Test Longevity Box - Weekly Report

Account Settings

Update Account Information

Contacts

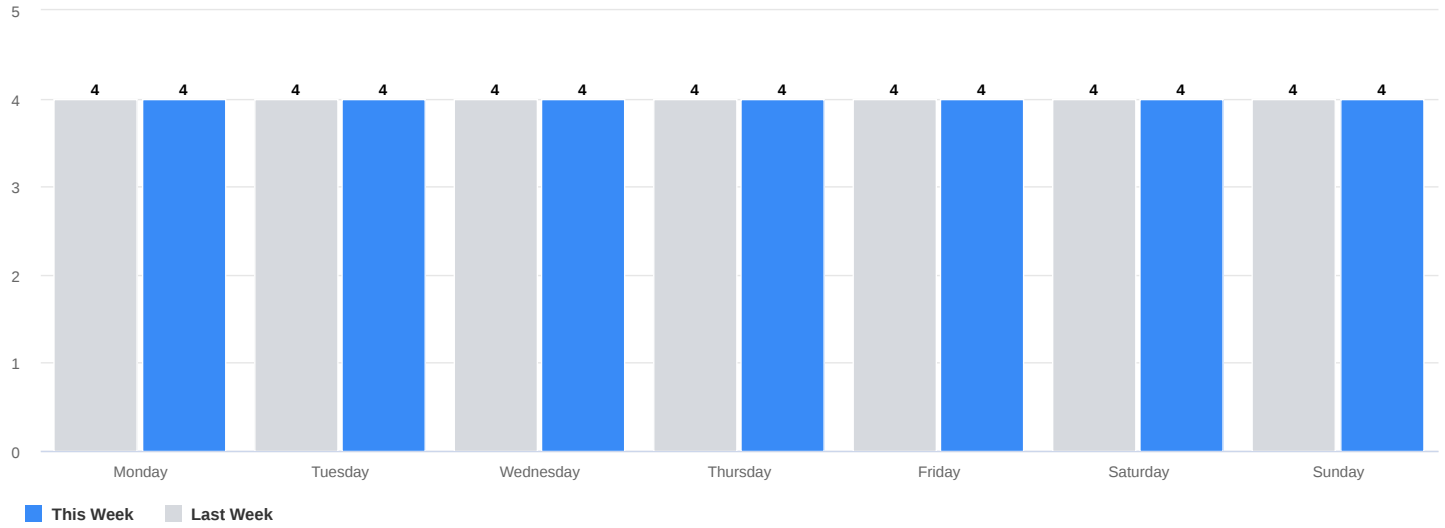
kevhulk67+test223@gmail.com
saitestsophos+638@gmail.com
shaq@gmail.com

