SecureIQlab®

Security Service Edge Command & Control Prevention Comparative Report

TEST PERIOD: DECEMBER 2022—DECEMBER 2022

LAST REVISION: 09 MARCH 2023

COMMISSIONED BY: PALO ALTO NETWORKS

www.secureiqlab.com

Report Contents:

1. Executive Summary

SecureIQLab tested the ability of Security Service Edge (SSE) products to block the command-and-control capabilities of the Cobalt Strike attack suite. Three products were tested: Palo Alto Networks Prisma Access, Cisco Umbrella, and Zscaler ZIA.

The test measured the block rate of the tested SSE solutions against Cobalt Strike in 5 attack scenarios.

From the results of these tests, SecureIQLab concludes Palo Alto Network's machine learning approach provides superior protection.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products		
	Cisco	Palo Alto Networks	Zscaler
	Umbrella SIG Essentials	Prisma Access Enterprise	ZIA Transformation Bundle
Overall Block Rate	**16.7%**	**99.2%**	**15.7%**

Table 1: Overall Block Rate Results.

2. INTRODUCTION

Command-and-control[1] ("C2") attacks include implants that report back to the attacker's server. The attacker's server, in turn, issues commands to a compromised machine. A compromised machine will carry out the commands from the attacker's server and may install additional software. This can be leveraged into complete control of the compromised machine and pivoting to attack other hosts in the environment.

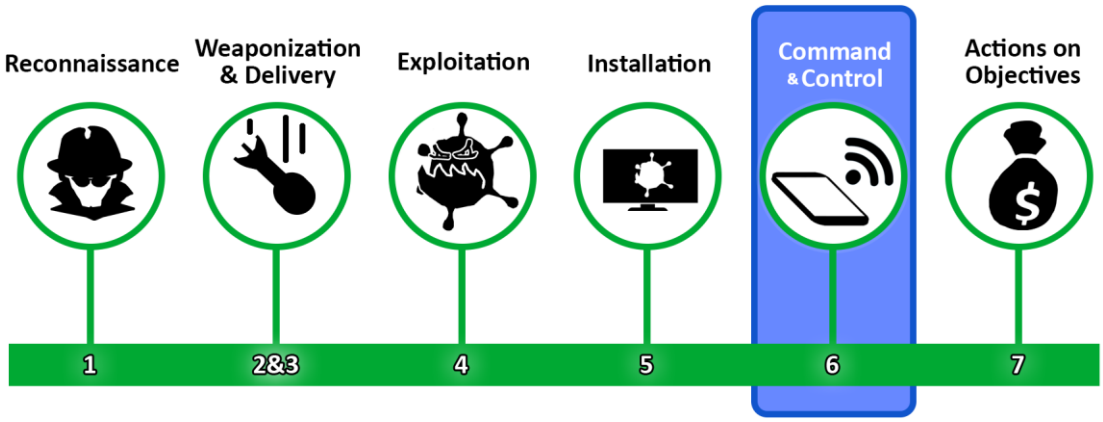

Figure 1: Position of Command and Control in the Lockheed Martin Cyber Kill Chain®.

Cobalt Strike is a commercial command-and-control attack suite now owned by Fortra (formerly HelpSystems). According to the Fortra website, Raphael Mudge created the Cobalt Strike command-and-control framework in 2012 to assist red teams in testing enterprise defense postures against post-exploitation activity.

The Cobalt Strike GUI makes it very easy to use by even unsophisticated hackers. Access to this commercial tool has historically been highly restricted; however, cracked versions have recently become available. As a result, Cobalt Strike has become a favorite post-exploitation framework for threat actors[2] and a force that security providers must reckon with.

Attackers using Cobalt Strike can change many settings using malleable C2 profiles. In the wild, there has been a proliferation of publicly available malleable C2 profiles that can be used to evade detection by security products. Researchers have also created and shared tools to generate new randomized Cobalt Strike profiles easily.

[1] https://attack.mitre.org/tactics/TA0011/

[2] https://go.recordedfuture.com/hubfs/reports/cta-2022-0118.pdf.

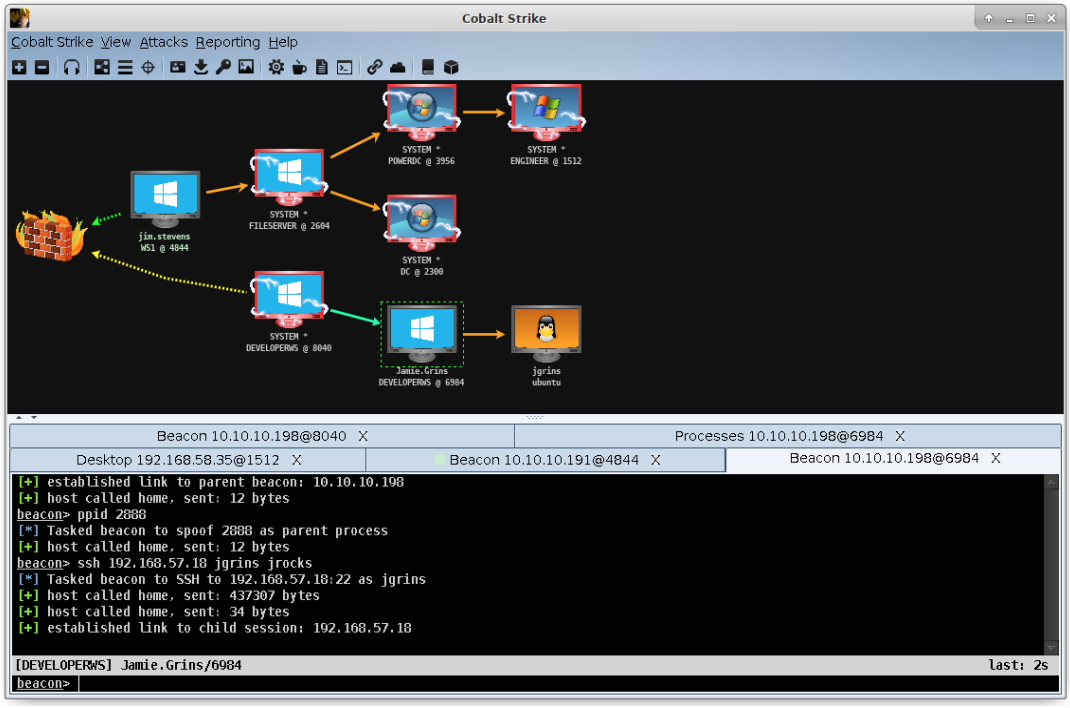

Figure 2: Official Screenshot of Cobalt Strike GUI from https://www.cobaltstrike.com/screenshots/.

