Technical

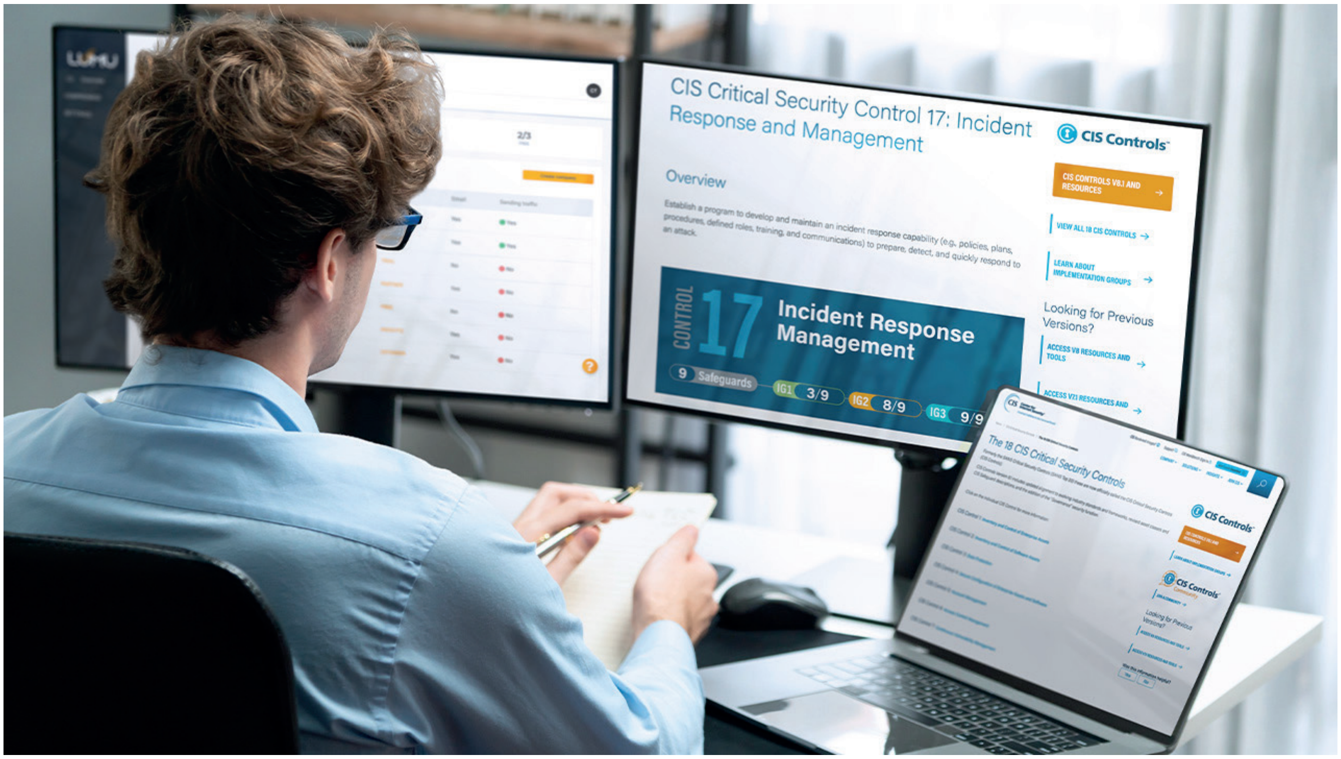
Lumu CIS Compliance Enablement for MSPs

Index

Accelerating Technology Adoption in SLED

What Is CIS?

The Center for Internet Security (CIS) is a nonprofit organization dedicated to improving cyber defense by creating and promoting best practices. They collaborate with cybersecurity and IT experts from government, business, and academia worldwide to develop their standards. These guidelines are established through a consensus-driven process, ensuring they reflect the collective expertise and experience of the global cybersecurity community.


CIS Critical Security Control 17: Incident Response and Management
Overview
CIS Controls
CONTROL 17 Incident Response Management
9 Safeguards
IG1 3/9
IG2 8/9
IG3 9/9
Looking for Previous Versions?
The 18 CIS Critical Security Controls

The CIS provides a set of globally recognized best practices known as CIS Controls, designed to enhance cybersecurity by mitigating common threats. These controls are categorized into basic, foundational, and organizational groups, which help organizations improve their security posture through prioritized and actionable guidance. Compliance with CIS simplifies regulatory compliance, enhances risk management, and optimizes resource allocation.

