Center for Internet Security®

CIS Services

Jeff Sparks
Sr. Account Executive – East

12/27/23

Proprietary

CIS Services

Table of Contents

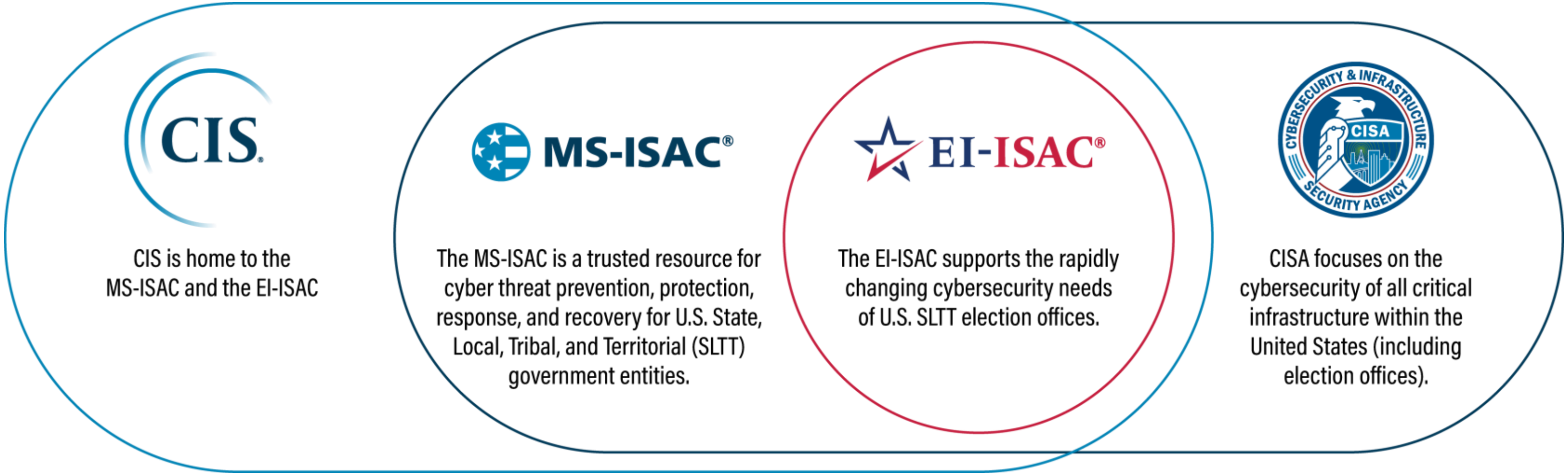
Center for Internet Security®

Who We Are

Proprietary

Center for Internet Security

Nonprofit leading the global community to secure our connected world



CIS is home to the MS-ISAC and the EI-ISAC

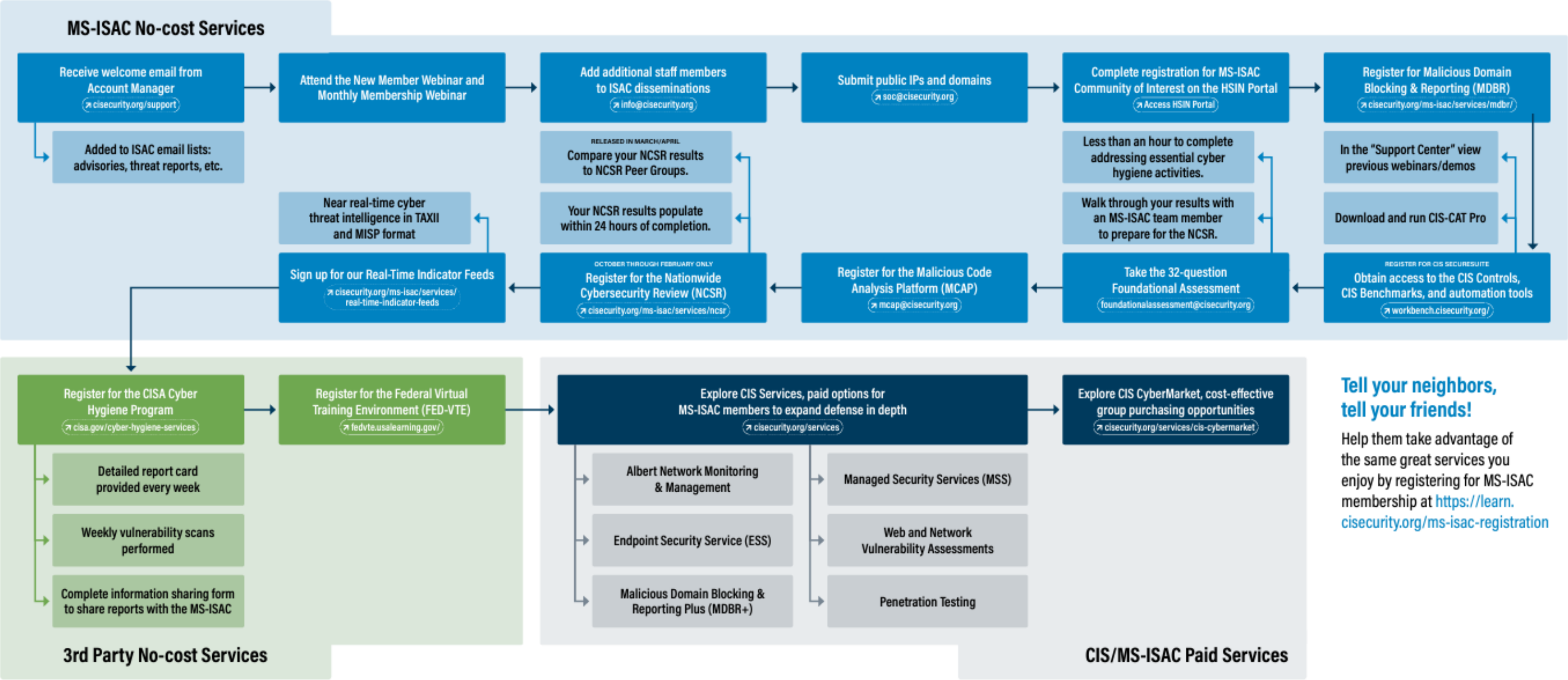
The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.

The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.

CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).

CIS “Placemat”

Flowchart CIS-MS-ISAC → CISA → to CIS Services



MS-ISAC No-cost Services

Receive welcome email from Account Manager
↗ cisecurity.org/support

Added to ISAC email lists: advisories, threat reports, etc.

Attend the New Member Webinar and Monthly Membership Webinar

Add additional staff members to ISAC disseminations
↗ info@cisecurity.org

Submit public IPs and domains
↗ soc@cisecurity.org

Complete registration for MS-ISAC Community of Interest on the HSIN Portal
↗ Access HSIN Portal

Register for Malicious Domain Blocking & Reporting (MDBR)
↗ cisecurity.org/ms-isac/services/mdbr/

REGISTER FOR CIS SECURESUITE
Obtain access to the CIS Controls, CIS Benchmarks, and automation tools
↗ workbench.cisecurity.org/

In the “Support Center” view previous webinars/demos

Download and run CIS-CAT Pro

Take the 32-question Foundational Assessment
foundationalassessment@cisecurity.org

Less than an hour to complete addressing essential cyber hygiene activities.

Walk through your results with an MS-ISAC team member to prepare for the NCSR.

Register for the Malicious Code Analysis Platform (MCAP)
↗ mcap@cisecurity.org

OCTOBER THROUGH FEBRUARY ONLY
Register for the Nationwide Cybersecurity Review (NCSR)
↗ cisecurity.org/ms-isac/services/ncsr

RELEASED IN MARCH/APRIL
Compare your NCSR results to NCSR Peer Groups.

Your NCSR results populate within 24 hours of completion.