This test did not cover all of Cobalt Strike's capabilities; instead, it was limited to testing SSE's ability to block Cobalt Strike's network callback functions.

To provide detection of command-and-control network activity between a "team server" and "beacon" (the Cobalt Strike attack server and the implant, respectively), network security products typically utilize traditional IPS signatures to match against specific static strings and patterns unique to Cobalt Strike. However, these signatures can be easily evaded with malleable profiles that can create endless combinations of the content that may have been used as Cobalt Strike "fingerprints" in creating static IPS signatures. To combat this, in addition to traditional IPS signatures, Palo Alto Networks has launched its Advanced Threat Prevention service that detects and blocks these modifications to typical command-and-control traffic in real-time. This is the second commissioned comparative test on this topic conducted by SecureIQLab. Our first test can be found here.

Palo Alto Networks commissioned this test to measure the value of their Advanced Threat Prevention capability compared to other leading security solutions in protecting customers against Cobalt Strike command-and-control network activity. This report is intended to indicate protection not only against Cobalt Strike's basic/standard command-and-control network activity but also to evaluate the relative resiliency of the protection provided by each product when modifications are made to evade detection.

This report is not intended as a how-to manual for hacking these products. Therefore, we omit or redact specific details of attacks.

3. Test Environment

Cobalt Strike version 4.7.2 was used in this test with Debian 5.16.18-1 kernel used as the platform to host Cobalt Strike's team server. On the attack side, the Cobalt Strike team server was hosted on the public internet. Windows 10 Enterprise running on ESXI 7.0.2 was used as the target platform for implant installation and subsequent command and control activities.

The following products and firmware/software versions were tested:

Prisma Access Enterprise:	Prisma Access 3.2
Cisco Umbrella SIG Essentials:	Umbrella SIG Essentials
Zscaler ZIA Transformation Bundle:	ZIA 6.2

High-security policies suitable for deployment in a typical enterprise environment were created for all available and applicable security functionality (e.g., DNS Security, Antivirus/Sandboxing, URL Filtering, Application Control, IPS/Vulnerability Protection, SSL/decryption). Because there were subtle differences in the product settings, URL Filtering and Application Control policies were matched up as closely as possible across all products.

Publicly available best-practice documentation and admin guides for each product were referred to confirm that all products were at least minimally configured to best-practice specifications for all security features/modules ("best-practice or better"). Because product performance is generally highly configuration-dependent, results might differ if different settings had been used for any of the products tested. True positive testing was then performed to confirm the functionality of all configured security policies.

False positive testing was also performed as needed to conservatively tune the policies to what would be appropriate/acceptable for a typical enterprise. For example, the ability to browse to and render general popular websites (e.g., Amazon, Bing, CNN, MSNBC, and Wikipedia) was tested. Additionally, our false positive testing included websites closely mirroring those used in various Cobalt Strike profiles through the product as configured.

