Network Control Validation Assessment Report

4/4/2024 04:54 GMT (GMT-0)

Security Control Tested:

- Cisco Firepower

Report generated On:

4/4/2024 05:03 GMT (GMT-0)

Report generated For:

christopherg-1

Christopher Grabowski - cgrabows@cisco.com

Contents

Executive Summary

christopherg-1 Corporation used the AttackIQ platform to evaluate their **Baseline** Security Prevention capabilities. The baseline assessment took place on 4/4/2024 04:54 GMT **against the AttackIQ Test Suite for** Cisco Firepower and tested the security control.

AttackIQ found security risks and offers recommendations for improving christopherg-1 Corporation's system and network security. AttackIQ determined that christopherg-1 Corporation achieved a Prevention Baseline Effectiveness Score of 100.0% (Table 1), which reflects their ability to counter basic adversarial behavior in important security control categories. For more details on this score, refer to the Appendix. This report provides information on the assessment methodology, insights, specific findings, and recommendations to address each identified issue.

Prevention Baseline Effectiveness Score

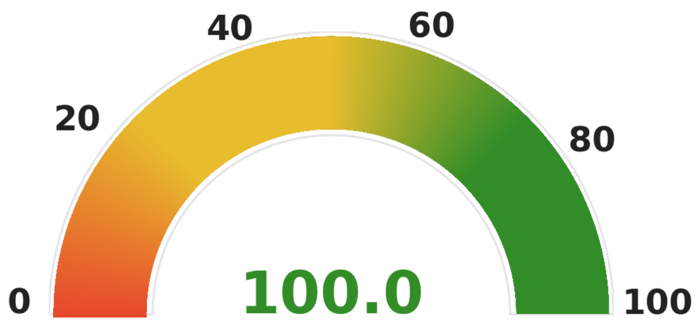


Table 1: christopherg-1 Corporation Prevention Baseline Effectiveness Score

Assessment Scope

During the assessment, the AttackIQ Flex service emulated 6 Test(s) on a single test point in christopherg-1's enviroiment to evaluate the effectiveness of prevention-based Security Controls against the **Cisco Firepower** Test Suite.

Testing Methodology

About the AttackIQ Service

Organizations use AttackIQ to test and audit their security controls to ensure that they work as expected. This threat-informed approach optimizes security control effectiveness by comparing current security control effectiveness to baseline cybersecurity best-practices, and maturing to actively testing against probable threats to fix misconfigurations or close gaps before an attacker exploits them.

User Activation	Execution	Activity on host	Post-Test-Cleanup	Results
User Selects Test Package from the Flex Portal” to “User Selects Test Package from the AttackIQ Portal	Package is executed on the targeted host	Attack Scenarios are executed on the host system	Automatic deletion of temporary files, artifacts and reversion of changes to original state after package is executed	User uploads results to Portal to generate a Report.

AttackIQ Architecture and Setup for Cisco Firepower

The AttackIQ architecture is designed to facilitate comprehensive testing of the effectiveness of security controls in an environment. It consists of multiple components that work together to enable efficient and accurate validation of security measures.

To assess network security controls, AttackIQ leverages the capabilities of the AttackIQ Platform which includes a library of Packet Captures (PCAPs) that represent relevant network malicious behavior from threat actors and malware groups. These PCAPs are based on extensive research and threat intelligence, encompassing a wide range of known attack vectors and methodologies. By utilizing this comprehensive PCAP library, the platform ensures that network security controls are tested against a diverse set of scenarios.

The AttackIQ Platform also includes reporting capabilities that capture detailed information about the test scenarios in real-time as they are executed, including the actions performed, responses received, and any vulnerabilities or weaknesses identified. This data is then used to generate comprehensive reports that provide insights into the effectiveness of the tested security controls. These reports help organizations identify areas for improvement, prioritize remediation efforts, and make informed decisions to enhance their overall security posture.

Package Details

Cisco Secure Firewall Extended Baseline v2

A series of Test Groups and Scenarios that are designed to exercise the basic features and functionality of a Cisco Firepower firewall that has implemented the following capabilities and policies: Malware, File Type, Application Filtering, URL Filtering, Intrusion (based on Balanced security and connectivity policy) and Security Intelligence.