Sign up for our Real-Time Indicator Feeds
↗ cisecurity.org/ms-isac/services/real-time-indicator-feeds

Near real-time cyber threat intelligence in TAXII and MISP format

3rd Party No-cost Services

Register for the CISA Cyber Hygiene Program
↗ cisa.gov/cyber-hygiene-services

Detailed report card provided every week

Weekly vulnerability scans performed

Complete information sharing form to share reports with the MS-ISAC

Register for the Federal Virtual Training Environment (FED-VTE)
↗ fedvte.usalearning.gov/

CIS/MS-ISAC Paid Services

Explore CIS Services, paid options for MS-ISAC members to expand defense in depth
↗ cisecurity.org/services

Albert Network Monitoring & Management

Endpoint Security Service (ESS)

Malicious Domain Blocking & Reporting Plus (MDBR+)

Managed Security Services (MSS)

Web and Network Vulnerability Assessments

Penetration Testing

Explore CIS CyberMarket, cost-effective group purchasing opportunities
↗ cisecurity.org/services/cis-cybermarket

Tell your neighbors, tell your friends!

Help them take advantage of the same great services you enjoy by registering for MS-ISAC membership at https://learn.cisecurity.org/ms-isac-registration

Center for Internet Security®

CIS 24x7x365 Security Operations Center (SOC)

Proprietary

CIS Security Operations Center (SOC)

24x7x365 Support

Support

SLTT Security Experts
+
On Call All Day, Every Day
+
Full-time Cyber Defense Partner

Analysis & Monitoring

Round-the-clock Monitoring
+
Leverage Largest SLTT Cyber Threat Database

Reporting

Industry-leading Response Times
+
Eliminate ~75% of False Positives
+
Saves Security Teams Time, Effort

"The MS-ISAC is a critical partner to our cybersecurity program, with the SOC serving as an extension of our internal team to provide the additional eyes and ears to aid in detection and response efforts…"

– a state CISO

EXIT

Cyber Incident Response Team (CIRT)

Cyber Incident Response Team (CIRT)

Supporting SLTTs Through Incidents

- Incident Response
- Malware Analysis
- Log Analysis

Expert Support When Organizations Need It Most

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

What is Cyber Incident Response?

Elements of Cyber Incident Response

Elements of Cyber Incident Response
Log Review
Device Triage
Monitoring
Mitigation

Goals of Cyber Incident Response
Scope of Impact
Incident Timeline
Root Cause
Remediation Recommendations

Albert Network Monitoring and Management

Proprietary

Albert Network Monitoring and Management

Features

High Performance IDS Engine

Efficient Storage/ Analysis of Historical Data NetFlow

Robust Threat Intelligence ~25k+ signatures on average

24x7x365 SOC Monitoring, No-Cost Incident Response

Industry-leading Response Times

Albert Network Monitoring and Management

Business Drivers

Rapid Alert Escalation

Under
5 minutes
from alert to notification

Updated Signature Sets

~25k+ signatures updated daily to detect malicious activity

Cost Effective, Turnkey

Low-cost IDS solution with round-the-clock monitoring, management

Advanced Threat Monitoring

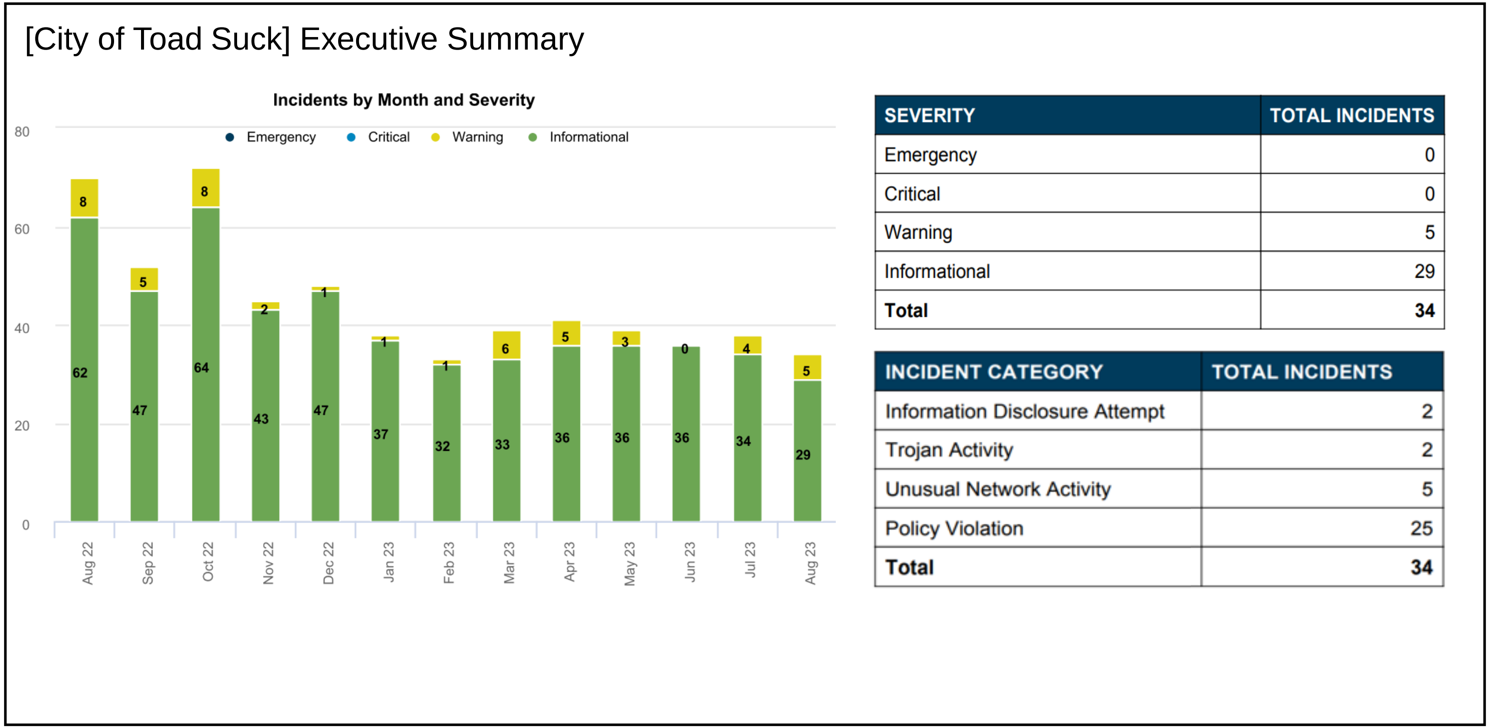
Monitor for traditional, advanced network threats

Monthly Activity Report (MAR)

Summary of Logged Activity

- **Nationwide Summary**
- **Agency Executive Summary**
- **Albert Event Summary**
  - Actionable events by severity
  - Ticket information
  - Generated events by severity YTD
  - Generated events by signature classification
  - Actionable events by signature classification
- **Albert Traffic Graphs**