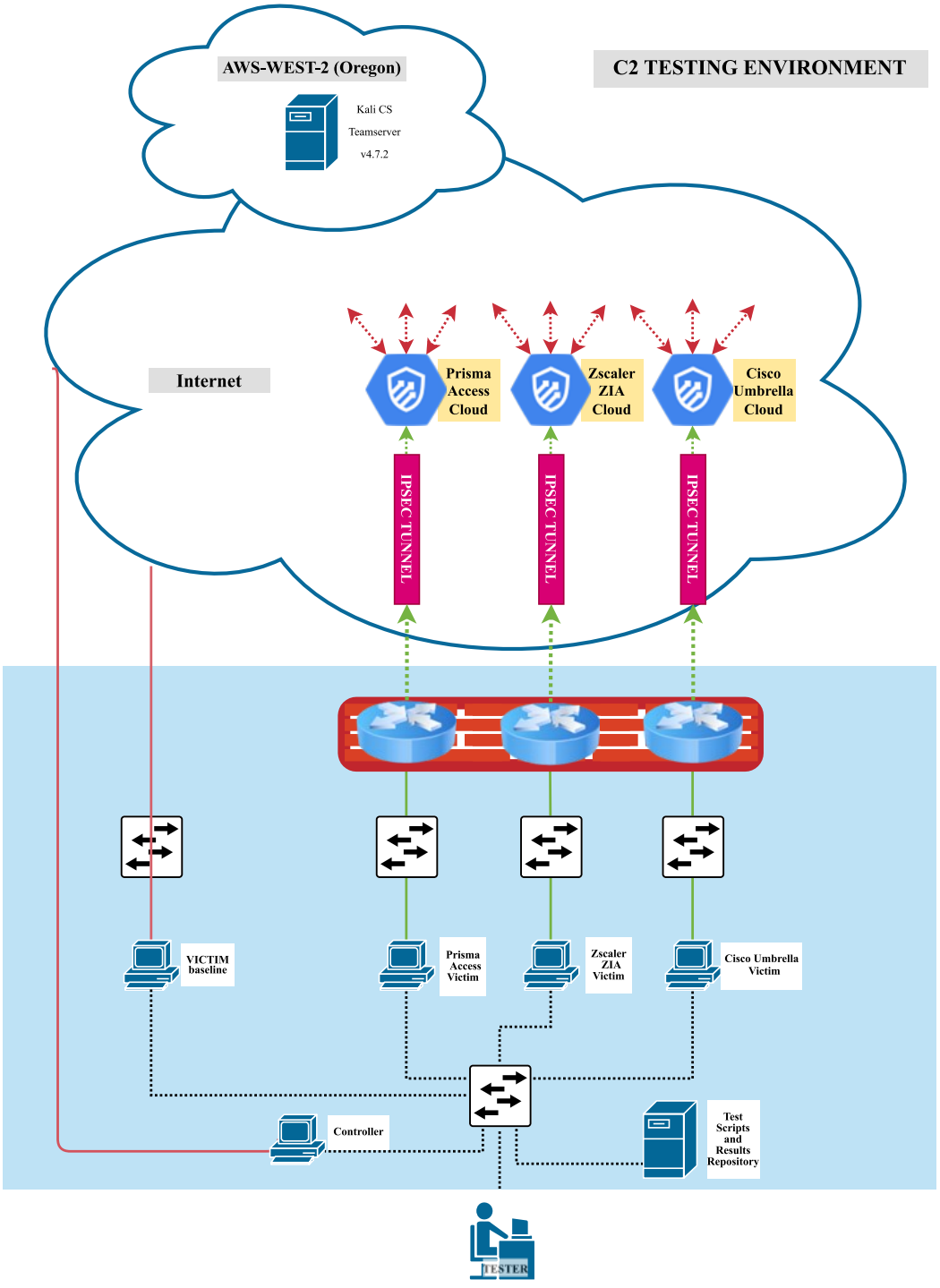

Figure 3: Command-and-Control Testing Environment.

4. Test Procedure

The overall command-and-control test procedure included five main categories of attack scenarios executed using the Cobalt Strike attack framework. Each of the five categories examines a major aspect of a product's capabilities in a specific real-world scenario. HTTP over TCP port 80 was used for command-and-control communication unless otherwise noted. For each profile tested, a stageless implant/beacon was generated and delivered to the "victims" for execution out-of-band prior to testing. In other words, only the product's capability to intervene and protect against Cobalt Strike callback network activity was tested, not the ability to block the initial delivery of the beacon itself; exploitation and delivery of the beacon are assumed to have already taken place.

The types of attacks we evaluated are:

1. **Basic Attack Scenario:** This test was performed to evaluate the product's basic protection against the most commonly available public attack profiles attempting data exfiltration and malware delivery via HTTP. The basic attack scenario included three subcategories: Normal, Crimeware, and APT. Each scenario had a multitude of profiles that were evaluated as a part of the Cobalt Strike attack framework.
2. **Random Attack Scenario:** This test was performed to evaluate the protection when Cobalt Strike is leveraged to generate "randomized" attack scenarios using tools that are part of the Cobalt Strike arsenal of researchers and the public. This randomization increases the probability that the traditional threat defenses of the firewall might be rendered ineffective against data exfiltration and malware delivery.
3. **Custom Attack Scenario:** This was the first of the confirmation tests, which used a smaller profile set. This test was performed using purposely chosen and modified attacks from the Basic and Random attack scenarios. The modifications were made to attacks that were previously blocked to confirm whether the modifications would be sufficient to bypass the defenses. Modifications were made on the different variables that are supported for customization.
4. **Non-Standard ports-based Attack Scenario:** The purpose of this testing was to confirm if the SSEs can continue to provide protection when attacks use HTTP over a non-standard port.
5. **HTTPS Attack Scenario:** The purpose of this testing was to confirm if the SSEs provide the same level of protection when attacks are delivered via HTTPS rather than HTTP.

The test cases did not have equal sample sizes. The Custom Attack Scenario, Nonstandard Ports-based Attack Scenario, HTTPS Ports-based Attack Scenario were verification exercises. Thus, they did not require many profiles. As a result, the majority of profiles were run in the Basic Attack and Random Attack Scenarios.

It is possible to block some of these command-and-control attacks on the Domain Name System (DNS) and Uniform Resource Locator (URL) level. However, threat actors can seed these domains/URLs for a long time to make them appear legitimate, and thus the entire attack might bypass these protections. Thus, for this test, these capabilities were disabled should they be responsible for a block. That is, to simulate seeding, in some cases the SSE's DNS and/or URL protections were disabled (e.g., newly observed domain category was set to monitor rather than block).

5. Scoring Criteria

Products under test earned blocking credit in two ways: First, by stopping the Cobalt Strike attack at the communication stage, and second, by blocking the attack at the exfiltration and download stage.

The communication stage is when the compromised machine checks in with the Cobalt Strike Team Server and command-and-control is established. Blocking credit at the communication stage was earned by preventing the command-and-control link from establishing.

The exfiltration and download stage is when the compromised machine sends out data or downloads malware, as directed in the communication stage. Blocking credit at the exfiltration and download stage was earned by blocking the exfiltration of system data (output of command output,e.g., 'whoami /all'), blocking output of one or more screenshots, and preventing the download of malware. At least one stage of the malicious traffic needed to be blocked in order to earn blocking credit at the exfiltration and download stage.

Some graphs differentiate between blocking credit at the communication stage and blocking credit at the exfiltration and download stages. Where blocking credit is not differentiated, blocking credit was given for blocking at either stage.

6. Overall Block Rate

The Overall Block Rate is intended to give a general overview of the capability of products under test to withstand, absorb, and mitigate variations in Cobalt Strike profiles generated via different tools and third-party maintained profiles. It includes the results from all the variations of attacks conducted. The Overall Block Rate is an unweighted calculation. It is computed by dividing the total number of attacks blocked by all the attacks launched.

$$Overall\ Block\ Rate = \left(\frac{blocked\ attacks}{total\ attacks} \right) \times 100\%$$

Equation 1: Formula for Computation of Overall Block Rate.

The higher the Overall Block Rate, the better the product's ability to withstand attacks. In this test, the product's responses to 485 attacks were evaluated.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products		
	Cisco	Palo Alto Networks	Zscaler
	Umbrella SIG Essentials	Prisma Access Enterprise	ZIA Transformation Bundle
Overall Block Rate	**16.7%**	**99.2%**	**15.7%**
Communication stage	15.5%	95.8%	7.63%
Additional Exfiltration and download stage	1.2%	3.4%	8.0%

Table 2: Table of Overall Block Rate Results by Block Stage.

