Test Longevity Box - Monthly Report

Account Settings

Update Account Information

Contacts

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

Response Mode

Authorize

Sophos MDR Protection Rating

Needs Attention

You have not implemented all required settings for optimal functionality.

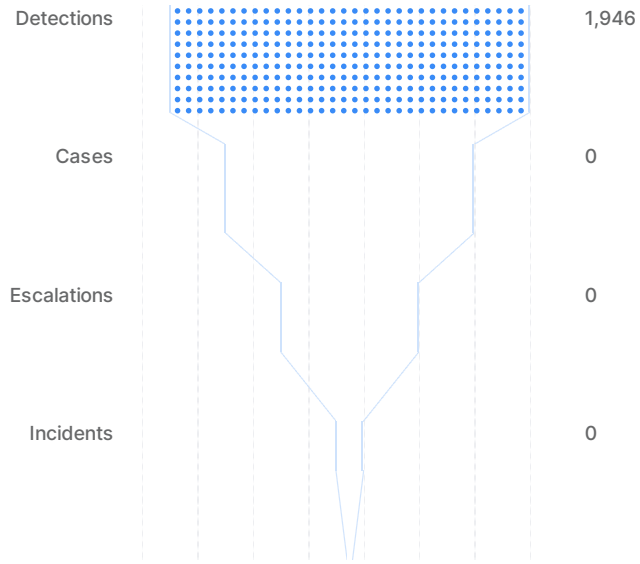
Learn more

Total Licenses Deployed

4 out of 99

You have 95 unused licenses.

Event Pipeline



Sophos MDR Cases

Total Cases: 94 View All

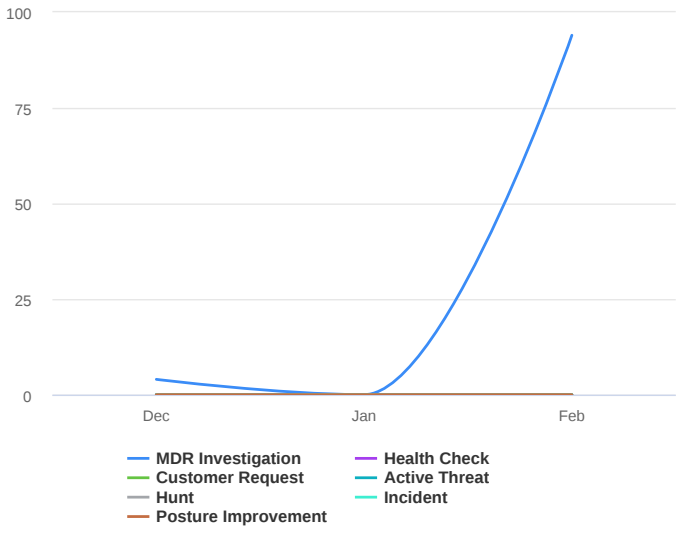
Cases by Status

New	In Progress	Action Required	Resolved/Closed
0 View	92 View	0 View	2 View

Cases by Type

MDR Investigation	Health Check	Customer Request	Active Threat
98 View	0 View	0 View	0 View

Hunt	Incident	Posture Improvement
0 View	0 View	0 View



Case Activity by Detection Source

Insufficient Threats

We didn't see enough adversarial behavior to generate a useful chart. This is a good thing.