The Importance of CIS Compliance for MSPs

As cyber threats escalate, businesses increasingly rely on MSPs for IT support and cybersecurity needs. However, this reliance also heightens the risk of cyber-attacks, as MSPs become attractive targets due to their access to multiple clients' systems. Cybercriminals frequently target MSPs, over the last two years, ransomware attacks against MSPs have risen approximately 94%.

Additionally, many Cyber-insurers are beginning to require that MSPs comply with CIS regulations as a condition for coverage. This mandate comes as insurers recognize the critical role MSPs play in safeguarding their clients' IT infrastructure and data. By enforcing CIS Compliance, insurers aim to mitigate cyber risks and reduce the likelihood of costly claims, thereby providing better protection for their clients' IT infrastructure and data.

The CIS framework, with its straightforward language and 18 high-priority best practice categories, is accessible and crucial for developing a formalized security program. By following CIS guidelines and leveraging security automation, MSPs can simplify the management of cybersecurity risks and protect their clients' data and systems.

Mapping Lumu to CIS Controls

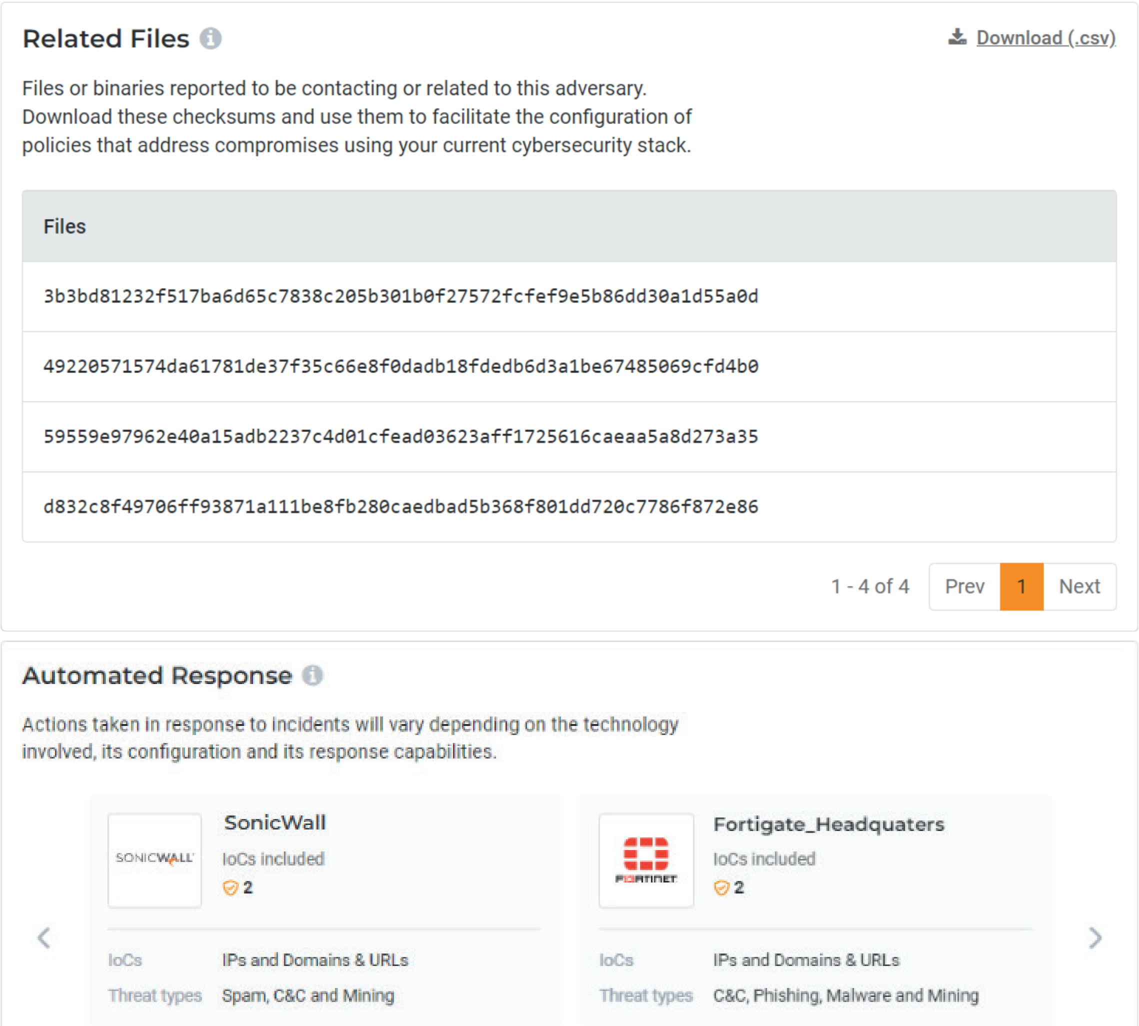
There is no single technology that will check all 18 CIS controls, however, Lumu helps MSPs check some of these critical requirements through its extensive visibility and automated response capabilities. Below we've highlighted where Lumu's capabilities help **cover some aspects of CIS Controls** and others which **enable full compliance with CIS controls.** All are mapped as follows:

These are the controls where Lumu helps cover **some requirements** with its capabilities:

Control 4: Secure Configuration of Enterprise Assets and Software

Control requirement: Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Lumu's Approach: Lumu helps with the security and management of Firewalls and DNS servers by automatically detecting threats and sending threat data directly to these tools for real-time action. Through this continuous process, Lumu ensures that an organization's enterprise assets are blocking the latest threats targeting the organization.



Related Files

Files or binaries reported to be contacting or related to this adversary. Download these checksums and use them to facilitate the configuration of policies that address compromises using your current cybersecurity stack.

Files
3b3bd81232f517ba6d65c7838c205b301b0f27572fcfef9e5b86dd30a1d55a0d
49220571574da61781de37f35c66e8f0dadb18fdedb6d3a1be67485069cfd4b0
59559e97962e40a15adb2237c4d01cfead03623aff1725616caeaa5a8d273a35
d832c8f49706ff93871a111be8fb280caedbad5b368f801dd720c7786f872e86

1 - 4 of 4

Automated Response

Actions taken in response to incidents will vary depending on the technology involved, its configuration and its response capabilities.

SonicWall
IoCs included
2

IoCs	IPs and Domains & URLs
Threat types	Spam, C&C and Mining

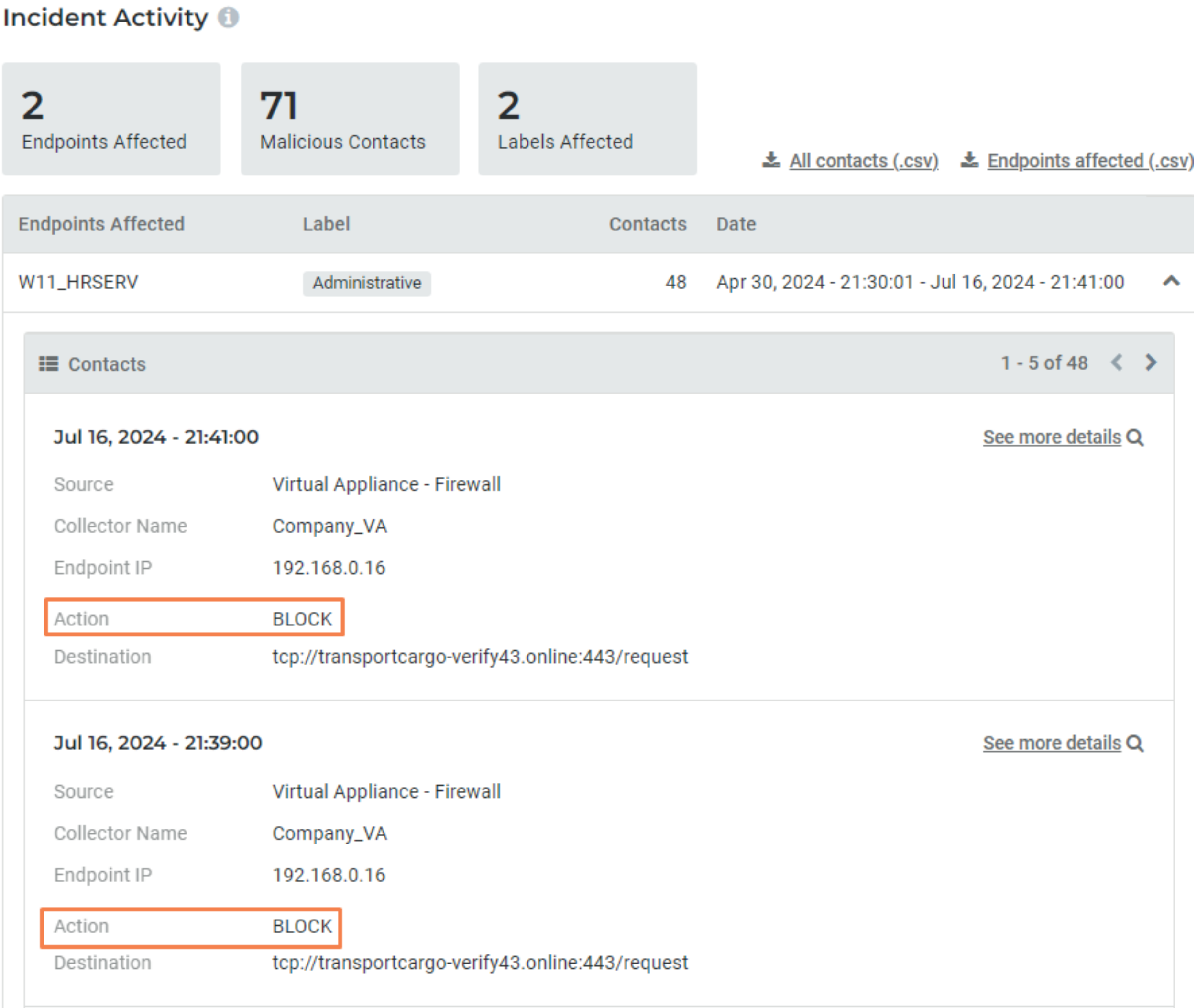
Fortigate_Headquaters
IoCs included
2

IoCs	IPs and Domains & URLs
Threat types	C&C, Phishing, Malware and Mining

Control 9: CIS Control 9: Email and Web Browser Protections

Control requirement: Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Lumu's approach: With its ability to automatically feed malicious URLs, enhance DNS filtering, and feed IoC data in real-time, Lumu proactively blocks threats targeting an organization. This stops threat actors from carrying out their attacks and protects users automatically. Blocked actions are shown in the Lumu portal, highlighting which devices were blocked and when.



Incident Activity

2 Endpoints Affected

71 Malicious Contacts

2 Labels Affected

Endpoints Affected	Label	Contacts	Date
W11_HRSERV	Administrative	48	Apr 30, 2024 - 21:30:01 - Jul 16, 2024 - 21:41:00

Contacts 1 - 5 of 48

Jul 16, 2024 - 21:41:00

Source	Virtual Appliance - Firewall
Collector Name	Company_VA
Endpoint IP	192.168.0.16
Action	BLOCK
Destination	tcp://transportcargo-verify43.online:443/request

Jul 16, 2024 - 21:39:00

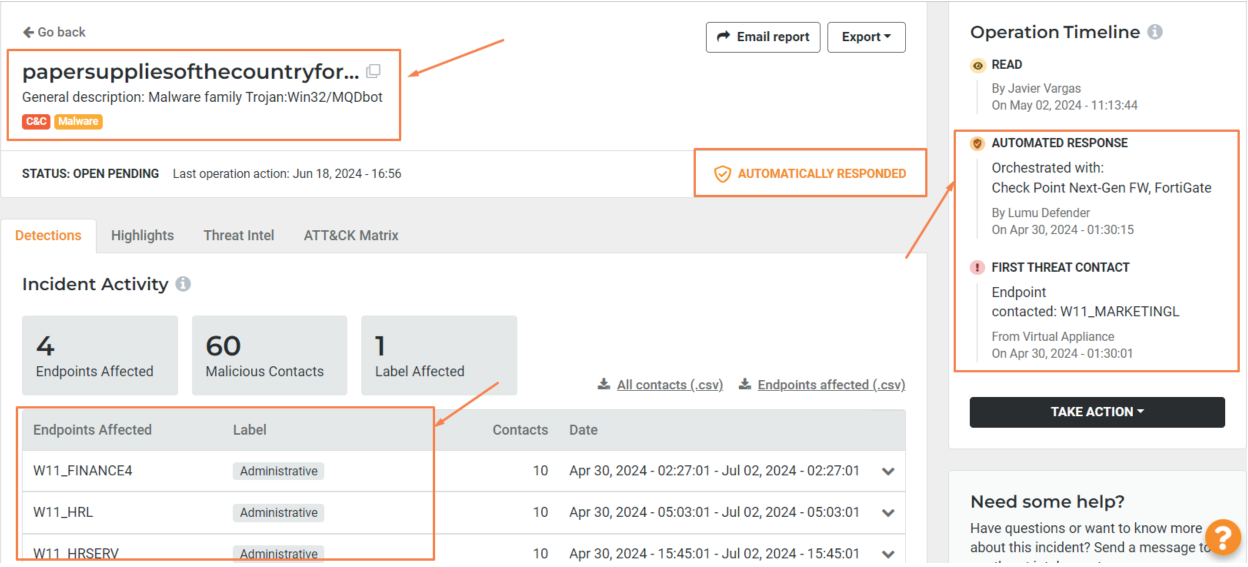
Source	Virtual Appliance - Firewall
Collector Name	Company_VA
Endpoint IP	192.168.0.16
Action	BLOCK
Destination	tcp://transportcargo-verify43.online:443/request