Overall Block Rate is only a general overview because not all attacks are equal: The composition of the various Cobalt Strike attacks targeting a given network may vary from the composition of the profiles in this test.

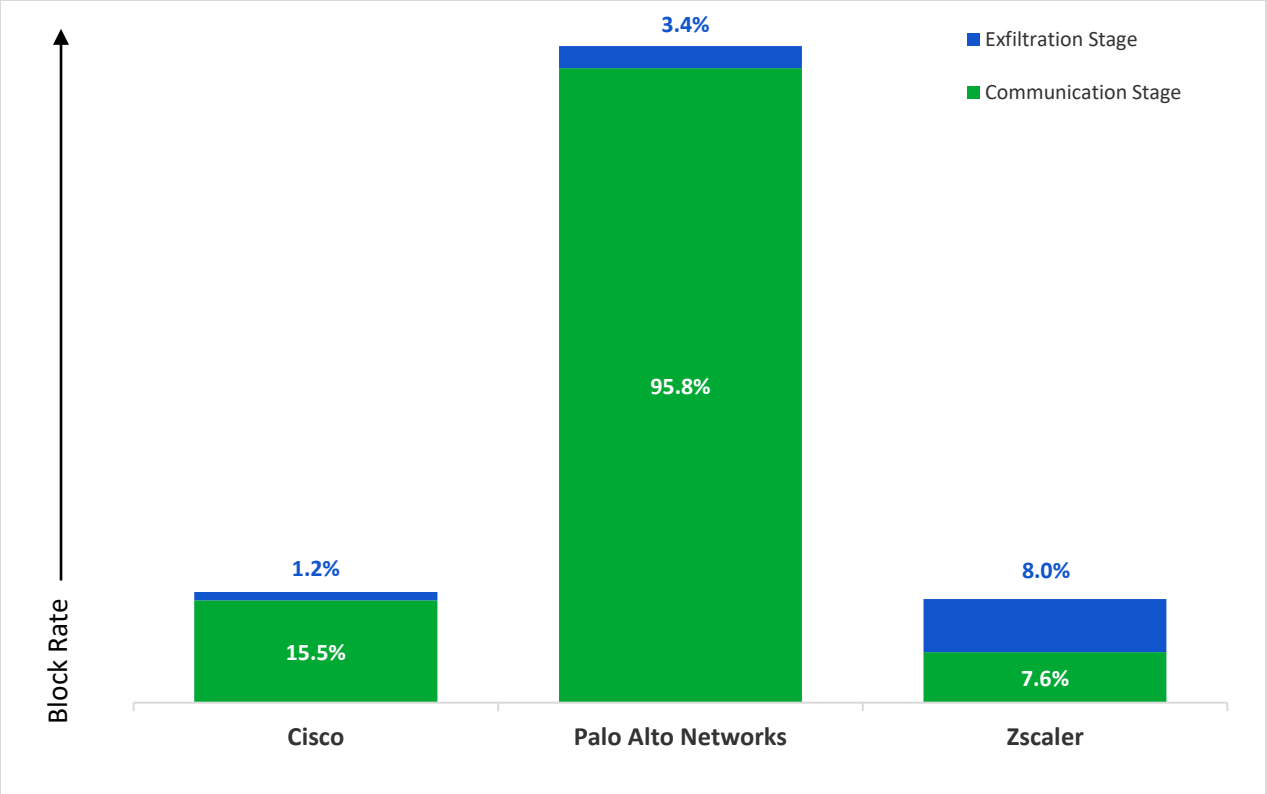

Figure 4: Overall Block Rate by Attack Stage.

7. Comparative Analysis

This section provides a breakdown of results by category. As such, it provides a more detailed analysis of the tested product's performance than the Overall Block Rate.

The summary of key results below shows how the three security vendors fared during our validation across five main categories of attack scenarios using the Cobalt Strike attack framework. This validation was performed alongside false positive validation during the entire test period. In all cases, results are reported using the unweighted percentages of attacks blocked.

$$Percentage\ of\ attacks\ blocked = \left(\frac{blocked\ attacks}{total\ attacks} \right) \times 100\%$$

Equation 2: Formula for Computation of Percentage of Attacks Blocked.

Attack scenarios are broken down into five categories: The Basic Attack Scenario, the Random Attack Scenario, the Custom Attack Scenario, the Non-standard Ports Attack Scenario and the HTTPS-based Attack Scenario. Each is discussed in greater detail in the following sections.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products		
	Cisco	Palo Alto Networks	Zscaler
	Umbrella SIG Essentials	Prisma Access Enterprise	ZIA Transformation Bundle
1. Basic Attack Scenario	**16.9%**	**100.0%**	**44.1%**
Enterprise Attack Profile Set 1	22.5%	100.0%	22.5%
Enterprise Attack Profile Set 2	0.0%	100.0%	100.0%
Enterprise Attack Profile Set 3	23.3%	100.0%	46.6%
Enterprise Attack Profile Set 4	16.7%	100.0%	16.7%
Enterprise Attack Profile Set 5	22.2%	100.0%	34.7%
2. Random Attack Scenario	**12.9%**	**100.0%**	**2.9%**
Random Attack Test Set 1	2.2%	100.0%	0.0%
Random Attack Test Set 2	4.9%	100.0%	0.8%
Random Attack Test Set 3	31.6%	100.0%	7.9%
3. Custom Attack Scenario	**33.3%**	**66.7%**	**41.7%**
4. Non-standard Ports Attack Scenario	**100.0%**	**100.0%**	**75.0%**
5. HTTPS-based Attack Scenario	**No**	**Yes**	**Yes**

Table 3: Overview Block Rate by Attack Scenario Category.

BASIC ATTACK SCENARIO COMPARATIVE ANALYSIS

This test was conducted to evaluate the product's basic protection against the most commonly available public attack profiles that attempt data exfiltration and malware delivery via HTTP.