Response Mode

Authorize

Devices Sending Telemetry

View All



Sophos MDR Cases

Total Cases: 24 View All

Cases by Status

0 View New	24 View In Progress	0 View Action Required	0 View Resolved/Closed

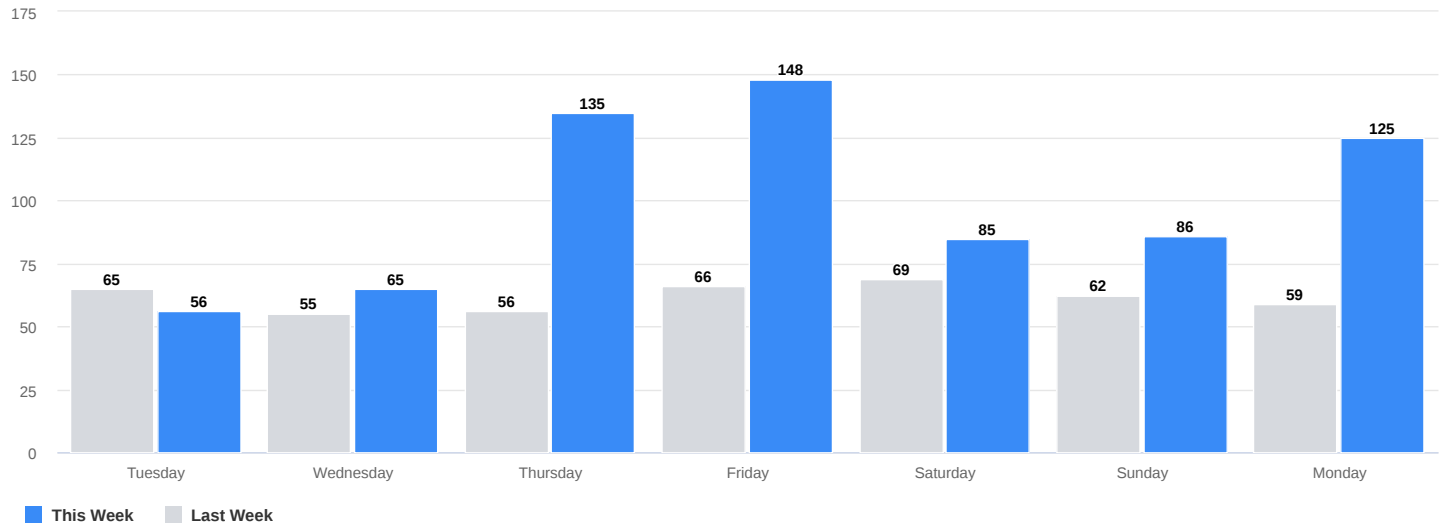
Cases by Type

24 View MDR Investigation	0 View Health Check	0 View Customer Requested Investigation

Sophos Detections

Detections This Week

View All



Test Longevity Box - Weekly Report

Account Settings

Update Account Information

Contacts

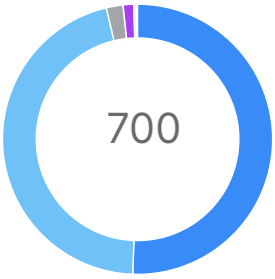
kevhulk67+test223@gmail.com
saitestsophos+638@gmail.com
shaq@gmail.com

Response Mode

Authorize

Detection Classification Summary

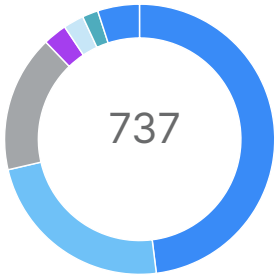
View More



Cloud Metadata API Accessed	354
Suspicious Activity	320
Process Dumping via Proc Detected	14
Systemd Service Modified	9
New File Executed	2
Interactive Shell Session Started	1

MITRE ATT&CK Framework

View More



Unsecured Credentials.Cloud Instance Metadata API	354
Hidden Files and Directories	172
Match Legitimate Name or Location	121
Data Encrypted for Impact	21
Create or Modify System Process.Systemd Service	18
OS Credential Dumping.Proc Filesystem	14
All Other Techniques	37

MDR Integrations with Detections

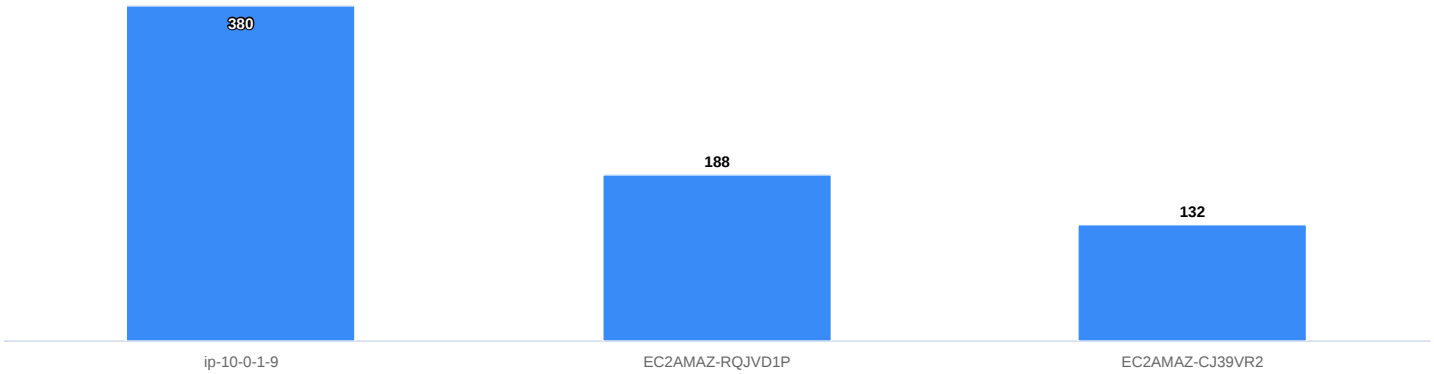
View More

MDR integrations with events that matched rules to generate detections for this week.

