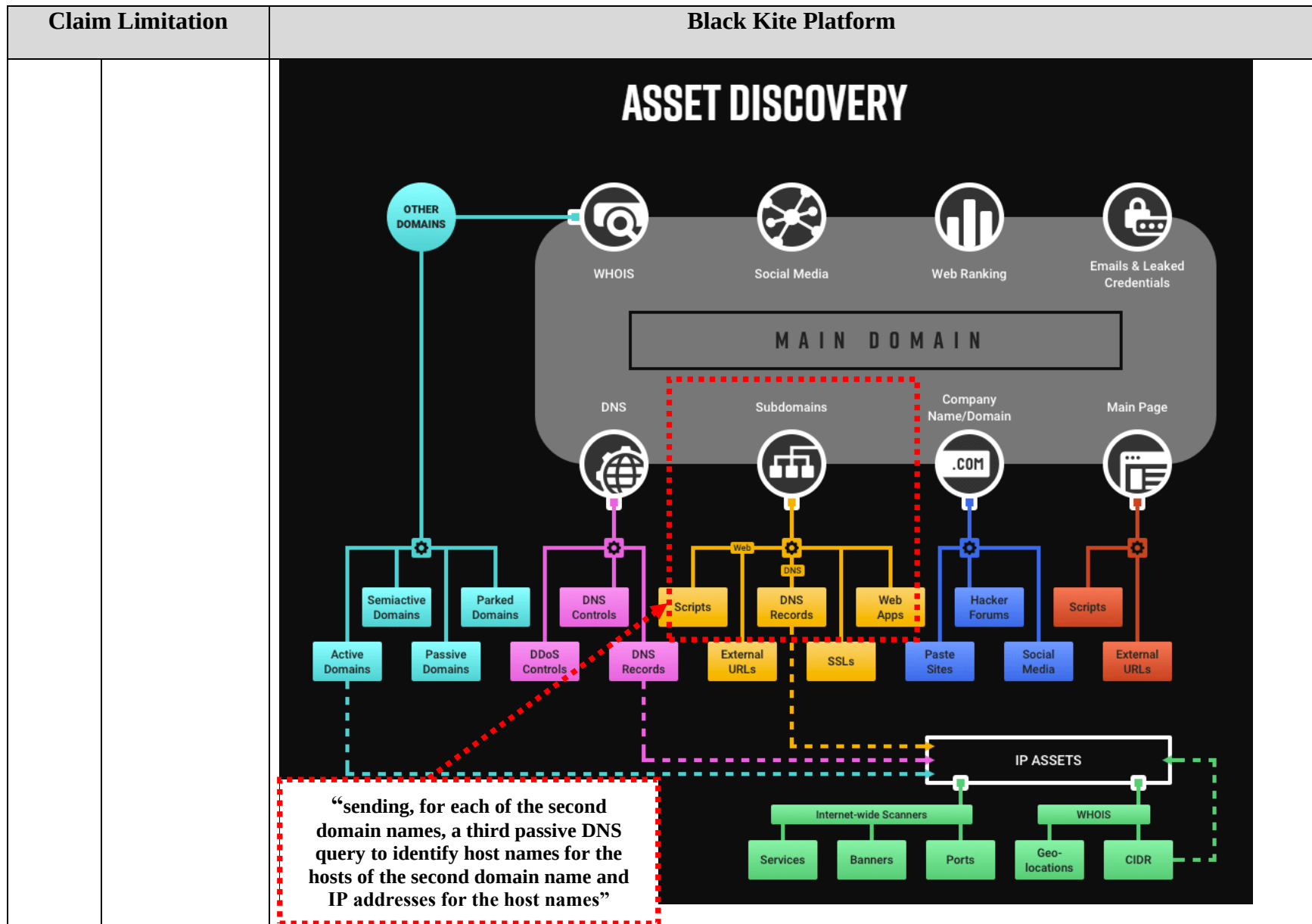


Exhibit 10: U.S. Patent No. 11,652,834

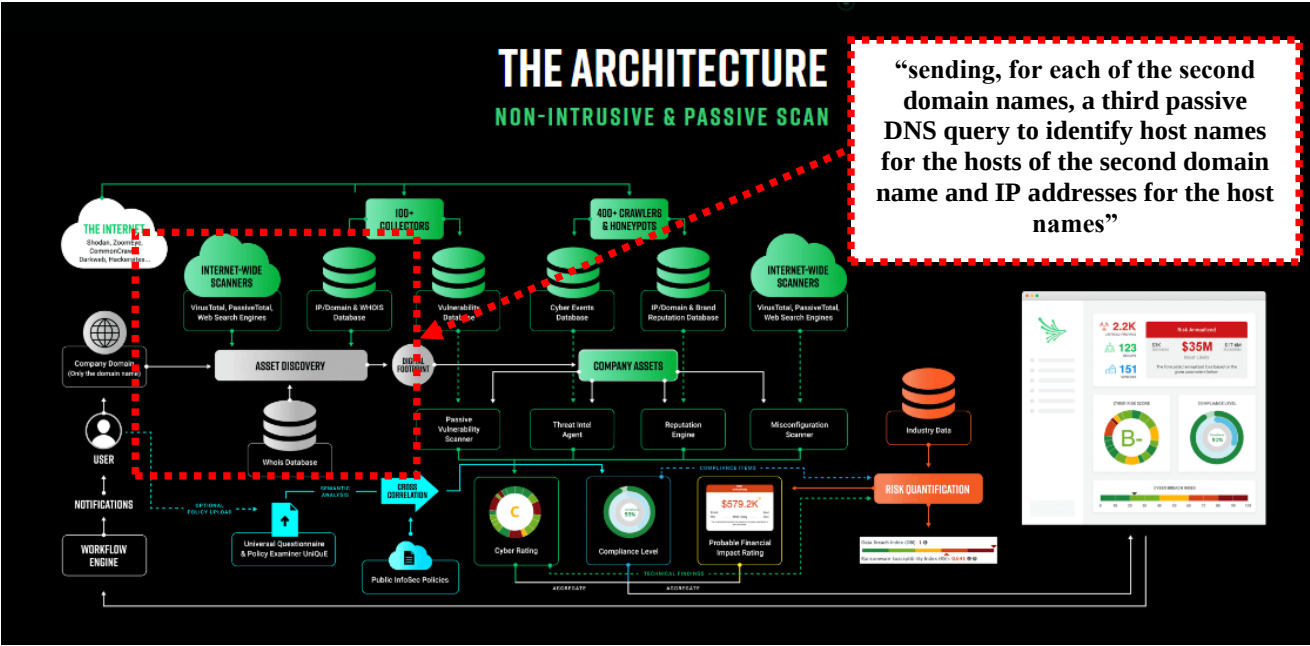
Claim Limitation	Black Kite Platform
	https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).  THE ARCHITECTURE NON-INTRUSIVE & PASSIVE SCAN “sending, for each of the second domain names, a third passive DNS query to identify host names for the hosts of the second domain name and IP addresses for the host names” https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).
1[g] receiving a list of the host names and the IP addresses for the host names; and	The Black Kite Platform receives a list of the host names and the IP addresses for the host names:

Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation	Black Kite Platform
	What is our Methodology? Cyber Threat Susceptibility Assessment (CTSA) is a methodology for evaluating the susceptibility of a system to cyberattacks developed by MITRE. CTSA quantitatively assesses a system's inability to resist a cyberattack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). To generate the cyber risk rating, Black Kite only needs the company domain. The engine collects information from VirusTotal, Passive DNS servers, web search engines, and other Internet-wide scanners, as well as Black Kite's proprietary databases, which hold more than 10 billion historic items. The engine searches the databases to find all IP address ranges and domain names that belong to the company. Black Kite uses what is called Open Source Intelligence (OSINT) to gather information. The following map shows how hackers can leverage their attack vectors by using OSINT resources like hacker forums, social networks, Google, leaked database dumps, paste sites, or even legitimate security services like VirusTotal, Censys, Cymon, Shodan, or Google Safe Browsing. Black Kite compiles this data into a simple, understandable report with letter-grade scores to help identify and mitigate potential security risks. The platform identifies the risks (CVE/CWE), the risk score of the corresponding vulnerabilities/weaknesses (CVSS/CWSS) and attack patterns (CAPEC/FIPS-199 impact level). Black Kite also classifies the findings into FISMA Cyber Security Framework Area and Maturity Level, NIST 800-53 Control Family, FIPS-200 Area, and NIST 800-37 Process Step. Black Kite does all of this without scanning or modifying any of the organization's business assets. https://blackkite.com/platform/ (accessed December 8, 2023).