The Basic Attack Scenario consisted of five Enterprise Attack Profile sets. These sets consisted of attacks that are being used in the wild. These five profiles sets each had three categories of profiles, Normal Operational Attack profiles, APT Attack Profiles, and Crimeware Attack Profiles. They are grouped together as basic attacks because the attack techniques are already known and well-researched by the cybersecurity community and publicly available. In total, this test consisted of 158 Cobalt Strike attack Profiles.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products		
	Cisco	Palo Alto Networks	Zscaler
	Umbrella SIG Essentials	Prisma Access Enterprise	ZIA Transformation Bundle
1. Basic Attack Scenario	**16.9%**	**100.0%**	**44.1%**
Enterprise Attack Profile Set 1	22.5%	100.0%	22.5%
Enterprise Attack Profile Set 2	0.0%	100.0%	100.0%
Enterprise Attack Profile Set 3	23.3%	100.0%	46.6%
Enterprise Attack Profile Set 4	16.7%	100.0%	16.7%
Enterprise Attack Profile Set 5	22.2%	100.0%	34.7%

Table 4: Overview Table Excerpt, Basic Attack Scenario by Toolset Used to Generate.

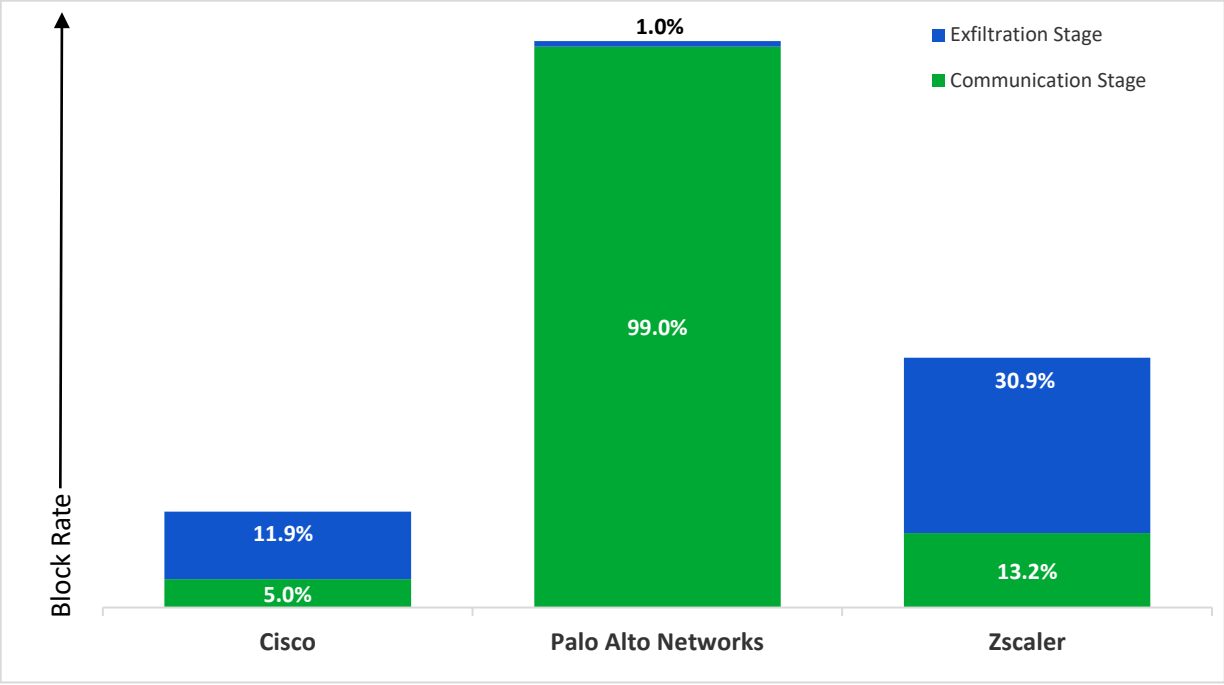

Figure 5: Block Rate for Basic Attack Scenario with Block Type Indicated.

Each of the profiles tested in the above Basic Attack Scenario, can also be categorized into three attack types: the Normal Operational Attack Set, the Crimeware Attack Set and the APT Operation Attack Set.

The following table gives the total block rates by attack type.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products		
	Cisco	Palo Alto Networks	Zscaler
	Umbrella SIG Essentials	Prisma Access Enterprise	ZIA Transformation Bundle
1. Basic Attack Scenario	**16.9%**	**100.0%**	**44.1%**
Normal Operational Attack Set	16.0%	100.0%	22.6%
Crimeware Attack Set	30.8%	100.0%	53.9%
APT Attack Set	0.0%	100.0%	41.7%

Table 5: Basic Attack Scenario Block Rate by Attack Type

The Normal Operational Attack Set consisted of attacks that mimicked Amazon, One Drive, and other "safe" browsing traffic requests and responses. This traffic looks harmless to most users and inspection tools, however in the test this traffic included malicious activity masked as part of this harmless traffic. The Normal Operational Attack Set tested the response to 75 attacks.

The Crimeware Attack Set consisted of attacks that mimicked known botnets as well as attacks that can hide in non-malicious traffic. An example of a known botnet that was tested was Emotet. Data from this test is useful to expose gaps in coverage to known threats. The Crimeware Attack Set tested the response to 65 attacks.

The APT Attack Set consisted of known APT (Advanced Persistent Threat) attacks. For example, one APT threat that was mimicked was The Dukes APT 29. These attacks were included to test the SSE product's ability to prevent attacks that are modus operandi for high-profile APT attacks. The APT Attack Set tested the response to 12 attacks.

The block rate by attack subcategory (Normal, Crimeware, APT) is shown visually in the table below. Because the Normal Operational Attack Set, the APT Attack Set, and the Crimeware Attack Set all consist of different numbers of attacks, the percentages in the table below added together and divided by three do not match the overall block rate in the Basic Attack Scenario.