MAR Reporting Sample



[City of Toad Suck] Executive Summary

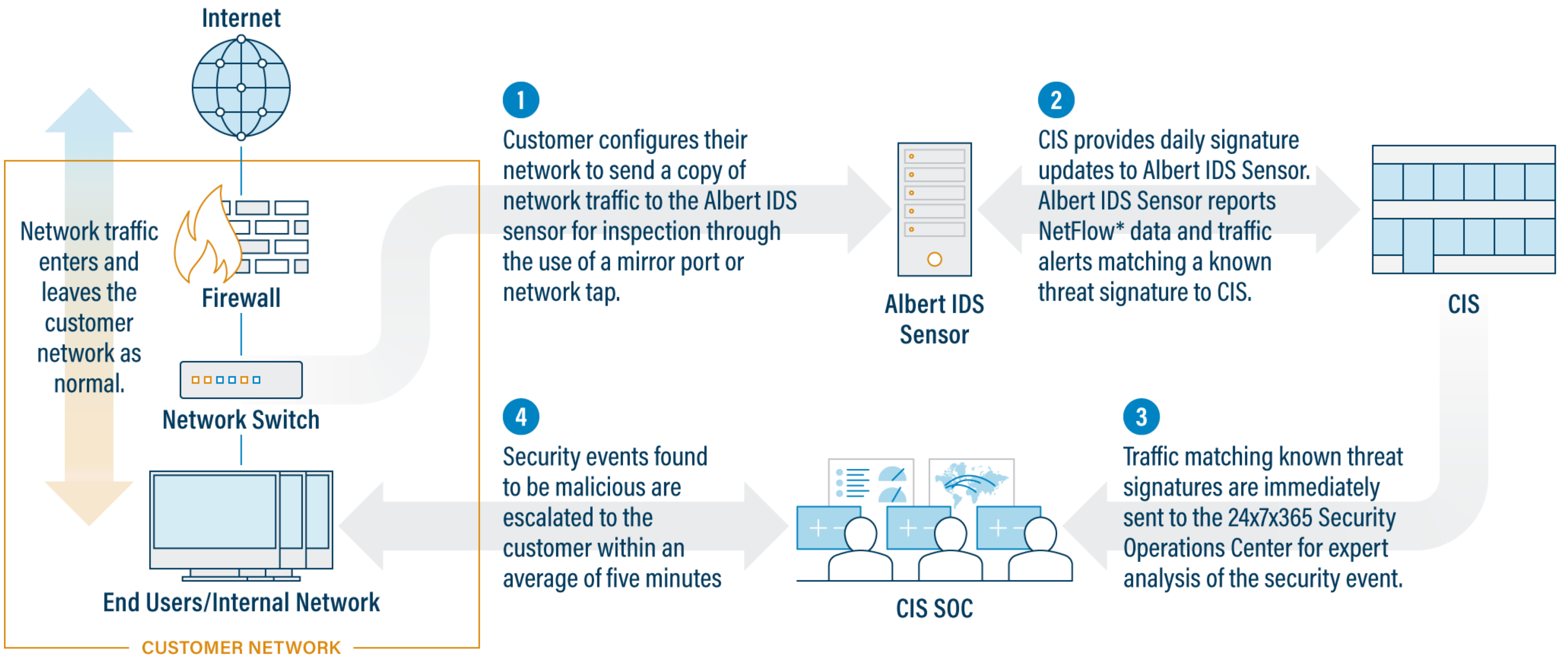
Incidents by Month and Severity

SEVERITY	TOTAL INCIDENTS
Emergency	0
Critical	0
Warning	5
Informational	29
Total	**34**

INCIDENT CATEGORY	TOTAL INCIDENTS
Information Disclosure Attempt	2
Trojan Activity	2
Unusual Network Activity	5
Policy Violation	25
Total	**34**

Albert in Action

Analyst Review



Internet
Network traffic enters and leaves the customer network as normal.
Firewall
Network Switch
End Users/Internal Network
CUSTOMER NETWORK
Albert IDS Sensor
CIS
CIS SOC

1. Customer configures their network to send a copy of network traffic to the Albert IDS sensor for inspection through the use of a mirror port or network tap.

2. CIS provides daily signature updates to Albert IDS Sensor. Albert IDS Sensor reports NetFlow* data and traffic alerts matching a known threat signature to CIS.

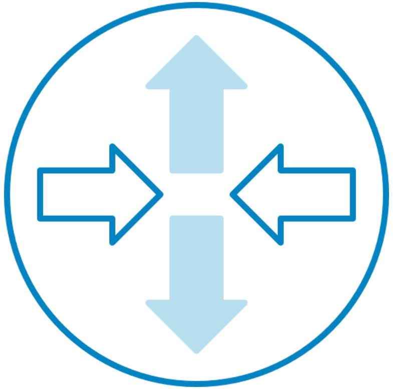
3. Traffic matching known threat signatures are immediately sent to the 24x7x365 Security Operations Center for expert analysis of the security event.

4. Security events found to be malicious are escalated to the customer within an average of five minutes

*NetFlow is a network protocol developed by Cisco for monitoring the flow and volume as well as collecting high-level metadata of IP traffic information as it passes in and out of a network interface.

Albert NetFlow

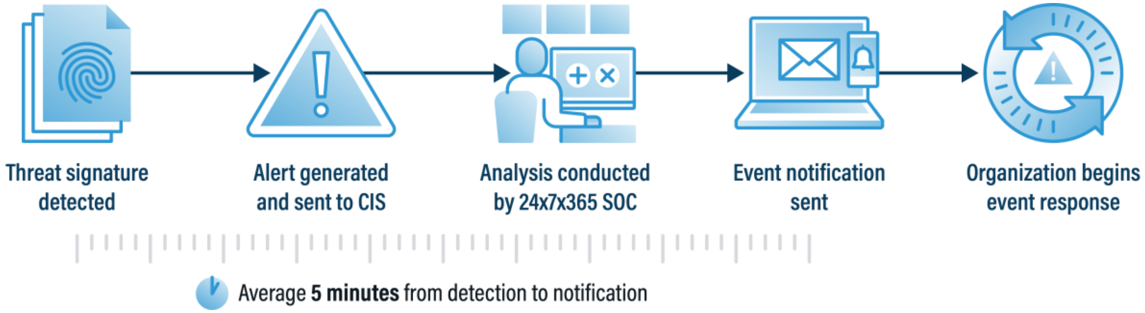
Unique Benefits of NetFlow



NetFlow

Metadata about network traffic

- NetFlow logging allows for retroactive detection of newly discovered threats
- Helps tell the story of when a network was first compromised
- NetFlow data retained for six months



Threat signature detected

Alert generated and sent to CIS

Analysis conducted by 24x7x365 SOC

Event notification sent

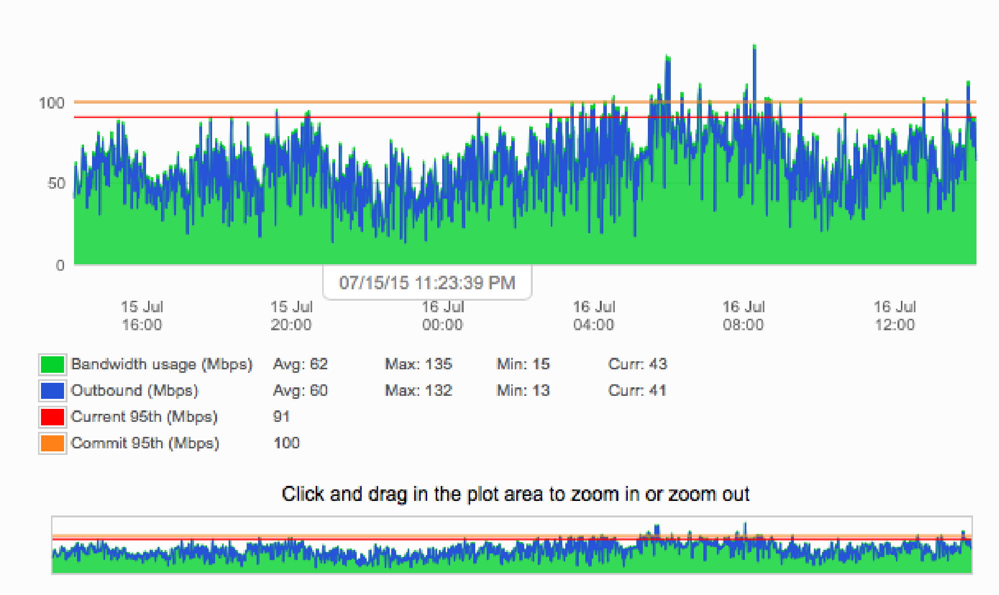
Organization begins event response

Average **5 minutes** from detection to notification

Albert Sizing

Daily Average Utilization

- **3 Server sizes based on Network Utilization**
  - Small = 0-100MB
  - Medium = 100MB-1GB
  - Large   = 1GB-5GB
  - Extra Large = Over 5GB



🟩 Bandwidth usage (Mbps)	Avg: 62	Max: 135	Min: 15	Curr: 43
🟦 Outbound (Mbps)	Avg: 60	Max: 132	Min: 13	Curr: 41
🟥 Current 95th (Mbps)	91			
🟧 Commit 95th (Mbps)	100			