Test Longevity Box - Monthly Report

Account Settings

Update Account Information

Contacts

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

Response Mode

Authorize

Case Activity

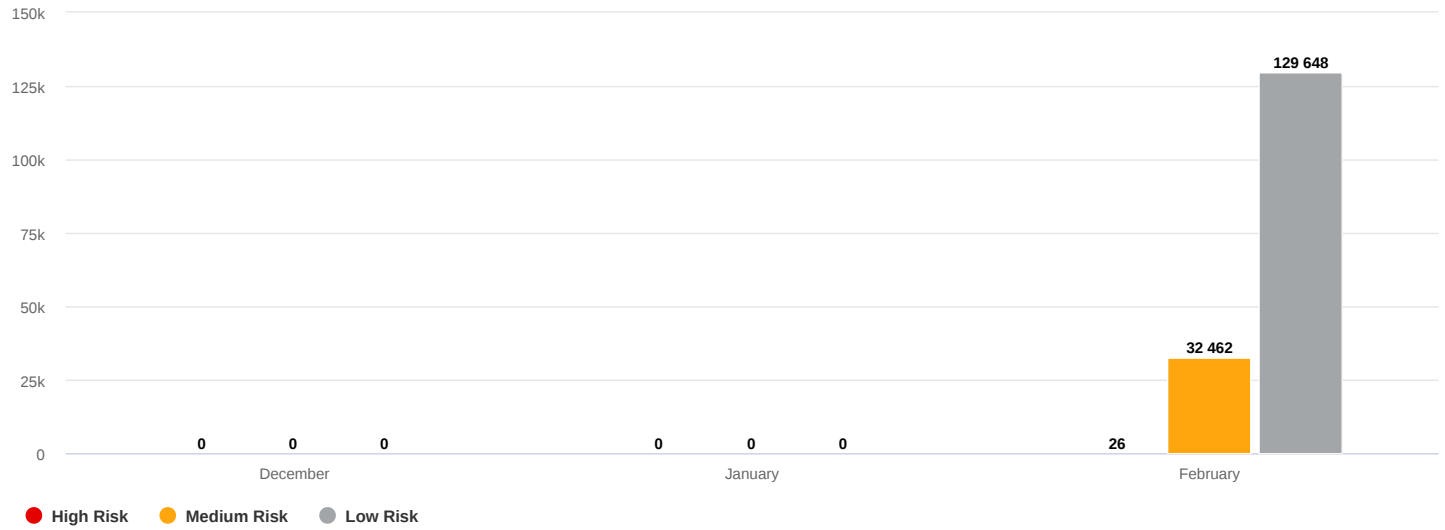
View All

Case Number	Case Type	Case Description	Status
#162225	Investigation	case to save 02/03/2023-Feb 3, 2023 at 03:01 AM	In Progress
Synopsis	only for automated testing on 02/03/2023		
#162226	Investigation	case to save & go 02/03/2023-Feb 3, 2023 at 03:02 AM	In Progress
Synopsis	only for automated testing on 02/03/2023		
#162237	Investigation	case to save 02/03/2023-Feb 3, 2023 at 06:35 PM	In Progress
Synopsis	only for automated testing on 02/03/2023		
#162238	Investigation	case to save & go 02/03/2023-Feb 3, 2023 at 06:35 PM	In Progress
Synopsis	only for automated testing on 02/03/2023		
#162239	Investigation	case to save 02/03/2023-Feb 3, 2023 at 06:53 PM	In Progress
Synopsis	only for automated testing on 02/03/2023		
#162240	Investigation	case to save & go 02/03/2023-Feb 3, 2023 at 06:53 PM	In Progress
Synopsis	only for automated testing on 02/03/2023		
#171491	Investigation	case to save 02/15/2023-Feb 23, 2023 at 12:00 AM	Resolved
Synopsis	only for automated testing on 02/15/2023		
#171520	Investigation	case to save 02/15/2023-Feb 15, 2023 at 05:45 PM	In Progress
Synopsis	only for automated testing on 02/15/2023		
#171492	Investigation	case to save & go 02/15/2023-Feb 15, 2023 at 06:09 PM	In Progress
Synopsis	only for automated testing on 02/15/2023		
#171521	Investigation	case to save & go 02/15/2023-Feb 15, 2023 at 06:08 PM	In Progress
Synopsis	only for automated testing on 02/15/2023		

Sophos Detections

Total Detections

View All



Test Longevity Box - Monthly Report

Account Settings

Update Account Information

Contacts

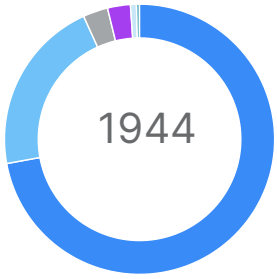
kevhulk67+test223@gmail.com
saitestsophos+638@gmail.com
shaq@gmail.com

Response Mode

Authorize

Detection Classification Summary

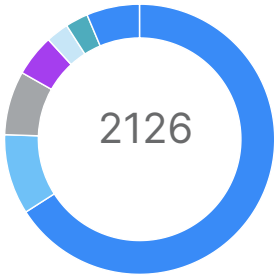
View More



Cloud Metadata API Accessed	1402
Suspicious Activity	410
Process Dumping via Proc Detected	58
Systemd Service Modified	53
Remote File Copy Detected	14
New File Executed	7
All Other Classifications	2

MITRE ATT&CK Framework

View More



Unsecured Credentials.Cloud Instance Metadata API	1402
Hidden Files and Directories	204
Match Legitimate Name or Location	163
Create or Modify System Process.Systemd Service	106
OS Credential Dumping.Proc Filesystem	58
Process Injection.Proc Memory	58
All Other Techniques	135

MDR Integrations with Detections

View More

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

Endpoint

Sophos Endpoint 1946

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)

Account Settings

Update Account Information

Contacts

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

Response Mode

Authorize

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