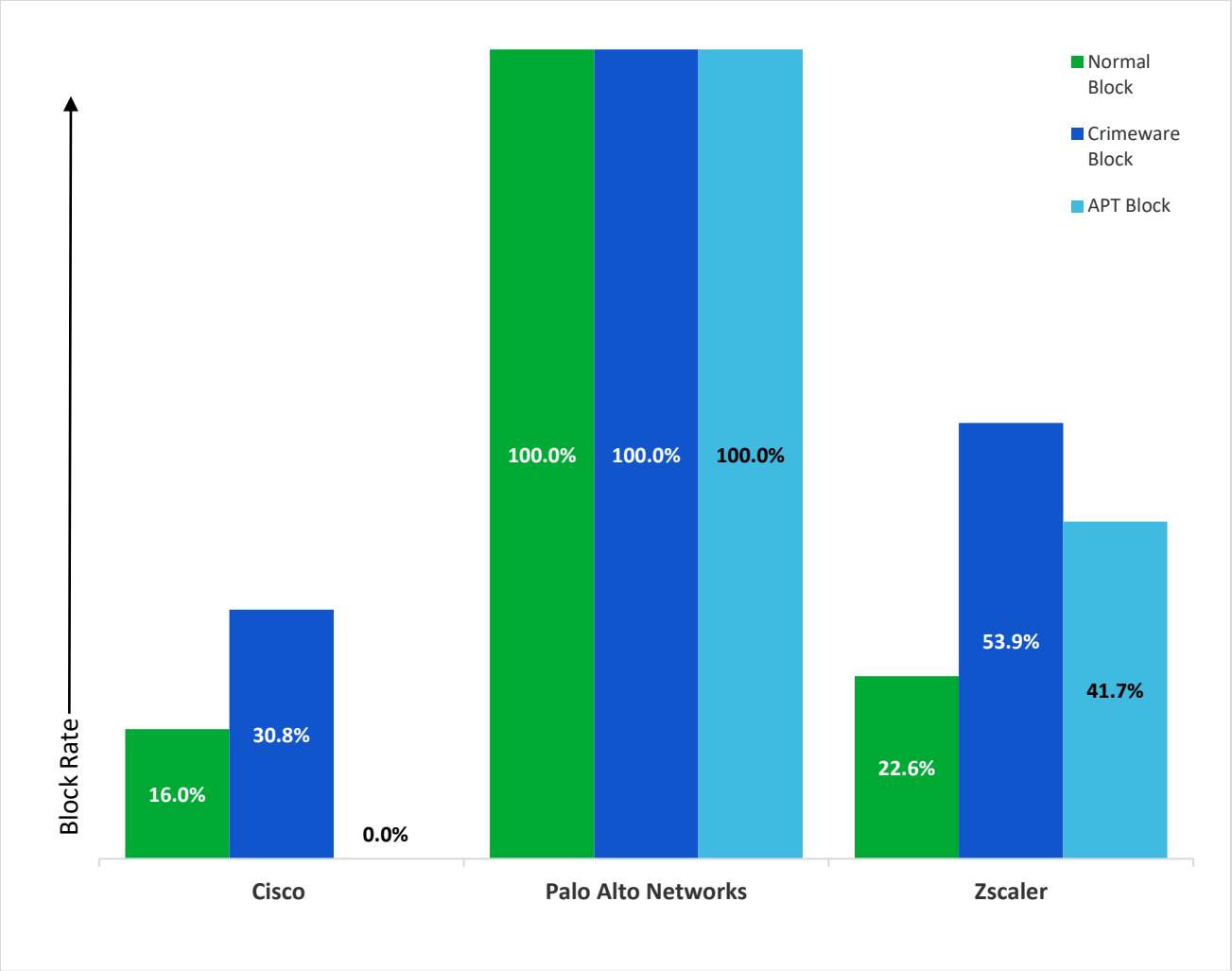

Figure 6: Overall Profile Block Rate for Basic Attack Scenario by Attack Type.

Random Attack Scenario Comparative Analysis

This test was intended to evaluate each product's protection against commonly available tools that are leveraged to generate "randomized" attack scenarios using Cobalt Strike, in turn increasing the probability of the traditional threat defenses of the firewall being rendered ineffective against data exfiltration and malware delivery via HTTP. SecureIQLab tested 311 attack profiles in this test.

The Random Attack Scenario consisted of profiles that were generated by three tools that were publicly available and maintained at the time of testing. Each tool was used to generate an attack set, labeled Random Attack Test Set 1, Random Attack Test Set 2, and Random Attack Test Set 3. The three toolsets used are not named because they are available in the wild, and our test results would show what vendors they are effective against.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products		
	Cisco	Palo Alto Networks	Zscaler
	Umbrella SIG Essentials	Prisma Access Enterprise	ZIA Transformation Bundle
2. Random Attack Scenario	12.9%	100.0%	2.9%
Random Attack Test Set 1	2.2%	100.0%	0.0%
Random Attack Test Set 2	4.9%	100.0%	0.8%
Random Attack Test Set 3	31.6%	100.0%	7.9%

Table 6: Overview Table Excerpt, Random Attack Scenario.

The following graph shows the overall block rate for each vendor within the Random Attack Scenario for each of the three Random Attack Sets. Because the three Random Attack Sets each had a different number of attack profiles, the sum of the percentages in the following graph divided by three does not equal the Random Attack Scenario block rate.