These are the controls where Lumu provides **full compliance** with its capabilities:

Control 10: Malware Defenses

Control Requirement: Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Lumu's Approach: Lumu detects malware related incidents on any device and automatically reports and blocks different types of malware and precursor ransomware in real-time. All details around endpoints affected and the behavior of a particular instance of malware can be found in the incident details.



papersuppliesofthecountryfor...

General description: Malware family Trojan:Win32/MQDbot

C&C Malware

STATUS: OPEN PENDING Last operation action: Jun 18, 2024 - 16:56

AUTOMATICALLY RESPONDED

Incident Activity

4 Endpoints Affected

60 Malicious Contacts

1 Label Affected

Endpoints Affected	Label	Contacts	Date
W11_FINANCE4	Administrative	10	Apr 30, 2024 - 02:27:01 - Jul 02, 2024 - 02:27:01
W11_HRL	Administrative	10	Apr 30, 2024 - 05:03:01 - Jul 02, 2024 - 05:03:01
W11_HRSERV	Administrative	10	Apr 30, 2024 - 15:45:01 - Jul 02, 2024 - 15:45:01

Operation Timeline

READ
By Javier Vargas
On May 02, 2024 - 11:13:44

AUTOMATED RESPONSE
Orchestrated with:
Check Point Next-Gen FW, FortiGate
By Lumu Defender
On Apr 30, 2024 - 01:30:15

FIRST THREAT CONTACT
Endpoint
contacted: W11_MARKETINGL
From Virtual Appliance
On Apr 30, 2024 - 01:30:01

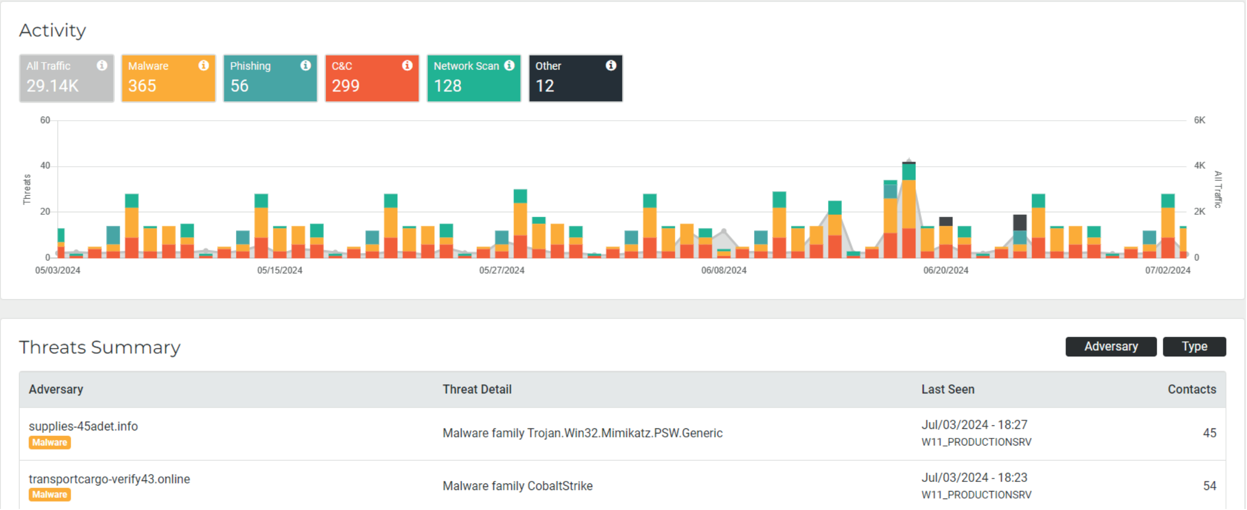
Need some help?

