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

Webinar, March 23

Mark LaVigne PhD
Deputy Director
NYSAC

NEW YORK STATE | Homeland Security and Emergency Services

Benjamin Voce-Gardner

Director, Office of Counterterrorism
NYS Division of Homeland Security and Emergency Services

March 23, 2023

NEW YORK STATE | Homeland Security and Emergency Services

NYS Joint Security Operations Center

Benjamin Voce-Gardner
Director, Office of Counter Terrorism

March 23, 2023

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

CROWDSTRIKE

Kevin Sexton

CIO

Onondaga County

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 Vocegardner, 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

CROWDSTRIKE

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

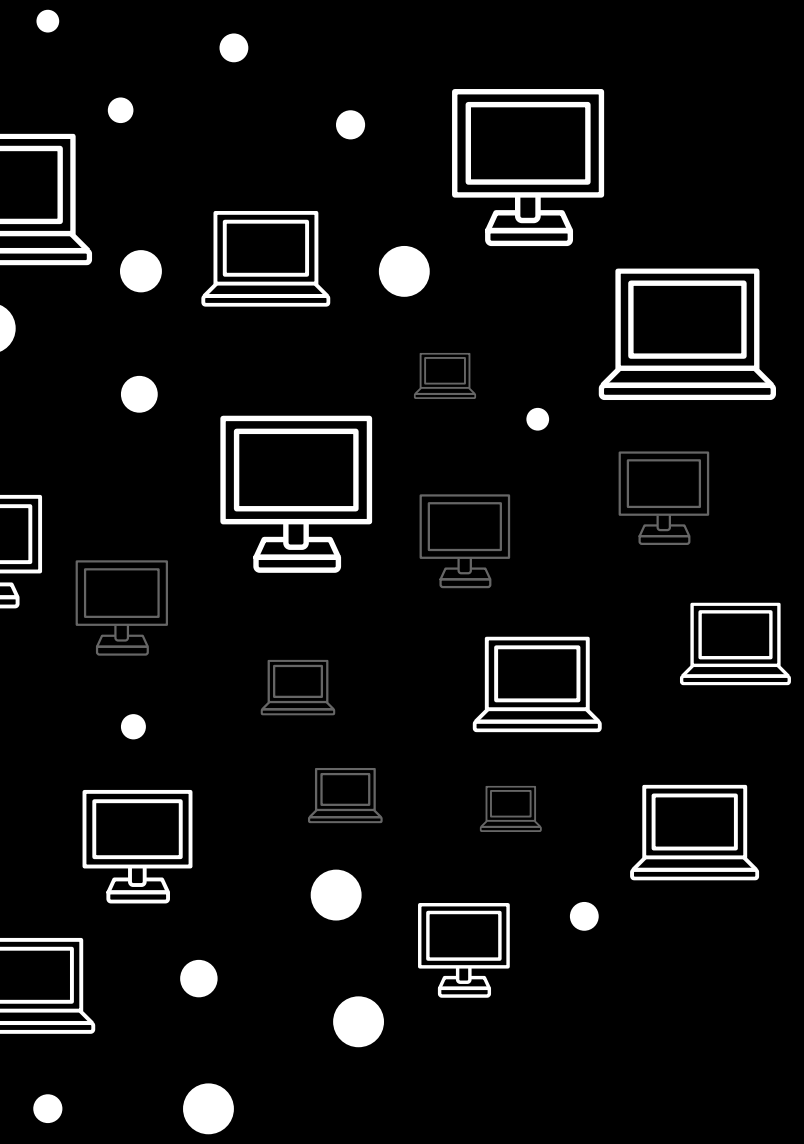
- Training investment:
  - New York has made investments in training
  - Self Paced Online Training

- 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

CROWDSTRIKE

CLOUD-NATIVE



PROTECTION OF THE CROWD

EFFORTLESS SCALABILITY

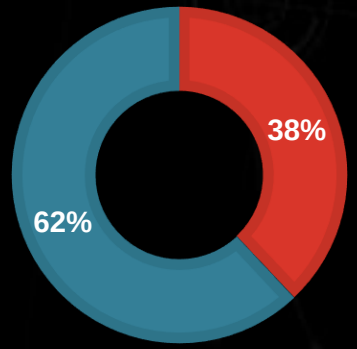
WORKS ON DAY ONE

CROWDSTRIKE

COMPONENTS OF THE ADVANCED MODERN ATTACK

ECRIME ADVERSARY EXPIDITED BREAKOUT TIME

2021 MALWARE V MALWARE FREE ATTACKS



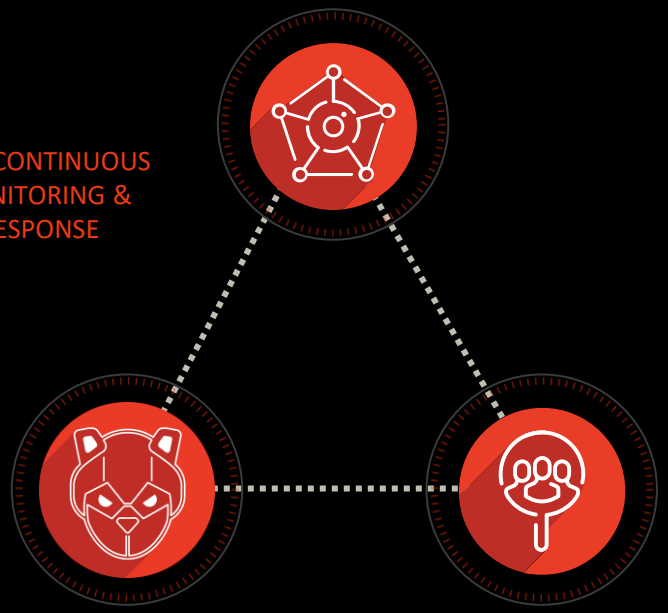
Falcon Complete Overview

HIDDEN Cost of Endpoint Security

REQUIREMENTS	COST
ACQUIRING ENDPOINT SECURITY TECHNOLOGY	$
IMPLEMENTING, CONFIGURING AND TUNING	$$
MANAGING, MAINTAINING AND UPDATING	$$$
MONITORING, TRIAGING AND ANALYZING ALERTS	$$$
RESPONDING TO AND REMEDIATING INCIDENTS	$$$
THE COST OF A DATA BREACH	$$$$

People

Effective Monitoring & Response



	Industry Average *	Continuous Monitoring & Response
Time to Detect	120 Hours	**1 Minute**
Time to Investigate	11 Hours	**6 Minutes**
Time to Remediate	31 Hours	**29 Minutes**

* Source: CrowdStrike 2020 Global Security Attitude Survey

FALCON COMPLETE EXCEEDS THE 1:10:60 GOAL

FALCON COMPLETE Stops BREACHES WITH PLATFORM, Intelligence, and EXPERTISE

COMPREHENSIVE PLATFORM

FALCON DISCOVER
IT HYGIENE

UNDERSTAND
CUSTOMER ASSETS AND RISK

FALCON INSIGHT
EDR

RECORD AND ANALYZE
ENDPOINT TELEMETRY

FALCON PREVENT
NGAV

BLOCK
99% OF TRADECRAFT

FALCON IDENTITY THREAT PROTECTION
ITP

PROTECT AND ENFORCE
IDENTITIES AND IDENTITY STORES

UNIQUE EXPERTISE & INTEL

FALCON OVERWATCH 24/7
HUNTERS

FALCON COMPLETE TEAM
24/7 RESPONDERS

HUNT AND RESPOND
CROWDSTRIKE PEOPLE AND PROCESS

CROWDSTRIKE