Click and drag in the plot area to zoom in or zoom out

Albert Pricing

	Turnkey (CIS Hardware)		Customer-Provided Hardware		
Average Utilization	**Annual**	**Per Month**	**Annual**	**Per Month**	**Per Day**
0MB-100 MB - Small	$13,600	$1,130	$11,200	$930	<$31
101MB-1.0GB - Medium	$16,800	$1,400	$14,400	$1,200	<$40
1.01GB-5.0GB - Large	$30,000	$2,500	$26,400	$2,200	<$73
5.01GB+ - Extra Large	Custom				

*One-time initialization fee of $950 applies per sensor

**Size is based on your Daily Average Network Utilization

Albert: Related Webpages & Files

- Albert Landing Page
- Albert Terms and Conditions
- Case Study: Identifying Suspicious Election Network Activity with Albert
- Blog: Albert, A Smart Solution for Network Monitoring
- Presentation: Albert Service Introduction and Overview

- All CIS Albert Related Webpages

Internal Use Only Resources:

- MarCom: Albert Market Intelligence Repository
- CIS Server: Albert Resources
- CIS Server: Gartner Research Network Detection

CIS Endpoint Security Services

ESS

Proprietary

CIS Endpoint Security Services (ESS)

Features

- Device-Level Managed Detection & Response
- Next-Generation Antivirus (NGAV)
- Asset & Software Inventory, USB Device Monitoring
- Host-Based Firewall Management
- 24x7x365 SOC Monitoring, No-Cost Incident Response

CIS Endpoint Security Services (ESS)

Business Drivers

Hybrid & Remote Work Support

Optimal protection against cyber threats where your employees are

Active Defense for Devices

Able to stop a cyber attack in its tracks; Can kill, quarantine malicious files

Protects Against Unknown Threats

Blocks known (signature-based) and unknown (behavioral-based) malicious activity

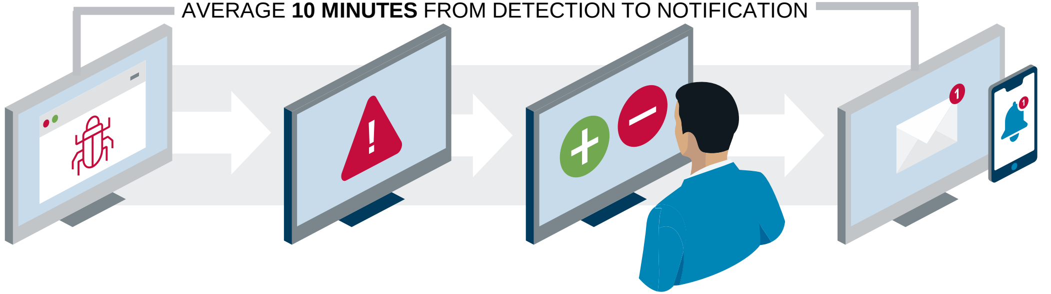
Full-time Cyber Defense Partner

24x7x365 CIS SOC monitors devices even when your security team is not

ESS in Action

Analyst Review

Industry-leading Response Times



AVERAGE **10 MINUTES** FROM DETECTION TO NOTIFICATION

ESS detects and/or blocks malicious activity

Alert generated and sent to 24×7×365 SOC

Analysis conducted in 24×7×365 SOC

Notification sent for actionable events only

FALSE POSITIVES ELIMINATED

Eliminating 75% of false positives saves time, simplifies decision-making

Incident Response

- <10 min Alert Analysis
- Customizable Escalation Procedures
- Remote System Quarantine
- Remote Incident Response/Remediation via Falcon platform

Defending SLTTs Together

Combining the Strengths of Two Industry Leaders

CROWDSTRIKE

- **Recognized as a leader in modern endpoint security**
  - Gartner, Forrester, IDC
- **Winner of multiple industry awards**
  - SC Awards, Forbes, Deloitte, Inc 500|5000

CIS Center for Internet Security®

- **Home of the MS-ISAC and EI-ISAC**
- **Leads development of globally-recognized security best practices**
  - CIS Critical Security Controls
  - CIS Benchmarks
- **Recognized as industry standard for cyber defense**
  - NIST, PCI DSS, DoD STIGs, FedRAMP

CIS Endpoint Security Services (ESS)

Device-Level Protection and Response

ESS Core Modules

- Falcon Prevent
- Falcon Insight
- Falcon Discover
- Falcon Device Control
- Falcon Firewall Management

ESS Spotlight

- Falcon Spotlight

Traditional Vulnerability Management

Stuck in the Dark Ages

Scanning is slow and burdensome

Vulnerability reports are unusable

Vulnerability scans have blind spots

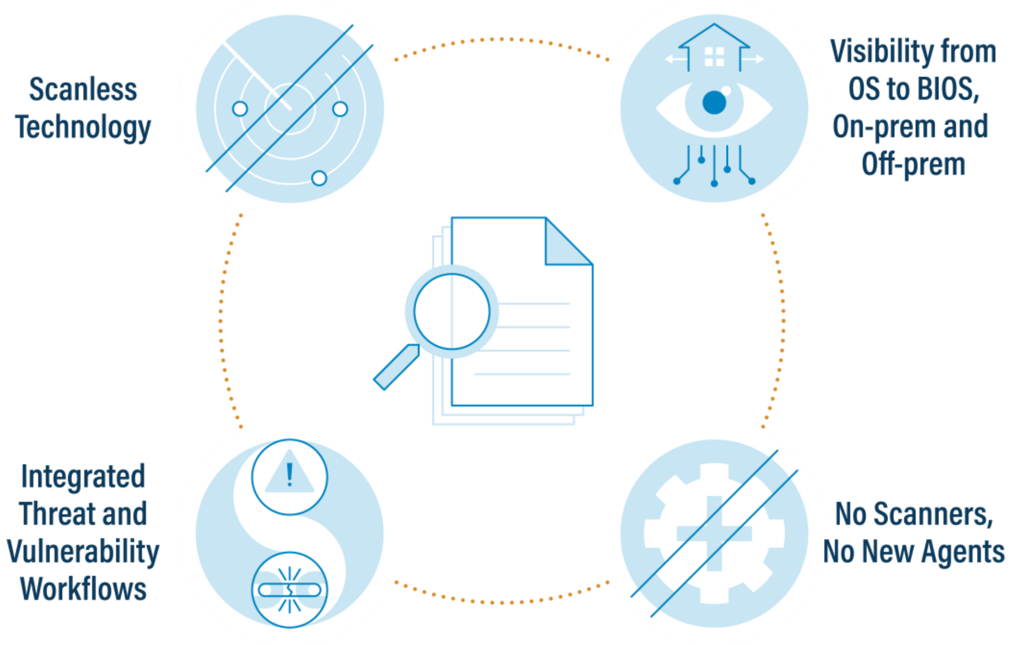
Real-time Vulnerability Management

ESS Spotlight

- Available as an additional module to the ESS service
- Monitor vulnerabilities on your devices in real-time
- Scan-less vulnerability
- Prioritize remediation of endpoint vulnerabilities
- Simplifies and shortens your response time with at-your-fingertips endpoint data
- On or off-network vulnerability assessment

ESS Spotlight

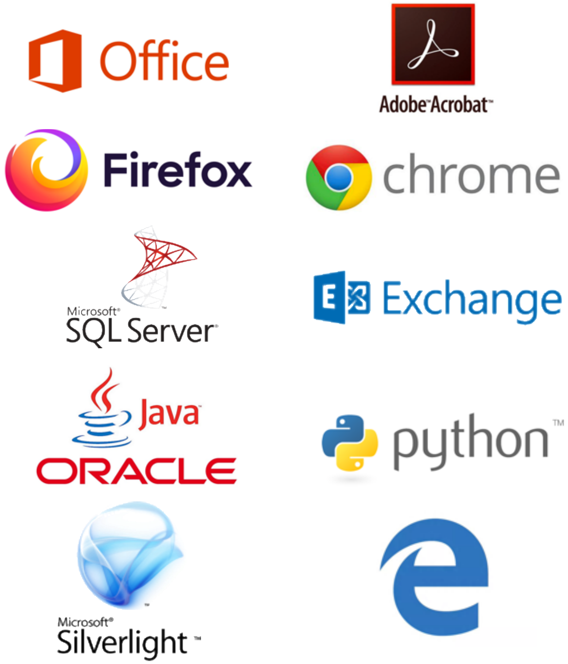
Illuminating Endpoint Vulnerabilities Using ESS Spotlight


