CIS Cybersecurity Services
Enhancing Your Defense-in-Depth Cybersecurity Program

Greg A. Lubert
Account Executive, CIS Services
July 28, 2022
Center for Internet Security
Nonprofit leading the global community to secure our connected world

Home of the MS-ISAC and EI-ISAC.

Security Operations Center
**Benefits**

**MS-ISAC Membership**

---

**No Cost Benefits**

- 24×7×365 Security Operations Center (SOC)
- Passive IP & Domain Monitoring
- Malicious Domain Blocking & Reporting (MDBR)
- Cybersecurity exercises
- Cybersecurity advisories
- Cyber event notifications
- Education and awareness materials
- CIS SecureSuite® Membership
- Incident response resources
- Malicious Code Analysis Platform (MCAP)
- Monthly newsletters, webinars and threat briefings
- Homeland Security Information Network (HSIN) access, including portals for communication and document sharing
- Deloitte Cyber Detect Cyber Respond Portal
- Nationwide Cybersecurity Review (NCSR)
- Discounts on training
- Vulnerability assessment services

[https://learn.cisecurity.org/ms-isac-registration](https://learn.cisecurity.org/ms-isac-registration)
CIS Endpoint Security Services (ESS)
Device-Level Protection and Response

- FALCON PREVENT
- FALCON DISCOVER
- FALCON DEVICE CONTROL
- FALCON INSIGHT
- FALCON FIREWALL MANAGEMENT
CIS Endpoint Security Services Features
Monitor, manage, respond, and prevent

Next Generation Antivirus (NGAV)
Endpoint Detection and Response (EDR)
Advanced Capabilities

Fully Managed Solution
Customizable Device Control
Alignment with Industry Standards
Next Generation Antivirus (NGAV)
Falcon Prevent

- **Active defense against ransomware; encrypted/unencrypted malicious traffic**
- **Stops attacks in their tracks upon detection**
  - Blocks malicious activity and can kill processes or quarantine files
- **Cloud integrated endpoint protection**
- **Signature and behavioral malware protection**
  - Identify both known and unknown threats (Zero Day protection)
- **Threat intel and threat indicators – Indicators of compromise**
Capturing endpoint activity for threat detection and escalation

Custom detection rules

Threat hunting

Secure remote system access while Quarantined

Endpoint Detection & Response (EDR)
Falcon Insight with ThreatGraph
Advanced Capabilities

Falcon Discover

**Asset inventory**
- Monitor assets to achieve, maintain, and prove compliance
- Pinpoint rogue devices

**User account monitoring**
- Track user account activity and unusual behavior
- Monitor administrator credential use
- Assess password update policy

**Application inventory**
- Search for any and all deployed applications
- Find specific versions
- Identify unauthorized or suspicious software

*Requested through the SOC*
Customizable Device Control
Falcon Device Control and Falcon Firewall Management

Access to Management Portal
Host-based Firewall Control
USB Device Control
Protection On and Off Network
Endpoint-level protection for today’s hybrid and remote work models

Defend employees and devices no matter the location.
Albert Network Monitoring & Management
Available to state, local, tribal, and territorial governments and election agencies

• **Cost-effective Intrusion Detection System (IDS)**
  – Turnkey solution incorporating 24x7x365 monitoring and management

• **Identifies malicious or potentially harmful network activity**
  – Based on an average of 32,000+ signatures
  – Signatures updated twice daily
Signatures and Indicators of Compromise
Three unique and targeted signature sources

- Commercial signatures
- CIS research Threat data analysis Incident response cases
- Recently declassified signatures
Albert Detection and Monitoring
Analyst review

Average 6 minutes from detection to notification

Albert detects signature match
Alert generated and sent to 24x7x365 SOC
Analysis conducted in 24x7x365 SOC
FALSE POSITIVES ELIMINATED
Notification Sent for Actionable Events Only
[Agency Acronym] Executive Summary

The following executive level summary provides an overview of actionable security events and monitored devices for [Agency Name] for the month of December 2017.

Events
The arrows represent the change in event counts from the previous month.