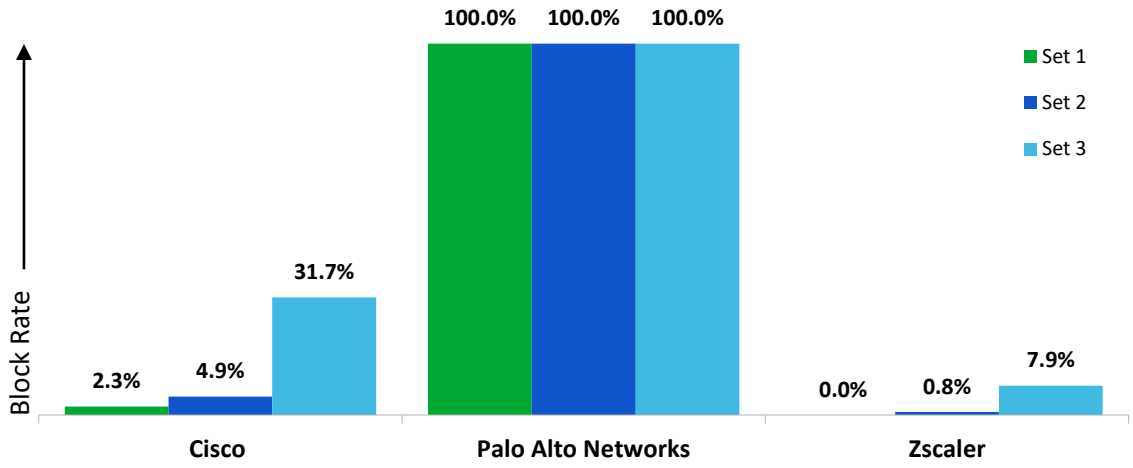

Figure 7: Random Attack Scenario Block Rate by Random Attack Set.

CUSTOM ATTACK SCENARIO COMPARATIVE ANALYSIS

This test was intended to evaluate the SSE solution's protection against intelligently modified attacks from the Basic Attack Scenario and Random Attack Scenario.

The Custom Attack Scenario was intended to model attacks from a more sophisticated actor. We started with attacks that were previously blocked in the Basic Attack Scenario or Random Attack Scenario. We then modified variables inside the profiles, which from data analysis, looked likely to impact block rate. For example, sleep time is a highly customizable variable inside the baseline profile. Increasing this value will force the product under test to wait for more time to inspect the incoming traffic. No attack was blocked by every SSE product we tested. At least one of the Custom Attack Profiles out of 12 [name redacted] was blocked by none.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products		
	Cisco	Palo Alto Networks	Zscaler
	Umbrella SIG Essentials	Prisma Access Enterprise	ZIA Transformation Bundle
3. Custom Attack Scenario	33.3%	66.7%	41.7%

Table 7: Overall Table Excerpt, Custom Attack Scenario.

Because of the individualized nature of the test, the sample size was relatively small. SecureIQLab tested twelve Cobalt Strike attack profiles in this test. Each attack was designed to test a specific aspect of the product's ability to block.

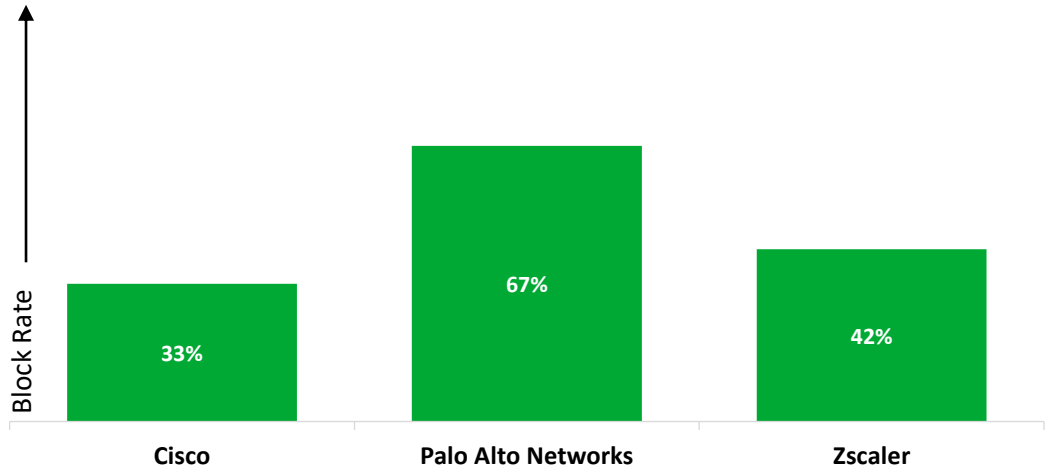

Figure 8: Custom Attack Scenario Block Rate.

Attackers in the wild may affirmatively target designated vendors. Because we did not tailor the attacks against specific vendors, this test is more useful as an indicator of relative product capabilities than as a measure of absolute protection afforded by a product.

NONSTANDARD PORTS COMPARATIVE ANALYSIS

The purpose of this testing is to confirm if the tested SSE products can continue to provide protection when attacks are targeting a nonstandard port.

The Non-standard Ports Attack Scenario consisted of profiles that were hosted via HTTP on a non-standard port. We used basic attack profiles for this validation. Typically, HTTP traffic is hosted on TCP port 80. We hosted previously blocked profiles on a different port to see if the evaluated SSEs maintained their prevention coverage for the same attacks when hosted on different ports. This test included 12 attacks.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products		
	Cisco	Palo Alto Networks	Zscaler
	Umbrella SIG Essentials	Prisma Access Enterprise	ZIA Transformation Bundle
4. Non-standard Ports Attack Scenario	100.0%	100.0%	75.0%

Table 8: Overview Table Excerpt, Non-standard Ports Attack Scenario.

As the data table above shows, the SSEs we tested from Cisco, Palo Alto Networks, and Zscaler were still able to consistently block the profiles that the SSEs had previously been able to block when attacks using those profiles were relaunched on a nonstandard port. However, on one of the profiles we tested, Zscaler had only protection for that profile on port 443 and port 80, even though the profile could be used over a variety of TCP ports. This indicated an inconsistent lack of coverage on different ports as opposed to deficiency of overall protection over various ports and protocols.