Have questions or want to know more about this incident? Send a message to

Control 13: Network Monitoring and Defense

Control Requirement: Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Lumu's Approach: Lumu works 24x7x365 monitoring the entire network for any unusual activity. Lumu is able to monitor all devices connected to the network, without the need for an agent. With every aspect of the network taken into account, Lumu is able to investigate unusual activity to identify active threats and stop them in real-time using existing perimeter defenses and endpoint tools. All activity is tracked and reported in detail. Incidents discovered by Lumu may also be sent to existing SecOps and PSA tools for further investigation.



Activity

All Traffic	Malware	Phishing	C&C	Network Scan	Other
29.14K	365	56	299	128	12

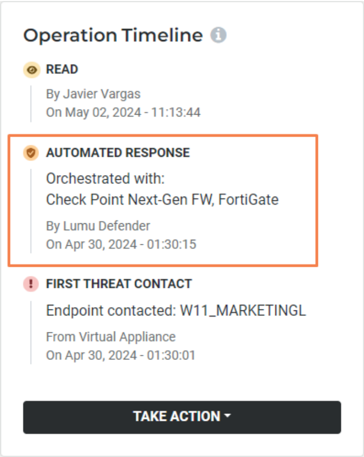
Threats Summary

Adversary	Threat Detail	Last Seen	Contacts
supplies-45adet.info Malware	Malware family Trojan.Win32.Mimikatz.PSW.Generic	Jul/03/2024 - 18:27 W11_PRODUCTIONSRV	45
transportcargo-verify43.online Malware	Malware family CobaltStrike	Jul/03/2024 - 18:23 W11_PRODUCTIONSRV	54

Control 17: Incident Response and Management

Control Requirement: Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Lumu's Approach: With hundreds of product integrations available, Lumu responds to incidents in real-time, without the need for human intervention. Once a threat is detected, actions are automatically taken to stop the adversary before any damage occurs. All incidents can be managed within the Lumu portal.

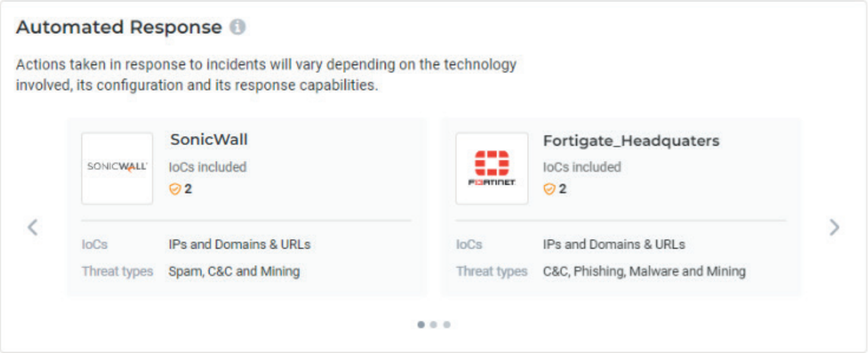


Operation Timeline

READ
By Javier Vargas
On May 02, 2024 - 11:13:44

AUTOMATED RESPONSE
Orchestrated with:
Check Point Next-Gen FW, FortiGate
By Lumu Defender
On Apr 30, 2024 - 01:30:15

FIRST THREAT CONTACT
Endpoint contacted: W11_MARKETINGL
From Virtual Appliance
On Apr 30, 2024 - 01:30:01