Scope of **Cisco Firepower** Test Suite

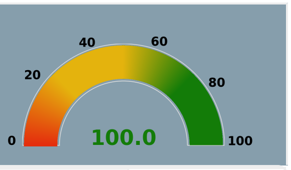
Category	Scenario Count	Description
Security Intelligence	3	-
Intrusion	5	-
URL Filtering	4	-
Application Filtering	3	-
File Type	3	-
Malware	5	-

Results

⊗ Scenario was Not Prevented ✓ Scenario was Prevented, requires no Action

Package Name: Cisco Secure Firewall Extended Baseline v2

23/23 scenario executions were prevented



Category	Scenario	Result
Security Intelligence	PCAP Replay - 2022-05 ViperSoftX PowerShell Download Payload Requests	✓
	PCAP Replay - Web Access to Cisco Botnet test site	✓
	PCAP Replay - Web Access to Cisco Malware test site	✓
Intrusion	PCAP Replay - 2022-03 NanoCore RAT Custom TCP Command and Control Traffic	✓
	PCAP Replay - 2022-06 LokiBot HTTP Command and Control Traffic	✓
	PCAP Replay - APT28 Zebrocy Delphi Downloader	✓
	PCAP Replay - Hancitor CnC Web Communication	✓
	PCAP Replay - NetWire C2 Communication	✓
URL Filtering	PCAP Replay - Web Access to Gambling site PokerStars	✓
	PCAP Replay - Web Access to Filter Avoidance site proxyway	✓
	PCAP Replay - Web access to Pornography site PornHub	✓
	PCAP Replay - Web access to Hacking site www.hackthissite.org	✓
Application Filtering	PCAP Replay - Application AOL videos	✓

Category	Scenario	Result
	PCAP Replay - Application TeamViewer	✓
	PCAP Replay - Application WinSCP	✓
File Type	PCAP Replay - Download Torrent .torrent file	✓
	PCAP Replay - Download Microsoft Outlook .pst file	✓
	PCAP Replay - Download Windows Registry .reg file	✓
Malware	PCAP Replay - GuLoader EXE download	✓
	PCAP Replay - Download Trickbot Loader Malware Sample	✓
	PCAP Replay - Download Ryuk Malware Sample	✓
	PCAP Replay - Emotet Malicious Macro Infection (Variant 1)	✓
	PCAP Replay - MyDoom SMTP communication	✓

Recommendations & Mitigations

Below are recommendations and mitigation strategies for any scenario that was not prevented. Where applicable, both AttackIQ and MITRE ATT&CK recommendations and mitigations are included.

Note: Sigma Rules and MITRE ATT&CK Mitigations contain third-party links.

Glossary

AttackIQ Security Prevention Effectiveness Scoring System: Calculated by measuring the prevention capability across all test points.

Attack Technique: Tactics, techniques and procedures (TTPs) that have been used by a threat actor.

Global Security Prevention Effectiveness Index: Calculated by taking the AttackIQ Security Prevention Effectiveness Score of all accessible AttackIQ customers, redacting the data and creating a score based off of the global average.

Mitigation: Steps that are recommended for each of the identified vulnerabilities. These are provided as general guidelines and may not be applicable in each customer’s specific use case.

AIQ Generic Mitigation: Asset-agnostic recommendations designed to address potential risks or vulnerabilities, not tied to specific assets, and encompassing a wide range of generic security strategies.

Prevention Rate: A calculation based on the total number of test points that prevented a scenario from successfully completing its final action (based on the scenarios success criteria).

Scenario: A set of TTPs that have been employed by the attacker.

Security Control Test Suite: A set of scenarios.

Security Control Testing Suite Prevention Rate: (See Prevention Rate).

Test: An atomic adversary technique that can map to a MITRE ATT&CK tactic and has been purpose-built with specific procedural parameters.

Test Point Prevention Capability: The indicator that describes whether the AttackIQ Test Point prevented an AttackIQ scenario from completing its final action based on the scenarios success criteria.