Exhibit 10: U.S. Patent No. 11,652,834

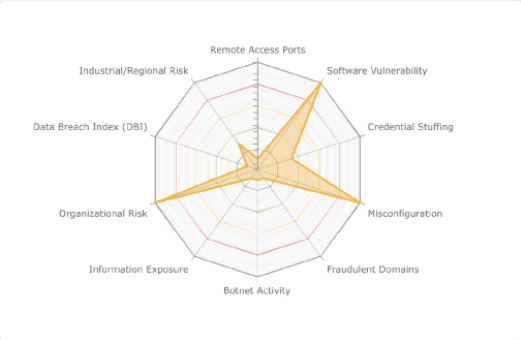
Claim Limitation		Black Kite Platform																		
		 Example Corp OTHER SERVICES (EXCEPT PUBLIC ADMINISTRATION) (NAICS: 81) You are 29% more susceptible to ransomware than the industry average LOWEST RISK HIGHEST RISK INDUSTRY AVERAGE YOU ARE HERE 0.58  FINDINGS SOFTWARE VULNERABILITY (83) <table><tr><td>Email Security</td><td>paradox-team.com</td><td>DMARC Record Warning SMTP-003 Medium CWSS: 4.7 Please check DMARC policy: v=dmARC1; p=none</td></tr><tr><td>Email Security</td><td>lejardinfrancais.fr</td><td>DMARC Record Failed SMTP-003 Medium CWSS: 4.7 DMARC Record Not Found</td></tr><tr><td>Credential Mgmt.</td><td>example.com</td><td>Leaked Credentials Failed LEAK-003 Critical CWSS: 8 Source: 1111_com_tw_leak Leaked Credential Count: 73</td></tr><tr><td>Credential Mgmt.</td><td>example.com</td><td>Leaked Credentials Failed LEAK-003 Critical CWSS: 8 Source: pawno_su_leak Leaked Credential Count: 22</td></tr><tr><td>Patch Management</td><td>example.com</td><td>Patch Management Failed PATCH-001 Critical CWSS: 9.8 35.202.250.208 (Product: php/5.6.31) An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.</td></tr><tr><td>Patch Management</td><td>example.com</td><td>Patch Management Failed PATCH-001 Critical CWSS: 9.8 128.127.180.84 (Product: php/5.6.40) The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .> with a long string.</td></tr></table> Ransomware Radar  https://blackkite.com/platform/ (accessed December 8, 2023).	Email Security	paradox-team.com	DMARC Record Warning SMTP-003 Medium CWSS: 4.7 Please check DMARC policy: v=dmARC1; p=none	Email Security	lejardinfrancais.fr	DMARC Record Failed SMTP-003 Medium CWSS: 4.7 DMARC Record Not Found	Credential Mgmt.	example.com	Leaked Credentials Failed LEAK-003 Critical CWSS: 8 Source: 1111_com_tw_leak Leaked Credential Count: 73	Credential Mgmt.	example.com	Leaked Credentials Failed LEAK-003 Critical CWSS: 8 Source: pawno_su_leak Leaked Credential Count: 22	Patch Management	example.com	Patch Management Failed PATCH-001 Critical CWSS: 9.8 35.202.250.208 (Product: php/5.6.31) An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.	Patch Management	example.com	Patch Management Failed PATCH-001 Critical CWSS: 9.8 128.127.180.84 (Product: php/5.6.40) The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .> with a long string.
Email Security	paradox-team.com	DMARC Record Warning SMTP-003 Medium CWSS: 4.7 Please check DMARC policy: v=dmARC1; p=none																		
Email Security	lejardinfrancais.fr	DMARC Record Failed SMTP-003 Medium CWSS: 4.7 DMARC Record Not Found																		
Credential Mgmt.	example.com	Leaked Credentials Failed LEAK-003 Critical CWSS: 8 Source: 1111_com_tw_leak Leaked Credential Count: 73																		
Credential Mgmt.	example.com	Leaked Credentials Failed LEAK-003 Critical CWSS: 8 Source: pawno_su_leak Leaked Credential Count: 22																		
Patch Management	example.com	Patch Management Failed PATCH-001 Critical CWSS: 9.8 35.202.250.208 (Product: php/5.6.31) An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.																		
Patch Management	example.com	Patch Management Failed PATCH-001 Critical CWSS: 9.8 128.127.180.84 (Product: php/5.6.40) The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .> with a long string.																		