Scanless Technology
Visibility from OS to BIOS, On-prem and Off-prem
Integrated Threat and Vulnerability Workflows
No Scanners, No New Agents

- Fast and Effective Vulnerability Management
- Holistic Protection
- Simplicity
- Timely Knowledge, On-Demand
- Zero Impact

ESS Spotlight

A More Complete Picture of Risks in Your Organization

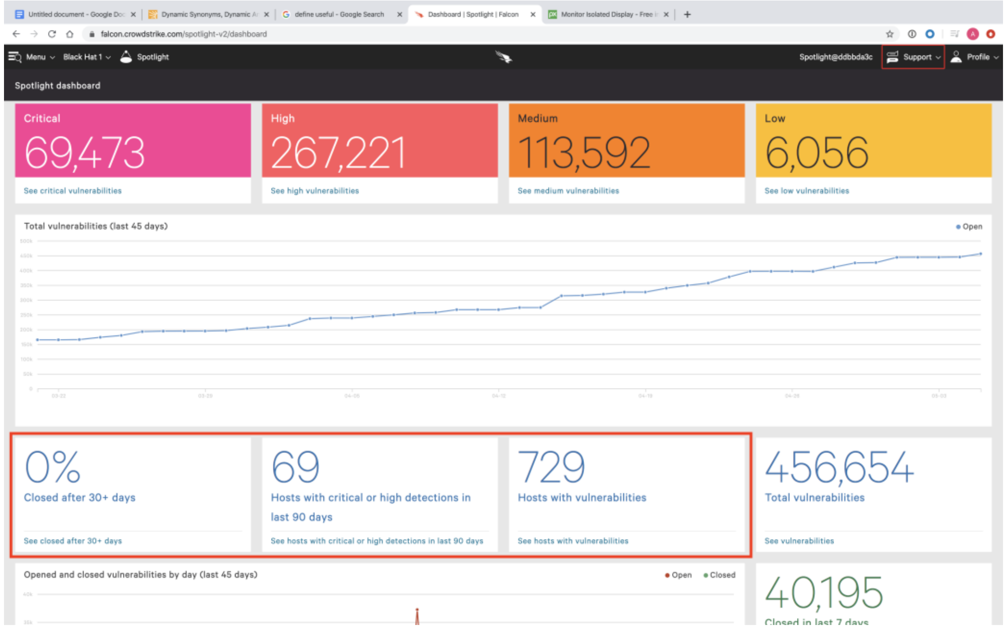


Expanded Vulnerability Visibility of:

- Windows desktop applications
- Server software
- Development tools

ESS Spotlight

Gain Security Efficiency and Efficacy


Untitled document - Google Doc
Dynamic Synonyms, Dynamic A
define useful - Google Search
Dashboard | Spotlight | Falcon
Monitor Isolated Display - Free
falcon.crowdstrike.com/spotlight-v2/dashboard
Menu
Black Hat 1
Spotlight
Spotlight@ddbbda3c
Support
Profile
500k
450k
400k
350k
300k
250k
200k
150k
100k
50k
0
03-22
03-29
04-05
04-12
04-19
04-26
05-03
● Open
● Closed
40k
30k

Spotlight dashboard

Critical
69,473
See critical vulnerabilities

High
267,221
See high vulnerabilities

Medium
113,592
See medium vulnerabilities

Low
6,056
See low vulnerabilities

Total vulnerabilities (last 45 days)

0%
Closed after 30+ days
See closed after 30+ days

69
Hosts with critical or high detections in last 90 days
See hosts with critical or high detections in last 90 days

729
Hosts with vulnerabilities
See hosts with vulnerabilities

456,654
Total vulnerabilities
See vulnerabilities

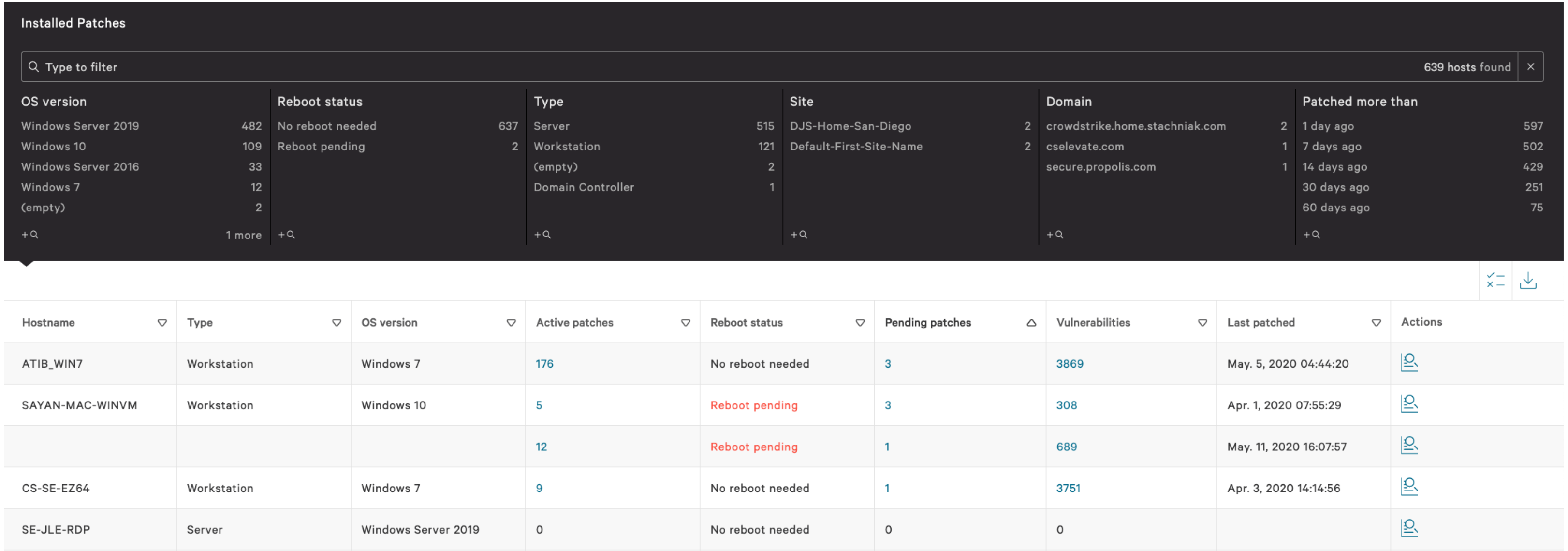
Opened and closed vulnerabilities by day (last 45 days)

40,195
Closed in last 7 days

- Prioritized Hosts With Detections
- Interactive Dashboards
- Saved Filters

ESS Spotlight

Easier to Prioritize, Manage, and Track Vulnerability Status



Installed Patches

Type to filter 639 hosts found

OS version	
Windows Server 2019	482
Windows 10	109
Windows Server 2016	33
Windows 7	12
(empty)	2
+Q	1 more

Reboot status	
No reboot needed	637
Reboot pending	2

Type	
Server	515
Workstation	121
(empty)	2
Domain Controller	1

Site	
DJS-Home-San-Diego	2
Default-First-Site-Name	2

Domain	
crowdstrike.home.stachniak.com	2
cselevate.com	1
secure.propolis.com	1

Patched more than	
1 day ago	597
7 days ago	502
14 days ago	429
30 days ago	251
60 days ago	75