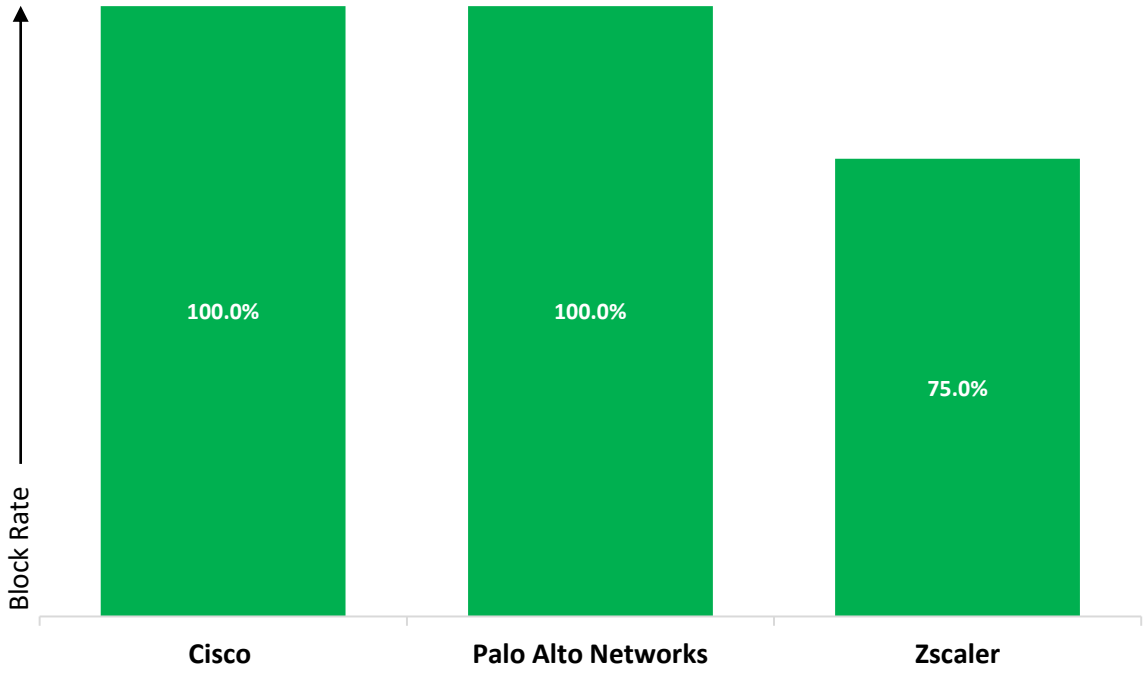

Figure 9: Non-standard Port Attack Scenario Block Rate.

HTTPS Port-based Attack Scenario Comparative Analysis

The purpose of this testing is to confirm if the next-generation SSE products provide the same level of protection when attacks are delivered via HTTPS. This test is important because over 80% of the Web traffic is SSL driven.

The HTTPS-based Attack Scenario consisted of profiles that used HTTPS rather than HTTP for communication. This included APT and Normal Operational attack profiles. In this test, we tested five Cobalt Strike attack profiles. Cisco's results indicate that it doesn't decrypt SSL traffic destined to its IPS module.

Cobalt Strike Command-and-Control Profile Categories	Vendors and Products		
	Cisco	Palo Alto Networks	Zscaler
	Umbrella SIG Essentials	Prisma Access Enterprise	ZIA Transformation Bundle
5. HTTPS-Based Attack Scenario	No	Yes	Yes

Table 9: Overview Table Excerpt, HTTPS-Based Attack Scenario.

8. Conclusion

In the five Cobalt Strike attack suite tests we performed, the Palo Alto Networks SSE solution we tested was either the top performer or tied for top performance.

Reviewing the results of the tests in sequence, the Palo Alto Networks SSE we tested performed better than the competition in the Basic Attack Scenario. The Palo Alto Networks SSE managed to block 99.2% of attacks, while the next best performance was Cisco's SSE at 16.7%. In the Random Attack Scenario, Palo Alto Networks' SSE blocked 100.0% of attacks. The next best performance was from Cisco's SSE, this time at 12.9% blocked.

Turning to the confirmation tests, in the Custom Attack Scenario, the Palo Alto Networks SSE blocked 66.7% of attacks. The next best performance was from the Zscaler's SSE, which blocked 41.7% of attacks. The SSE of Palo Alto Networks and Cisco blocked 100% of attacks in the Non-standard ports Attack Scenario while Zscaler achieved 75%. The SSE of Palo Alto Networks and Zscaler continued to block HTTPS-based attacks that were previously tested using HTTP, while Cisco did not. The results indicate that Cisco's SSE doesn't have full SSL decryption ability.

Overall, Palo Alto Networks performed well against the Cobalt Strike attack profiles we tested. Compared with the other products tested, Palo Alto Network's Advanced Threat Prevention capability outperformed the competition by a significant margin in most of the Cobalt Strike tests we executed.

9. Appendix

Product Staging

The following documentation was referred to during product configuration:

Zscaler:

- https://help.zscaler.com/zia/recommended-ips-control-policy
- https://help.zscaler.com/zia/recommended-malware-protection-policy
- https://help.zscaler.com/zia/recommended-advanced-threat-protection-policy
- https://help.zscaler.com/zia/recommended-sandbox-policy
- https://help.zscaler.com/zia/recommended-url-cloud-app-control-policy
- https://help.zscaler.com/zia/recommended-file-type-control-policy

Cisco:

- https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/umbrella-design-guide.pdf

On page 81 in the above document, Cisco recommends disabling intelligent proxy if you have Web Policy enabled.

Palo Alto Networks:

- https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/create-prisma-access-policy/best-practices

10. About SecureIQLab

SecureIQLab is a cybersecurity testing lab that was founded in 2019. SecureIQLab works with enterprises, governments, and security vendors to bridge the applied intelligence gap that exists between market and technology research. SecureIQLab also provides services to operationalize security and the metrics to help organizations improve their return on security investments.

SecureIQLab, LLC.
9600 Great Hills Trail, Suite 150W
Austin, TX 78759 USA

+1.512.575.3457

www.secureiqlab.com
info@secureiqlab.com

11. Copyright and Disclaimer

This publication is Copyright © 2023 by SecureIQLab®. Any use of the results, etc., in whole or in part, is ONLY permitted after the explicit written agreement of SecureIQLab prior to any publication. SecureIQLab cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper.

We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the research results cannot be taken by any representative of SecureIQLab. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time.

No one else involved in creating, producing, or delivering research results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, research documents or any related data.

For more information about SecureIQLab and the testing methodologies, please visit our website.

SecureIQLab (March 2023)