Exhibit 10: U.S. Patent No. 11,652,834

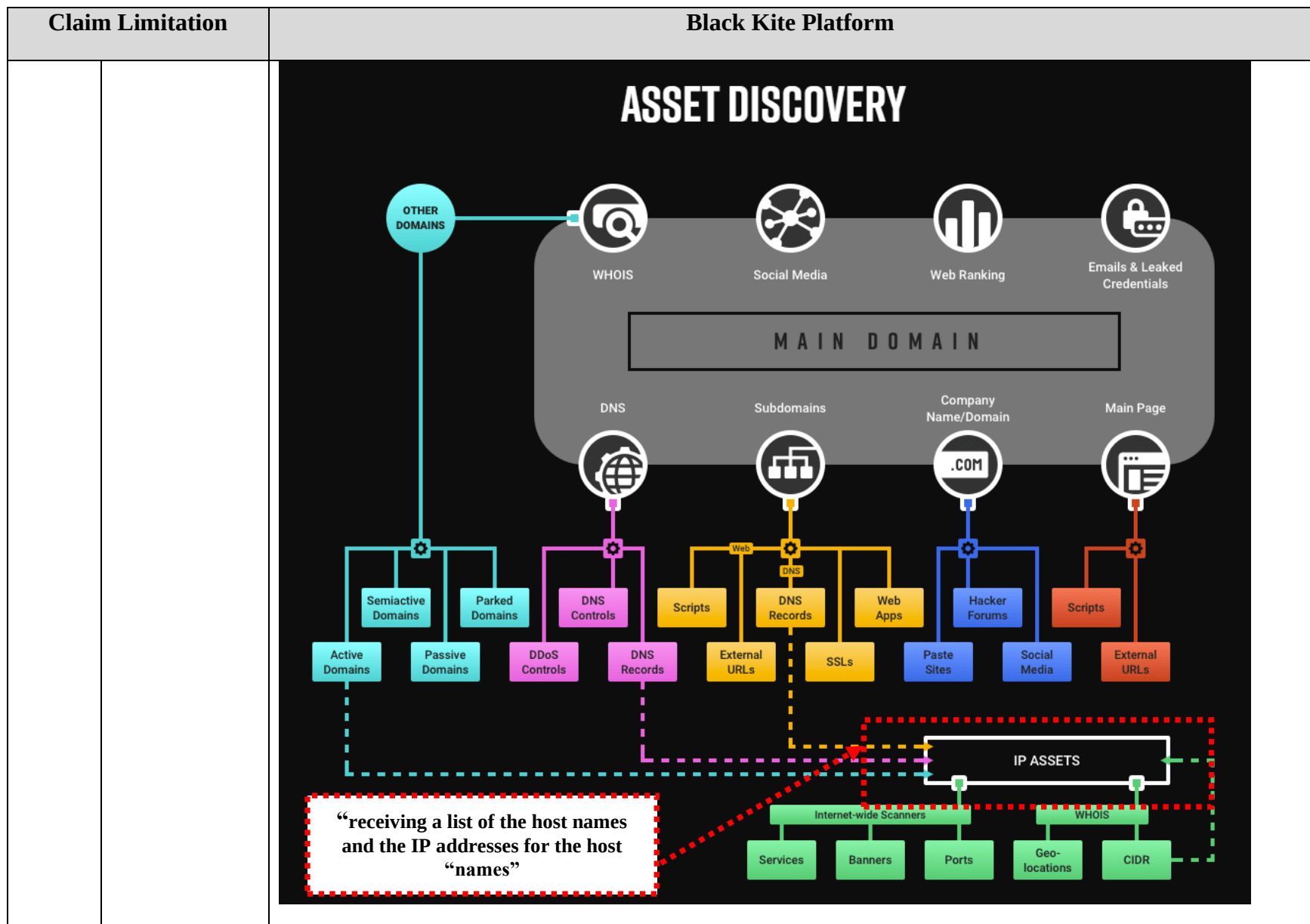


Exhibit 10: U.S. Patent No. 11,652,834

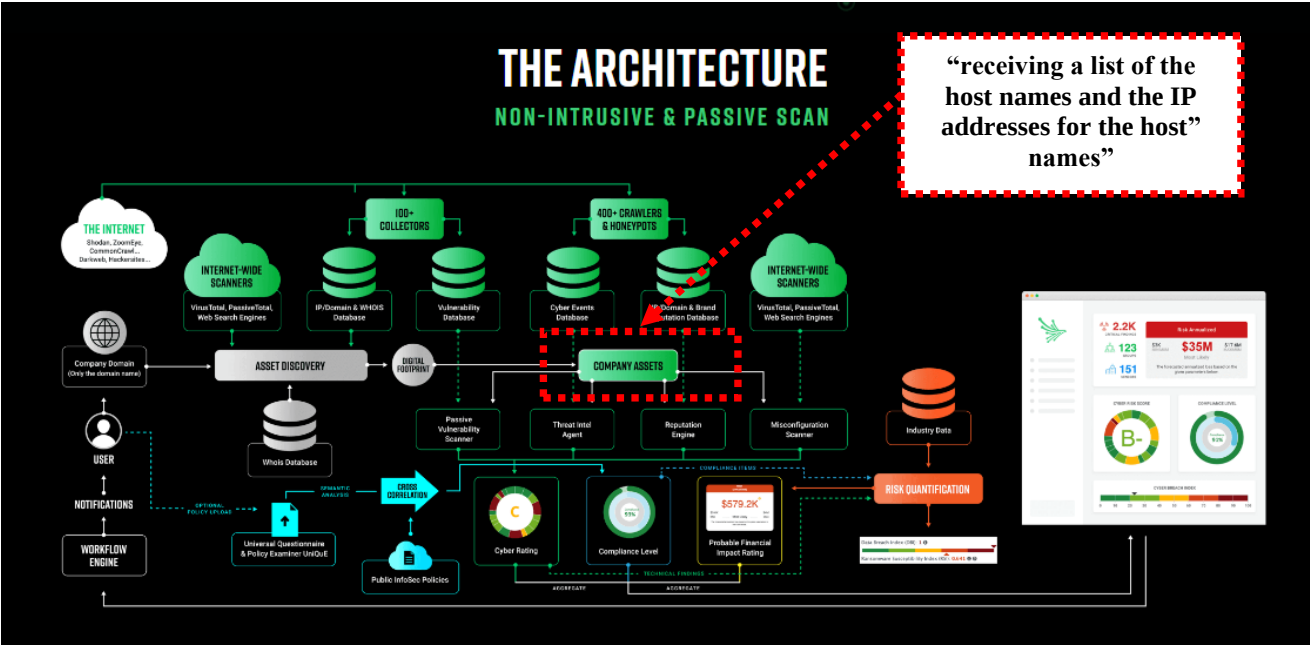
Claim Limitation	Black Kite Platform
	https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).  https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).
1[h]	mapping each IP address to an attribute for the entity. The Black Kite Platform maps each IP address to an attribute for the entity:

Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation		Black Kite Platform					
		What is our Methodology? Cyber Threat Susceptibility Assessment (CTSA) is a methodology for evaluating the susceptibility of a system to cyberattacks developed by MITRE. CTSA quantitatively assesses a system's inability to resist a cyberattack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). To generate the cyber risk rating, Black Kite only needs the company domain. The engine collects information from VirusTotal, Passive DNs servers, web search engines, and other Internet-wide scanners, as well as Black Kite's proprietary databases, which hold more than 10 billion historic items. The engine searches the databases to find all IP address ranges and domain names that belong to the company. Black Kite uses what is called Open Source Intelligence (OSINT) to gather information. The following map shows how hackers can leverage their attack vectors by using OSINT resources like hacker forums, social networks, Google, leaked database dumps, paste sites, or even legitimate security services like VirusTotal, Censys, Cymon, Shodan, or Google Safe Browsing. Black Kite compiles this data into a simple, understandable report with letter-grade scores to help identify and mitigate potential security risks. The platform identifies the risks (CVE/CWE), the risk score of the corresponding vulnerabilities/weaknesses (CVSS/CWSS) and attack patterns (CAPEC/FIPS-199 impact level). Black Kite also classifies the findings into FISMA Cyber Security Framework Area and Maturity Level, NIST 800-53 Control Family, FIPS-200 Area, and NIST 800-37 Process Step. Black Kite does all of this without scanning or modifying any of the organization's business assets. https://blackkite.com/platform/ (accessed December 8, 2023). <table><tr><td>M-7</td><td>Discovery Footprinting</td><td>Digital footprint should include all registered domains, sub domain sand assigned/used IP addresses with daily updates. User should be able to exclude exceptional assets like honeypots, malware sandboxes, guest networks and BYOD networks. User should be able to remove implausible items from (and add new assets to monitor to) the scorecard.</td><td>Yes. NormShield compiles an organization's digital presence on the web. This process is part of the initial and continuous asset discovery delivered in the digital footprint category. The digital Footprint includes domains (Active or Dormant), Subdomains, IP addresses, CIDR blocks, services, etc.. Like any other module in the NormShield platform, it is customizable to the customer's requirements. Whether you need to manually add a domain/IP or exclude an asset that is part of a Sandbox or honey pot, all can be done with the click of a button.</td></tr></table> NormShield, <i>CISO Investigate: Third Party Risk Management</i>, at 78 (2020), https://blackkite.com/wp-content/uploads/2020/09/CISOs-Investigate-TPRM-NormShield-1-compressed.pdf (accessed December 8, 2023).		M-7	Discovery Footprinting	Digital footprint should include all registered domains, sub domain sand assigned/used IP addresses with daily updates. User should be able to exclude exceptional assets like honeypots, malware sandboxes, guest networks and BYOD networks. User should be able to remove implausible items from (and add new assets to monitor to) the scorecard.	Yes. NormShield compiles an organization's digital presence on the web. This process is part of the initial and continuous asset discovery delivered in the digital footprint category. The digital Footprint includes domains (Active or Dormant), Subdomains, IP addresses, CIDR blocks, services, etc.. Like any other module in the NormShield platform, it is customizable to the customer's requirements. Whether you need to manually add a domain/IP or exclude an asset that is part of a Sandbox or honey pot, all can be done with the click of a button.
M-7	Discovery Footprinting	Digital footprint should include all registered domains, sub domain sand assigned/used IP addresses with daily updates. User should be able to exclude exceptional assets like honeypots, malware sandboxes, guest networks and BYOD networks. User should be able to remove implausible items from (and add new assets to monitor to) the scorecard.	Yes. NormShield compiles an organization's digital presence on the web. This process is part of the initial and continuous asset discovery delivered in the digital footprint category. The digital Footprint includes domains (Active or Dormant), Subdomains, IP addresses, CIDR blocks, services, etc.. Like any other module in the NormShield platform, it is customizable to the customer's requirements. Whether you need to manually add a domain/IP or exclude an asset that is part of a Sandbox or honey pot, all can be done with the click of a button.				

Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation	Black Kite Platform
	Black Kite establishes the assessment scope during the asset discovery process, which discovers all publicly visible/accessible domains, subdomains, IP/CIDR ranges, etc. IP/Domain Reputation: Identify IP addresses that send unwanted requests. Using the IP reputation list you can identify if an IP address has a bad reputation or member of a botnet. Fraudulent Domains: Domains registered by fraudsters plan to launch phishing attacks, sell knock-off goods on spoofed sites, or use "typo-squatting" domains to make money off unintentional traffic for other sites. Digital Footprint: Your digital footprint refers to a digital collection of data that can be traced back to you. This includes IPs, domains, subdomains, email addresses and server fingerprints. Attack Surface: The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter or extract data. Black Kite, <i>Cyber Risk Assessment Documentation</i>, at 9, 18-19 (Mar. 29, 2021), https://blackkite.com/wp-content/uploads/2021/04/Black-Kite-Cyber-Risk-Assessment-Documentation.pdf (accessed December 8, 2023).

Exhibit 10: U.S. Patent No. 11,652,834

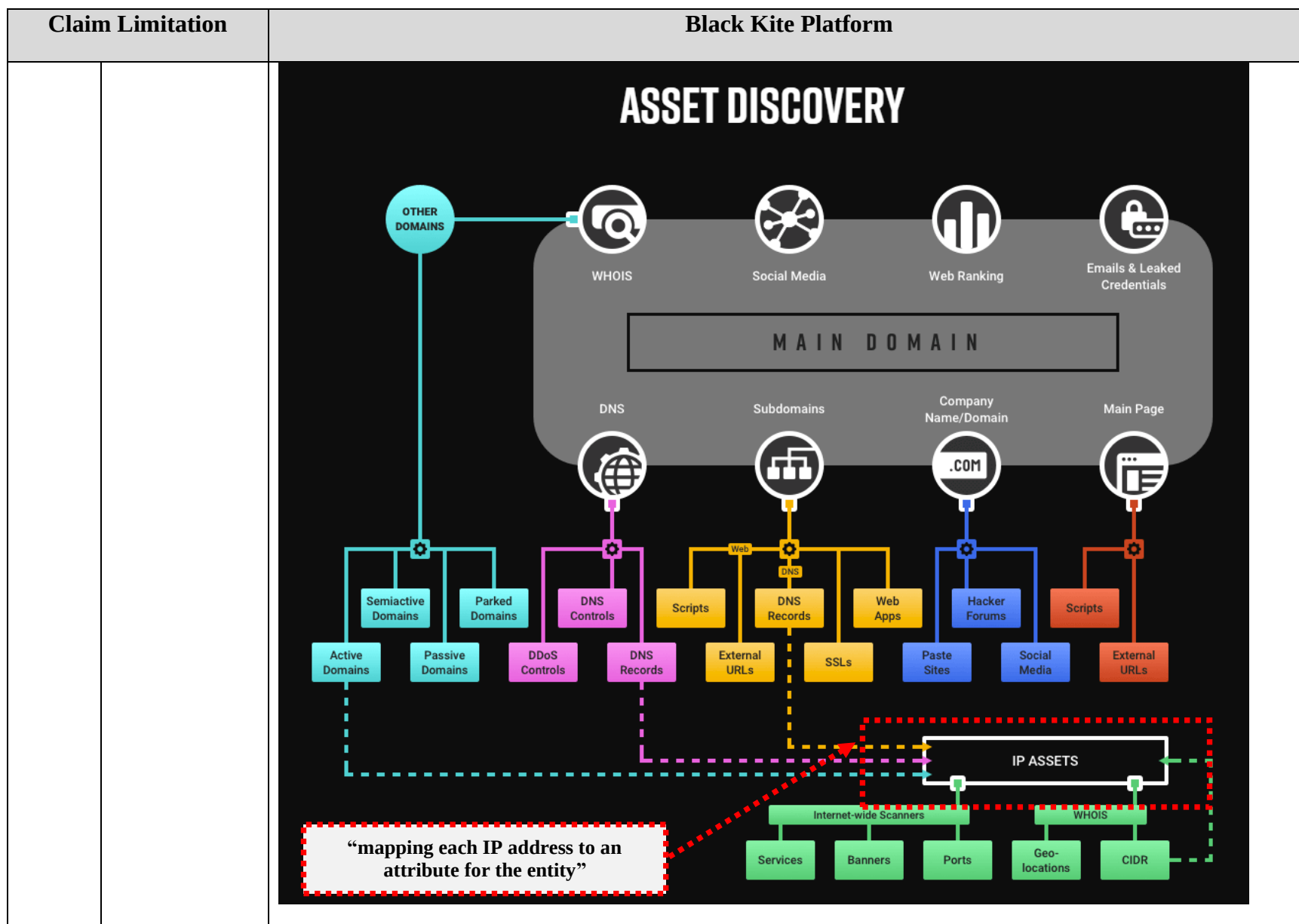
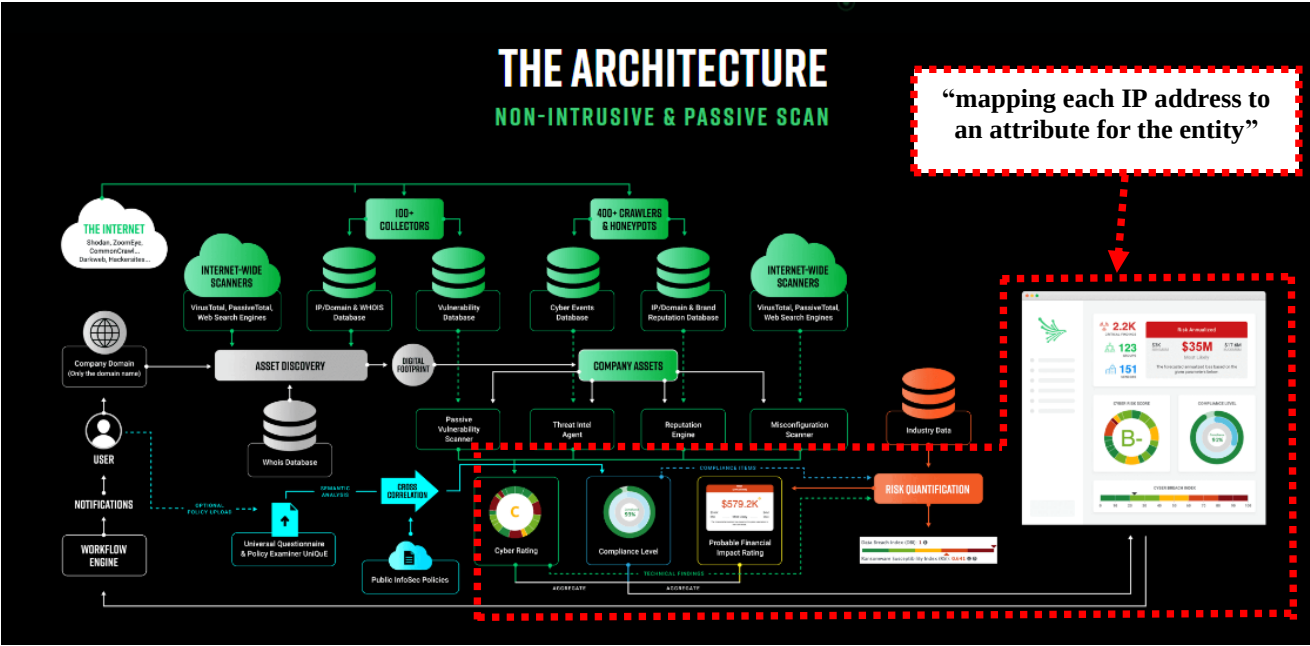


Exhibit 10: U.S. Patent No. 11,652,834

Claim Limitation	Black Kite Platform
	https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).  https://blackkite.com/black-kites-methodology/ (accessed December 8, 2023) (annotated).