Hostname	Type	OS version	Active patches	Reboot status	Pending patches	Vulnerabilities	Last patched	Actions
ATIB_WIN7	Workstation	Windows 7	176	No reboot needed	3	3869	May. 5, 2020 04:44:20	
SAYAN-MAC-WINVM	Workstation	Windows 10	5	Reboot pending	3	308	Apr. 1, 2020 07:55:29	
			12	Reboot pending	1	689	May. 11, 2020 16:07:57	
CS-SE-EZ64	Workstation	Windows 7	9	No reboot needed	1	3751	Apr. 3, 2020 14:14:56	
SE-JLE-RDP	Server	Windows Server 2019	0	No reboot needed	0	0		

Alignment with Industry Standards

9 CIS Controls

MITRE ATT&CK framework aligned

FedRAMP certified

Assists with CIS Critical Security Controls (CIS Controls) implementation

- CIS Control 1: Asset Inventory
- CIS Control 2: Software Inventory
- CIS Control 4: Secure Configuration of Enterprise Assets and Software
- CIS Control 5: Account Management
- CIS Control 6: Access Control Management
- CIS Control 7: Continuous Vulnerability Management
- CIS Control 10: Malware Defense
- CIS Control 13: Network Monitoring and Defense
- CIS Control 17: Incident Response Management

ESS Pricing

ESS Core	
Yearly	**Monthly**
$60 per endpoint	$5 per endpoint

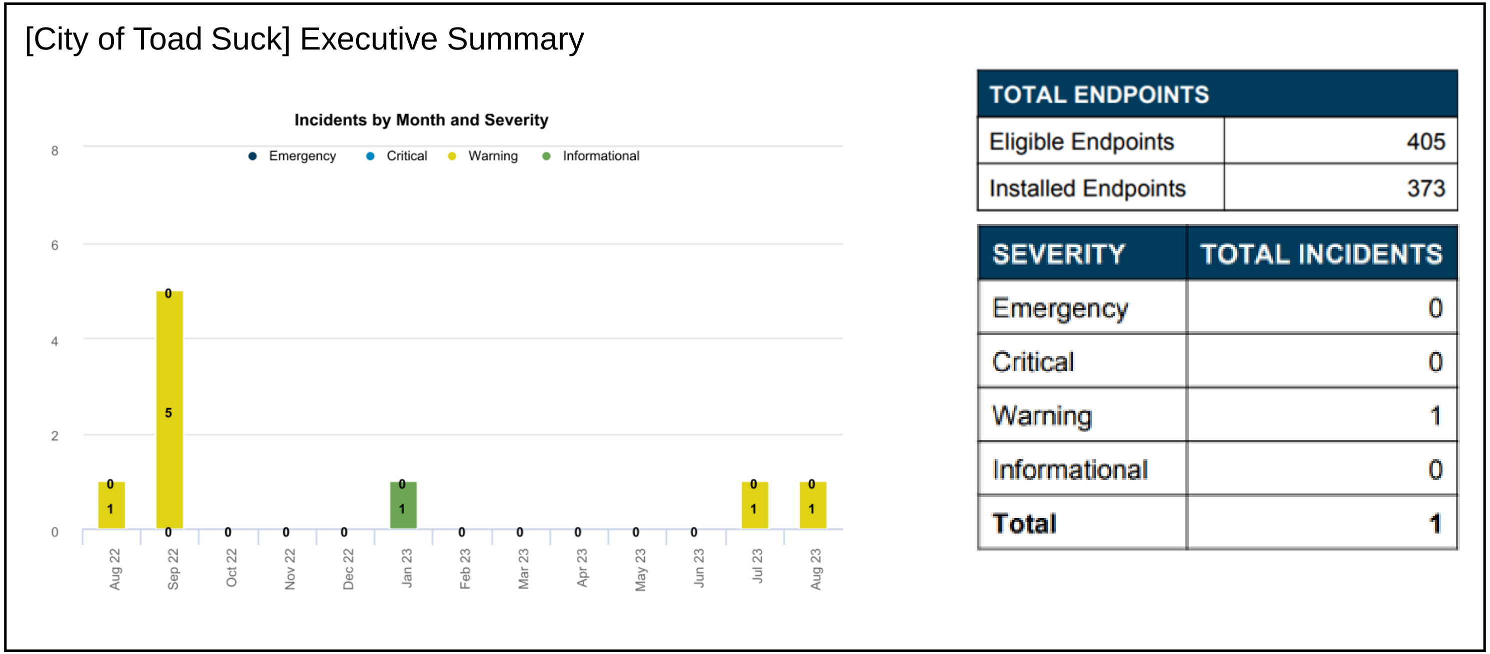
ESS Spotlight	
Yearly	**Monthly**
$6 per endpoint	$0.50 per endpoint

Monthly Activity Report (MAR)

Summary of Logged Activity

- **Agency Executive Summary**
- **ESS Endpoints Summary**
- **ESS Incident Summary**
  - Incidents by severity
  - Incidents by category
  - Ticket information
  - Incidents by severity monthly and YTD
  - Incidents and events by severity YTD
  - Incidents and events by category YTD

MAR Reporting Sample



[City of Toad Suck] Executive Summary

TOTAL ENDPOINTS	
Eligible Endpoints	405
Installed Endpoints	373

SEVERITY	TOTAL INCIDENTS
Emergency	0
Critical	0
Warning	1
Informational	0
Total	**1**

ESS Related Webpages & Files

- ESS Landing Page
- Blog: Endpoint Security, The Key to Combatting Sophisticated CTAs
- Blog: Announcing CIS Endpoint Security Services for SLTTs
- Webinar: Defending Today's Workforce with CIS Endpoint Security Services
- Webinar: CIS Endpoint Security Services – C Level Roundtable Discussion
- Terms and Conditions: CIS Endpoint Security Service via CrowdStrike
- All CIS Endpoint Security Service Related Webpages

Internal Use Only Resources:

- CIS Server: Gartner Research Endpoint Security
- MarCom: ESS Market Intelligence Repository