Endpoint

Sophos Endpoint 700

Top 10 Devices with Most Detections



Test Longevity Box - Weekly Report

Account Settings

Update Account Information

Contacts

kevhulk67+test223@gmail.com
saitestsophos+638@gmail.com
shaq@gmail.com

Response Mode

Authorize

Top 10 Devices with Most Detections

Hostname	Top Detections	Count	Category
ip-10-0-1-9	SPL-LNX-BEH-Cloud-Metadata-API-Accessed	354	Cloud Metadata API Accessed
	SPL-LNX-BEH-Process-Dumping-Via-Proc	14	Process Dumping via Proc Detected
	SPL-LNX-BEH-Systemctl-Usage-Detected	8	Systemd Service Modified
EC2AMAZ-RQJVD1P	WIN-MITRE-Behavioral-TA0005-T1036.005	121	Suspicious Activity
	WIN-MITRE-Behavioral-TA0005-T1564.001	46	Suspicious Activity
	WIN-MITRE-Behavioral-TA0040-T1486	21	Suspicious Activity
EC2AMAZ-CJ39VR2	WIN-MITRE-Behavioral-TA0005-T1564.001	126	Suspicious Activity
	WIN-MITRE-Behavioral-TA0009-T1119	6	Suspicious Activity

Top 5 Detections

Detection Name	Count	Description	Category
SPL-LNX-BEH-Cloud-Metadata-API-Accessed	354	Attackers commonly enumerate cloud environment details and gain access to instance credentials by accessing the...	Cloud Metadata API Accessed
WIN-MITRE-Behavioral-TA0005-T1564.001	172	-	Suspicious Activity
WIN-MITRE-Behavioral-TA0005-T1036.005	121	-	Suspicious Activity
WIN-MITRE-Behavioral-TA0040-T1486	21	-	Suspicious Activity
SPL-LNX-BEH-Process-Dumping-Via-Proc	14	Adversaries may inject malicious code into processes via the /proc filesystem in order to evade process-based...	Process Dumping via Proc Detected

Bottom 5 Detections

Detection Name	Count	Description	Category
SPL-LNX-BEH-Interactive-Shell-Tagger	1	Adds interactive shell and suspicious command tracking tags to interactive shell programs.	Interactive Shell Session Started
SPL-LNX-BEH-Systemd-Unit-File-Modified	1	Changes to systemd units could result in security controls being relaxed or disabled, or the installation of a malicious...	Systemd Service Modified
SPL-LNX-BEH-New-File-Executed	2	Newly created files from sources other than system update programs may be backdoors, kernel exploits, or part of an...	New File Executed
WIN-MITRE-Behavioral-TA0009-T1119	6	-	Suspicious Activity
SPL-LNX-BEH-Systemctl-Usage-Detected	8	Changes to systemd units could result in security controls being relaxed or disabled, or the installation of a malicious...	Systemd Service Modified

Account Settings

Update Account Information

Contacts

kevhulk67+test223@gmail.com
saitestsophos+638@gmail.com
shaq@gmail.com

Response Mode

Authorize

Additional Sophos MDR Efforts

Recent Response Actions

Date & Time	Case #	Analyst	Action	Result
02/28/2023 03:02 GMT	35089	saitestsophos@gmail.com	DEVICE_ACTION_CREATED	upload_threat_file performed on EC2AMAZ-CJ39VR2 (status: success)
02/28/2023 03:02 GMT	35089	saitestsophos@gmail.com	DEVICE_ACTION_CREATED	download_file performed on EC2AMAZ-CJ39VR2 (status: fail)
02/27/2023 21:54 GMT	35089	saitestsophos@gmail.com	DEVICE_ACTION_CREATED	upload_threat_file performed on EC2AMAZ-CJ39VR2 (status: success)
02/27/2023 21:54 GMT	35089	saitestsophos@gmail.com	DEVICE_ACTION_CREATED	download_file performed on EC2AMAZ-CJ39VR2 (status: fail)
02/27/2023 20:21 GMT	35089	saitestsophos@gmail.com	DEVICE_ACTION_CREATED	upload_threat_file performed on EC2AMAZ-CJ39VR2 (status: success)

Recent Communications

Date & Time	Case #	Analyst	Action	Result
02/27/2023 21:56 GMT	35089	saitestsophos@gmail.com	Sent a message	sent through Automation for testing message send functionality Mr. Sai Test user | sophos (888) 201-7672 | saitestsophos@gmail.com
02/27/2023 20:22 GMT	35089	saitestsophos@gmail.com	Sent a message	sent through Automation for testing message send functionality Mr. Sai Test user | sophos (888) 201-7672 | saitestsophos@gmail.com
02/27/2023 03:04 GMT	35089	saitestsophos@gmail.com	Sent a message	sent through Automation for testing message send functionalityThis comment is sent through Automation for testing new comment add...
02/26/2023 03:04 GMT	35089	saitestsophos@gmail.com	Sent a message	sent through Automation for testing message send functionality Mr. Sai Test user | sophos (888) 201-7672 | saitestsophos@gmail.com
02/25/2023 03:04 GMT	35089	saitestsophos@gmail.com	Sent a message	sent through Automation for testing message send functionality Mr. Sai Test user | sophos (888) 201-7672 | saitestsophos@gmail.com