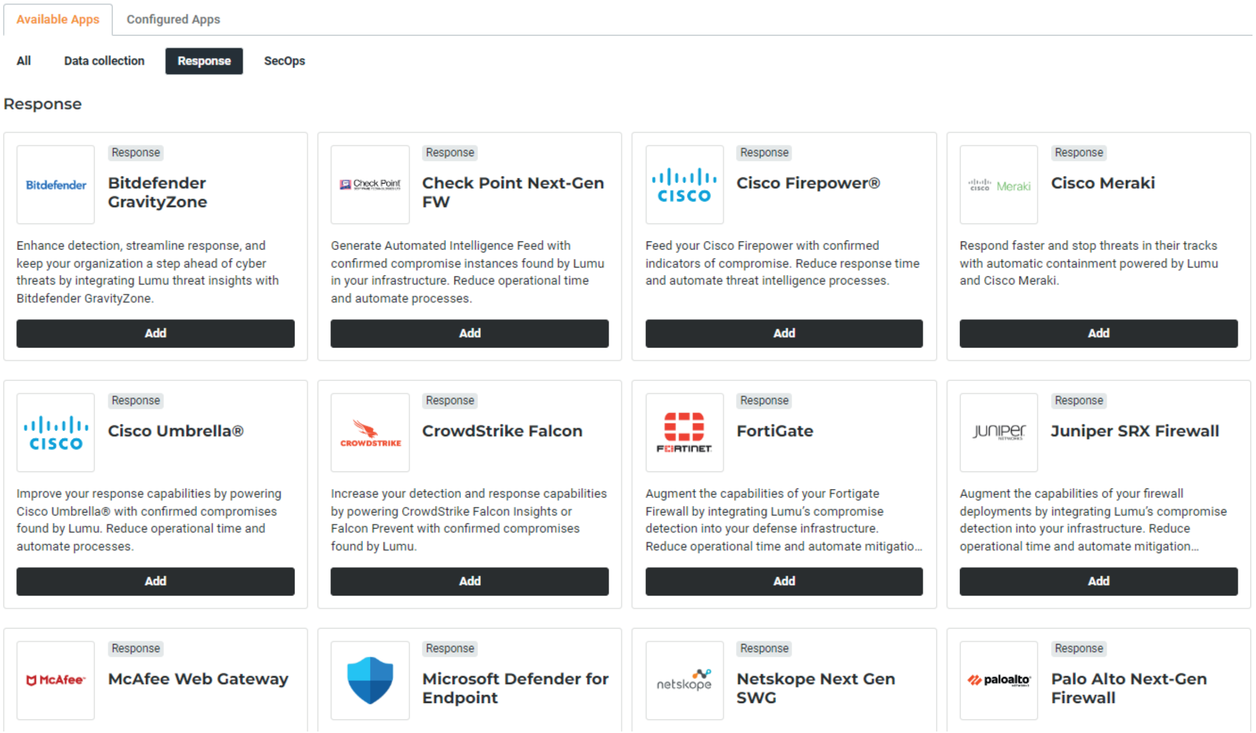


Automated Response

Actions taken in response to incidents will vary depending on the technology involved, its configuration and its response capabilities.

SonicWall
IoCs included: 2
IoCs: IPs and Domains & URLs
Threat types: Spam, C&C and Mining

Fortigate_Headquaters
IoCs included: 2
IoCs: IPs and Domains & URLs
Threat types: C&C, Phishing, Malware and Mining



Response

Response	Bitdefender GravityZone	Enhance detection, streamline response, and keep your organization a step ahead of cyber threats by integrating Lumu threat insights with Bitdefender GravityZone.
Response	Check Point Next-Gen FW	Generate Automated Intelligence Feed with confirmed compromise instances found by Lumu in your infrastructure. Reduce operational time and automate processes.
Response	Cisco Firepower®	Feed your Cisco Firepower with confirmed indicators of compromise. Reduce response time and automate threat intelligence processes.
Response	Cisco Meraki	Respond faster and stop threats in their tracks with automatic containment powered by Lumu and Cisco Meraki.
Response	Cisco Umbrella®	Improve your response capabilities by powering Cisco Umbrella® with confirmed compromises found by Lumu. Reduce operational time and automate processes.
Response	CrowdStrike Falcon	Increase your detection and response capabilities by powering CrowdStrike Falcon Insights or Falcon Prevent with confirmed compromises found by Lumu.
Response	FortiGate	Augment the capabilities of your Fortigate Firewall by integrating Lumu's compromise detection into your defense infrastructure. Reduce operational time and automate mitigatio...
Response	Juniper SRX Firewall	Augment the capabilities of your firewall deployments by integrating Lumu's compromise detection into your infrastructure. Reduce operational time and automate mitigation...
Response	McAfee Web Gateway	
Response	Microsoft Defender for Endpoint	
Response	Netskope Next Gen SWG	
Response	Palo Alto Next-Gen Firewall	

Get Started with Lumu

Though being fully compliant with CIS may seem like a daunting task, the best approach is to handle it a few steps at a time. Lumu offers a free solution for MSPs including up to 3 tenants, with 3 integrations (including integrations for data collection, response, and security operations), and up to 50 endpoints. To learn more about how Lumu can help achieve compliance with CIS and to get started with Lumu, access our MSP page.