Malicious Domain Blocking and Reporting Plus

MDBR+

Proprietary

MDBR+

Advanced Web Security Service: Features

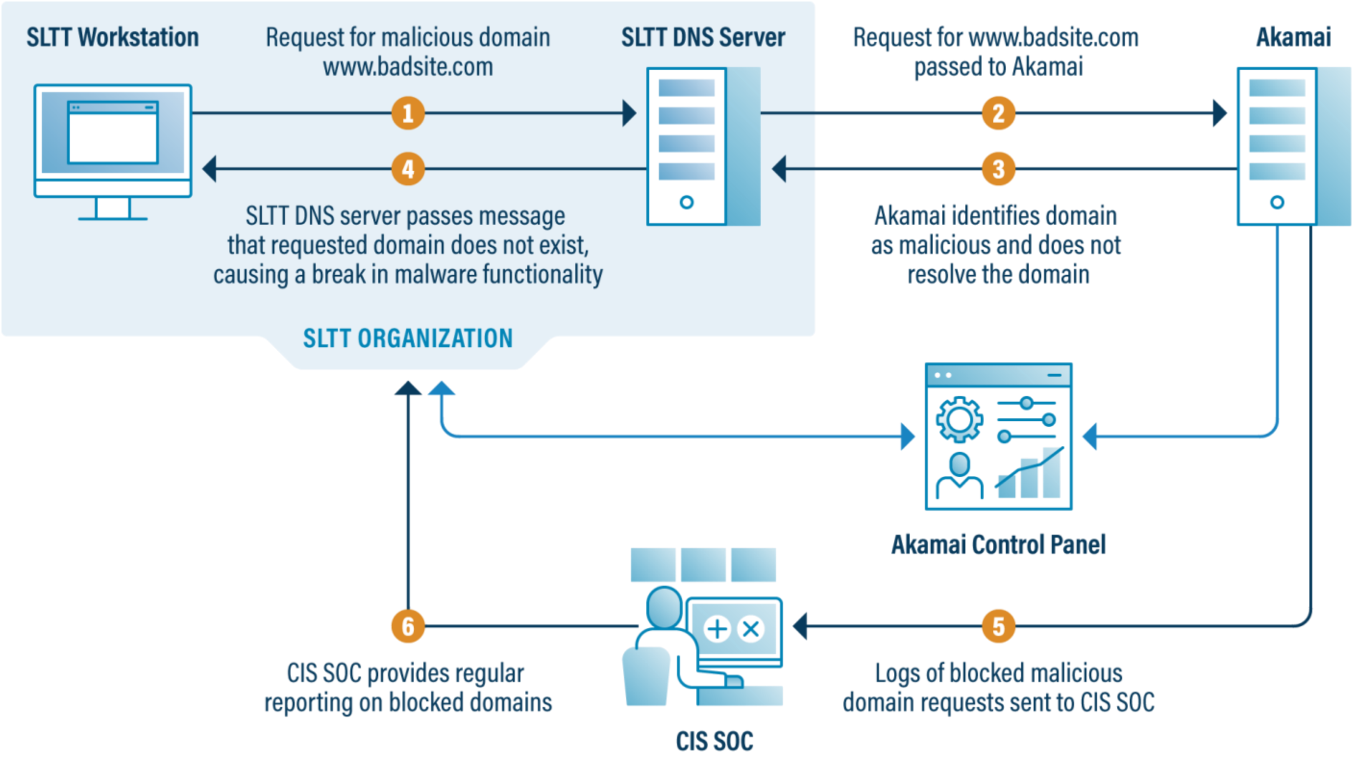
Cloud-Based Management Portal

Custom Acceptable Use Policies, Allow/Deny Lists

Enhanced Reporting & Visibility

Impactful Threat Intelligence from Akamai and the CIS SOC

MDBR+ in Action



SLTT Workstation

SLTT DNS Server

Akamai

1 Request for malicious domain www.badsite.com

2 Request for www.badsite.com passed to Akamai

3 Akamai identifies domain as malicious and does not resolve the domain

4 SLTT DNS server passes message that requested domain does not exist, causing a break in malware functionality

SLTT ORGANIZATION

Akamai Control Panel

5 Logs of blocked malicious domain requests sent to CIS SOC

6 CIS SOC provides regular reporting on blocked domains

CIS SOC

Why MDBR+?

Business Drivers

Real-time Access to Portal Dashboard and Reports

Acceptable Use Policy (AUP) Enforcement

Security Connector or Agents for Host-based Reports and Portable Device Protection

Customer-specific Allow and Deny Lists with Customer-specific Error Pages

Save Security Teams Time by Administering Security Polices Globally in Seconds

MDBR+ Feature Comparison

What’s the Difference between MDBR and MDBR+?

	MDBR	MDBR+
Security		
Block Malware, Phishing, and C&C	X	X
Identify DNS Data Exfiltration	X	X
URL Inspection		X
Enforce Security for Roaming users		X
Configurable Security Policies		X
Investigation of Security Alerts		X

	MDBR	MDBR+
AUP		
Enforce AUP		X
Enforce Safe Search		X
Reporting/Monitoring/Analytics		
CIS MDBR Report	X	X
Real-time Enterprise Wide Activity and Search		X
Delegated Administration		X
Customized & Automated Reports		X

User Stories

K-12 Director of Technology in Indiana

“MDBR+ has given us **greater insight into our environment**. We can now see what devices on our network are trying to connect to these harmful domains and allows us to create actionable steps to mitigate these connections.”

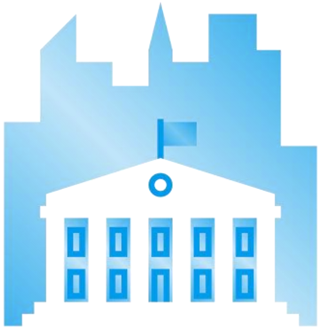
“We also can **install client software on our mobile users’ devices** to help protect them when they are off-network. As an educational entity with limited resources, the use of MDBR+ helps us to be proactive by mitigating these connections before they become real problems.”

User Stories

Director of IT and Communications in Pennsylvania

“MDBR+ has proven to be a valuable addition to the Township’s cyber security infrastructure and initiatives. The overall **health of the network traffic and DNS requests are easily observed via the dashboard** view and Akamai’s threat reporting features allow you to get granular and as deep as you need to go.”

“The deployment and **installation is very simple and a quick process**. The ability to update remote agents is a welcomed feature. We have been very happy with the MDBR+ service that Akamai and CIS provide and I would recommend it as a part of any well maintained and hardened security protocol.”



MDBR+ Pricing

MDBR+	
Tier	**Cost**
Tier 1	$200 per month up to 150 users *$0.75 per user per month for 151 – 1,999 additional users*
Tier 2	2,000 – 4,000 users $0.60 per month per user
Tier 3	Over 4,000 users $0.50 per month per user *Bulk discounts may be approved at manager discretion*

Defending SLTTs Together

Combining the Strengths of Two Industry Leaders

Akamai

- **Powers and protects life online**
- **Trusted globally**
  - – All 6 U.S. military branches
  - – 14 of 15 U.S. federal civilian cabinet agencies
  - – 9 of top 10 software companies
  - – 8 of top 10 retail companies
- **Recognized as industry leader by**
  - – Forrester, SC Awards, IDC

CIS Center for Internet Security®

- **Home of the MS-ISAC and EI-ISAC**
- **Leads development of globally-recognized security best practices**
  - – CIS Critical Security Controls
  - – CIS Benchmarks
- **Recognized as industry standard for cyber defense**
  - – NIST, PCI DSS, DoD STIGs, FedRAMP

MDBR+ Related Webpages & Files

- MDBR+ Landing Page
- Spotlight: Election Security Spotlight – What is MDBR+?
- Press Release: Industry Leaders Collaborate on New Cybersecurity Offering
- Terms and Conditions: MDBR+
- Akamai Blog MDBR+ Partnership
- MDBR+ Launch Welcome Campaign
- MDBR+ Video

Internal Use Only Resources:

- CIS Server: Gartner Research Managed Detection and Response
- MarCom: MDBR+ Market Intelligence Repository

Center for Internet Security®

CIS Managed Security Services

MSS

Proprietary

Managed Security Services (MSS)

Features

- Expert Event & Log Analysis by 24x7x365 CIS SOC
- Eliminate False Positive Alerts
- Available for Host of Devices in IT Environments

Managed Security Services (MSS)

Business Drivers

Alleviate Alert & Log Fatigue

Filter out false positives so security teams only deal with credible threats

Save Time, Effort

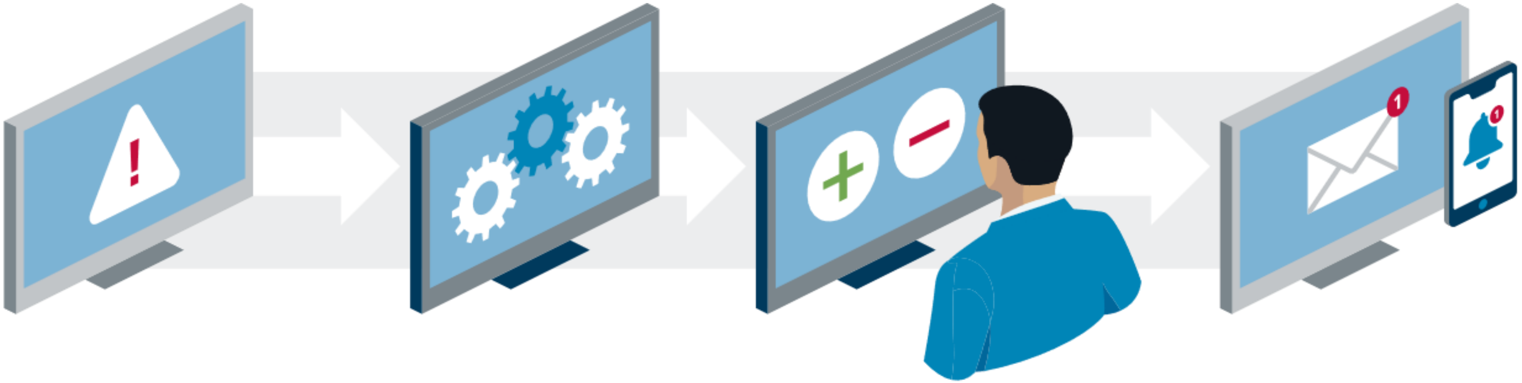
Security teams can focus on what is important without wading through time-consuming false positives