<table>
<thead>
<tr>
<th>Event Type</th>
<th>December</th>
<th>2017 YTD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Critical</td>
<td>14</td>
<td>176</td>
</tr>
<tr>
<td>Warning</td>
<td>5</td>
<td>42</td>
</tr>
<tr>
<td>Informational</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Top Event Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>December</th>
<th>2017 YTD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan Activity</td>
<td>14</td>
<td>176</td>
</tr>
<tr>
<td>Unusual Network Activity</td>
<td>5</td>
<td>42</td>
</tr>
</tbody>
</table>

Events by Month

[Agency Acronym] Event Count by Month

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>6</td>
<td>11</td>
<td>15</td>
<td>19</td>
<td>11</td>
<td>16</td>
<td>13</td>
<td>11</td>
<td>16</td>
<td>26</td>
<td>26</td>
<td>19</td>
<td></td>
</tr>
</tbody>
</table>

[Agency Acronym] Events by Severity

- Emergency
- Critical
- Warning
- Informational

Devices

The arrow for Albert Netflow represents a change of 25% or more from the previous three month average.

<table>
<thead>
<tr>
<th>Devices</th>
<th>Albert Netflow</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>870.0 TB</td>
</tr>
</tbody>
</table>
Managed Security Services
Log and security event monitoring of existing devices

• Monitoring including, but not limited to
  – IDS, IPS, firewalls, switches & routers, servers, endpoints, and web proxies.
ESS/Albert/MSS Monitoring and Management
24x7x365 Security Operations Center

- SOC analysts become an extension of your security team
- Expert human analysis of malicious activity
  - Industry-leading response times
  - Specific experience with the challenges faced by SLTTs
- SLTT-focused threat database
- 3 Letter Agencies; Federal Partners
- CISA (Federal SOC)
Phishing Engagements
Enhance cyber defenses with education and awareness

• Most common and successful technique used by cybercriminals
• Assess vulnerability to phishing attacks
  – Highly customizable and specially-crafted emails
• Detailed report
  – How susceptible
  – Likelihood of successful intrusion
  – Attack method
• CIS Phishing Engagements in Action
  – 69% of new-hire targets susceptible to open and click
  – 62% of new-hires submitted credentials to spoofed login form
Vulnerability Assessment: Network and Web App

Cost-effective solution to understand and improve overall security posture

• **Identify critical system weaknesses**
  – Help organization prioritize remediation steps
  – Offer customized reporting features
  – Manually verify assessment results
  – Assist in meeting PCI DSS, HIPAA, and others

• **Assessments include**
  – Network discovery and mapping
  – Asset prioritization
  – Reporting
  – Remediation tracking
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

• Findings delivered in detailed report
  – How vulnerability was discovered
  – Potential impact
  – Recommendations
  – Vulnerability references
The MS-ISAC provides cyber incident response services free of cost to State, Local, Tribal, and Territorial (SLTT) organizations. These services are provided by our Cyber Incident Response Team (CIRT), a team of highly knowledgeable and skilled analysts trained in digital forensics and incident response. Services include:

• Emergency conference calls
• Log analysis
• Ongoing communication throughout the incident
• Mitigation recommendations (Attended Remediation)
• Computer forensic analysis of forensic images to determine root cause analysis as needed in support of an ongoing incident response case
• At the close of the incident, written communication will be provided that summarizes the incident.
• In every incident, CIRT exerts a concerted effort to provide a personal level of service to SLTT organizations, seeking to engage with customers based on their organizational needs and circumstances.
Questions?
Thank You!

Greg A. Lubert
Gregory.Lubert@cisecurity.org
518-894-4637
# Pricing

Fully managed, premium endpoint security solution as a service

## Standard Pricing

<table>
<thead>
<tr>
<th>Yearly</th>
<th>Monthly</th>
</tr>
</thead>
<tbody>
<tr>
<td>$60/endpoint</td>
<td>$5/endpoint</td>
</tr>
</tbody>
</table>

Contact services@cisecurity.org to get started
Albert Pricing

Albert Tiers based on Daily Average Network Utilization

- One time initiation fee of $900 applies (per sensor)

**Albert Hardware Included**

- Up to 100 Mbps - $13,080/Annually - $36 a day
- >100 Mbps - 1 Gbps - $16,200/Annually - $44 a day
- 1 Gbps – 6Gbps - $28,800/Annually - $79 a day
- Over 6Gbps – Custom Pricing.

- Hardware provided by CIS

**Albert Member Provided Hardware**

- Up to 100 Mbps - $10,680/Annually - $30 a day
- >100 Mbps - 1 Gbps - $13,800/Annually - $38 a day
- >1 Gbps – 6Gbps - $25,200/Annually - $70 a day
- Over 6Gbps – Custom Pricing.

- Hardware (Obtained by entity)
- Albert can be deployed using a VMWare or Hyper V VM (Up to 100Mbps only) or you can repurpose existing hardware if it meets the attached specs