Cybersecurity for Non IT Leaders: NY’s Endpoint Detection Solution for Counties

Webinar, March 23
March 23, 2023

Benjamin Voce-Gardner
Director, Office of Counterterrorism
NYS Division of Homeland Security and Emergency Services
NYS JSOC Mission

The New York JSOC Will Serve as a First-of-its-Kind Hub for Data Sharing and Cyber Coordination Across New York State, New York City, the Five Major Upstate Cities, Local and Regional Governments, Critical Infrastructure and Federal Partners
EDR Rollout Progress

• 46 Counties and 5 Cities signed up (representing over 70,000 endpoints)
  – Over 30,000 endpoints active. Others are coming online every day.
• Remaining Counties encouraged to join
• Existing County endpoint review
CrowdStrike Falcon Complete

Key Benefits include:

• Proactive Management and Optimization
• 24/7 Expertise to Defend the Cloud
• Continuous Human Threat Hunting
• 24/7 Monitoring and Response
• Surgical Remediation
• Transparent and Secure Collaboration
Benefits to the Counties

• 24/7 cybersecurity support
• Shared statewide view of our cyber risk
• Economy of scale purchasing
• Next steps
Onondaga County Testimonial with Kevin Sexton
Jeremy Pafundi
Regional Sales Manager
SLED New York
CrowdStrike – NYSAC / NYS JSOC Endpoint Protection Service Update

Jeremy Pafundi, Regional Sales Manager, SLED New York
Russ Harnish, Sales Engineer, SLED New York
David Beckett, Principal Sales Engineer, SLED New York
Kevin Sexton, CIO, Onondaga County
Ben Voci, Director, Office Counter Terrorism
Agenda

- Update from CrowdStrike on NYS JSOC
- Review of Support
- Cloud Native and Modern Attack
- Value of Falcon Complete
- Testimonial from Onondaga County
- Q/A
Proven Track Record Customer Support

- Basic Workflow
  - Signed Inter Government Agreement
  - Welcome Email from CrowdStrike Account team
  - Kick Off Call with Onboarding team

- Key areas of focus:
  - Falcon Sensor Deployment
  - Falcon Policy Configuration
  - Users/Roles
  - Falcon Modules
  - Falcon API

- Why Successful:
  - New York Made the right investment in support services
  - White Glove Service
  - Tool Rationalization

- Training investment:
  - New York has made investments in training
  - Self Paced Online Training

- Elite Level TAM:
  - Named TAM
  - 24/7 Customer Support
  - Custom Reporting
  - Product Mgmt. Access

- Where are we today and results:
  - 50+ County/Cities in process of roll out
  - All different AV’s and Environments
  - All different skill levels and team make ups
CLOUD-NATIVE

PROTECTION OF THE CROWD

EFFORTLESS SCALABILITY

WORKS ON DAY ONE
COMPONENTS OF THE ADVANCED MODERN ATTACK

ECRIME ADVERSARY EXPEDITED BREAKOUT TIME

- 9H 42M
- 1H 38M
- 162H

2021 MALWARE V MALWARE FREE ATTACKS

- Malware: 38%
- Malware-Free: 62%
Falcon Complete Overview
## HIDDEN Cost of Endpoint Security

<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
<th>COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACQUIRING ENDPOINT SECURITY TECHNOLOGY</td>
<td>$</td>
</tr>
<tr>
<td>IMPLEMENTING, CONFIGURING AND TUNING</td>
<td>$$</td>
</tr>
<tr>
<td>MANAGING, MAINTAINING AND UPDATING</td>
<td>$$$</td>
</tr>
<tr>
<td>MONITORING, TRIAGING AND ANALYZING ALERTS</td>
<td>$$$</td>
</tr>
<tr>
<td>RESPONDING TO AND REMEDIATING INCIDENTS</td>
<td>$$$</td>
</tr>
<tr>
<td>THE COST OF A DATA BREACH</td>
<td>$$ $$</td>
</tr>
</tbody>
</table>
### People

**Effective Monitoring & Response**

<table>
<thead>
<tr>
<th>Time to Detect</th>
<th>Industry Average *</th>
<th>Continuous Monitoring &amp; Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>120 Hours</td>
<td>1 Minute</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Time to Investigate</th>
<th>11 Hours</th>
<th>6 Minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to Remediate</td>
<td>31 Hours</td>
<td>29 Minutes</td>
</tr>
</tbody>
</table>

* Source: CrowdStrike 2020 Global Security Attitude Survey

**Falconstrike Complete Exceeds the 1:10:60 Goal**
**FALCON COMPLETE Stops BREACHES WITH**

**PLATFORM, Intelligence, and EXPERTISE**

<table>
<thead>
<tr>
<th><strong>COMPREHENSIVE PLATFORM</strong></th>
<th><strong>UNIQUE EXPERTISE &amp; INTEL</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FALCON DISCOVER</strong></td>
<td><strong>FALCON OVERWATCH 24/7</strong></td>
</tr>
<tr>
<td><strong>IT HYGIENE</strong></td>
<td><strong>HUNTERS</strong></td>
</tr>
<tr>
<td><strong>UNDERSTAND</strong></td>
<td><strong>FALCON COMPLETE TEAM</strong></td>
</tr>
<tr>
<td><strong>CUSTOMER ASSETS AND RISK</strong></td>
<td><strong>24/7 RESPONDERS</strong></td>
</tr>
<tr>
<td><strong>FALCON PREVENT</strong></td>
<td><strong>HUNT AND RESPOND</strong></td>
</tr>
<tr>
<td><strong>NGAV</strong></td>
<td><strong>CROWDSTRIKE PEOPLE AND PROCESS</strong></td>
</tr>
<tr>
<td><strong>BLOCK</strong></td>
<td></td>
</tr>
<tr>
<td><strong>99% OF TRADECRAFT</strong></td>
<td></td>
</tr>
<tr>
<td><strong>FALCON INSIGHT</strong></td>
<td></td>
</tr>
<tr>
<td><strong>EDR</strong></td>
<td></td>
</tr>
<tr>
<td><strong>RECORD AND ANALYZE</strong></td>
<td></td>
</tr>
<tr>
<td><strong>ENDPOINT TELEMETRY</strong></td>
<td></td>
</tr>
<tr>
<td><strong>FALCON IDENTITY</strong></td>
<td></td>
</tr>
<tr>
<td><strong>THREAT PROTECTION</strong></td>
<td></td>
</tr>
<tr>
<td><strong>ITP</strong></td>
<td></td>
</tr>
<tr>
<td><strong>PROTECT AND ENFORCE</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IDENTITIES AND IDENTITY STORES</strong></td>
<td></td>
</tr>
</tbody>
</table>