Gain a Full-time Security Partner

CIS SOC works round-the-clock to analyze and escalate your logs/events

MSS in Action

Alleviate Alert and Log Fatigue



MSS Monitored Device Alert/Event

CIS SIEM

Analysis conducted in 24×7×365 SOC

FALSE POSITIVES ELIMINATED

Notification Sent for Actionable Events Only

Defending SLTTs Together

Combining the Strengths of Two Industry Leaders

accenture

- **Recognized as industry leader by**
  - Fortune, Fast Company, BrandZ
- **Trusted by 89 of the Fortune Global 100 companies**

CIS Center for Internet Security®

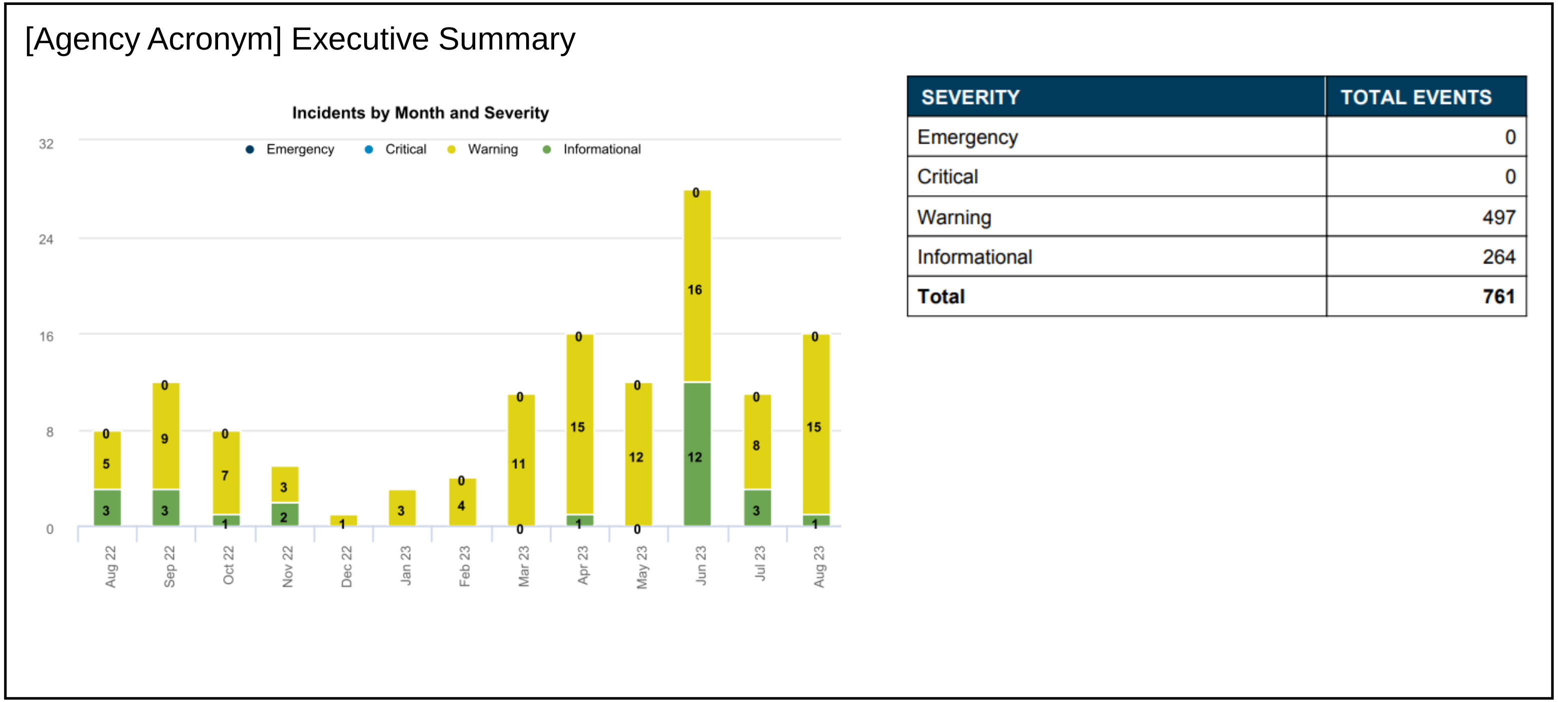
- **Home of the MS-ISAC and EI-ISAC**
- **Leads development of globally-recognized security best practices**
  - CIS Critical Security Controls
  - CIS Benchmarks
- **Recognized as industry standard for cyber defense**
  - NIST, PCI DSS, DoD STIGs, FedRAMP

Monthly Activity Report (MAR)

Summary of Logged Activity

- **Nationwide Summary**
- **Agency Executive Summary**
- **MSS Event Summary**
  - – Actionable events by severity
  - – Ticket information
  - – Generated events by severity YTD
  - – Generated events by signature classification
  - – Actionable events by signature classification
- **MSS Traffic Graphs**

MAR Reporting Sample



[Agency Acronym] Executive Summary

SEVERITY	TOTAL EVENTS
Emergency	0
Critical	0
Warning	497
Informational	264
Total	**761**

MSS Related Webpages & Files

- MSS Landing Page
- Terms and Conditions: MSS

Internal Use Only Resources:

- CIS Server: Gartner Research MSS
- MarCom: MSS Market Intelligence Repository

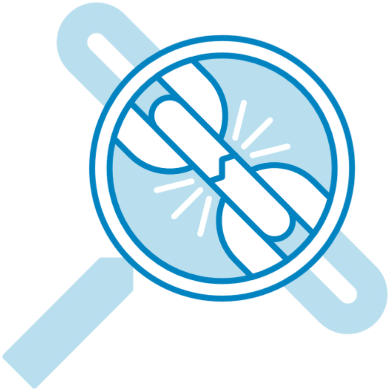
Center for Internet Security®

Vulnerability Assessment

Proprietary

Vulnerability Assessment: Network and Web App

Expert Analysis, Prioritization, and Remediation



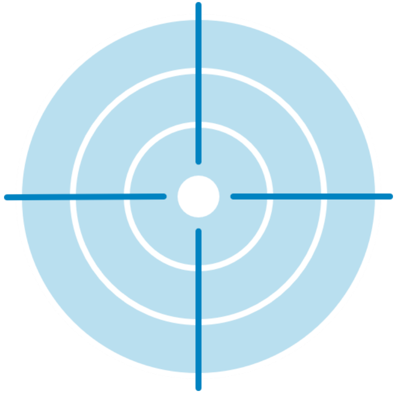
- **Identify critical system weaknesses**
  - Help organization prioritize remediation steps
  - Manually verify assessment results
  - Assist in meeting PCI DSS, HIPAA, and others compliance frameworks
- **Assessments include**
  - Network discovery and mapping
  - Asset prioritization
  - Remediation tracking
- **Reporting**
  - Prioritized remediation guidance
  - Based on severity of threat

Penetration Testing

Proprietary

Pen Testing: Web App, Internal/External Network

Clear Assessment of Cybersecurity Policies, Processes, and Defenses



- **Simulate a real-world cyber attack**
  - Experts attempt to exploit vulnerabilities
  - Determine likelihood and potential scope of cyber attack
- **Provides a safe review of an organization’s security posture**
- **Detailed reporting**
  - Prioritized actionable information

    Based on severity with remediation guidance
  - Identify how vulnerability was discovered
  - Potential impact
  - Recommendations
  - Vulnerability references

CIS Center for Internet Security®

Thank You