

# Darktrace and CrowdStrike: How the Integration between Industry Leaders Benefits Utilities

Greg Gray | Cybersecurity Services | NISC

Jay Patel | Cybersecurity Specialist | Cumberland EMC

# THE CHALLENGE

# EXISTING SOLUTIONS

## WHY THEY DON'T SOLVE MODERN NETWORK SECURITY CHALLENGES



### Lack of Visibility

Traditional NDR lacks coverage of OT, cloud, remote workers and identities, leaving blind spots. EDR and most XDR lack native network visibility.



### Historical Attack Data

Over-reliance on 'known bad'. Blind to novel and unknown threats. Creates false positives and responsible for existing SOC model that leads to zero-day risk.



### Alert Fatigue

Guessing game of detecting alerts and lack of investigation context across all IT domains has left the SOC reliant on manual efforts, integrations, task automation, and still years behind in triage.



### Business Disruption

Pre-determined, 'one size fits all' response actions have become the norm with the expectation of business operation disruption.

nisc

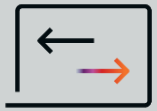
# DETECTION EXAMPLES

## COMPLETE COVERAGE FOR MITRE ATT&CK CATEGORIES



### Internal Reconnaissance

- Device / Suspicious SMB Scanning Activity
- Device / Network Scan
- Device / RDP Scan
- Device / ICMP Address Scan
- Device / Suspicious Network Scan Activity



### Lateral Movement

- Device / Multiple Lateral Movement Model Breaches
- Anomalous Connection / Unusual Admin RDP Session
- Device / SMB Lateral Movement
- Compliance / SMB Drive Write



### C2 Communication

- Anomalous Server Activity / Outgoing from Server
- Anomalous Connection / Multiple Connections to New External TCP Port
- Anomalous Connection / Rare External SSL Self-Signed
- Device / Suspicious Domain



### Exfiltration

- Unusual Activity / Enhanced Unusual External Data Transfer
- Anomalous Connection / Data Sent to Rare Domain
- Unusual Activity / Unusual External Data Transfer
- Compliance / FTP / Unusual Outbound FTP

nisc

# INTEGRATION POINTS BETWEEN DARKTRACE AND CROWDSTRIKE

# SINGLE PANE OF GLASS

## IT + OT + EMAIL + NDR + XDR VISIBILITY

DARKTRACE

CROWDSTRIKE

**57% of organizations** report that they plan to integrate Network security products focused on threat detection into their current XDR toolset.

Gartner

DARKTRACE DETECT™

Enhance Detection with CVE Data and CrowdStrike Alerts

DARKTRACE RESPOND™

Manually Trigger a CrowdStrike Device Quarantine via the Darktrace UI

nisc

# BENEFITS

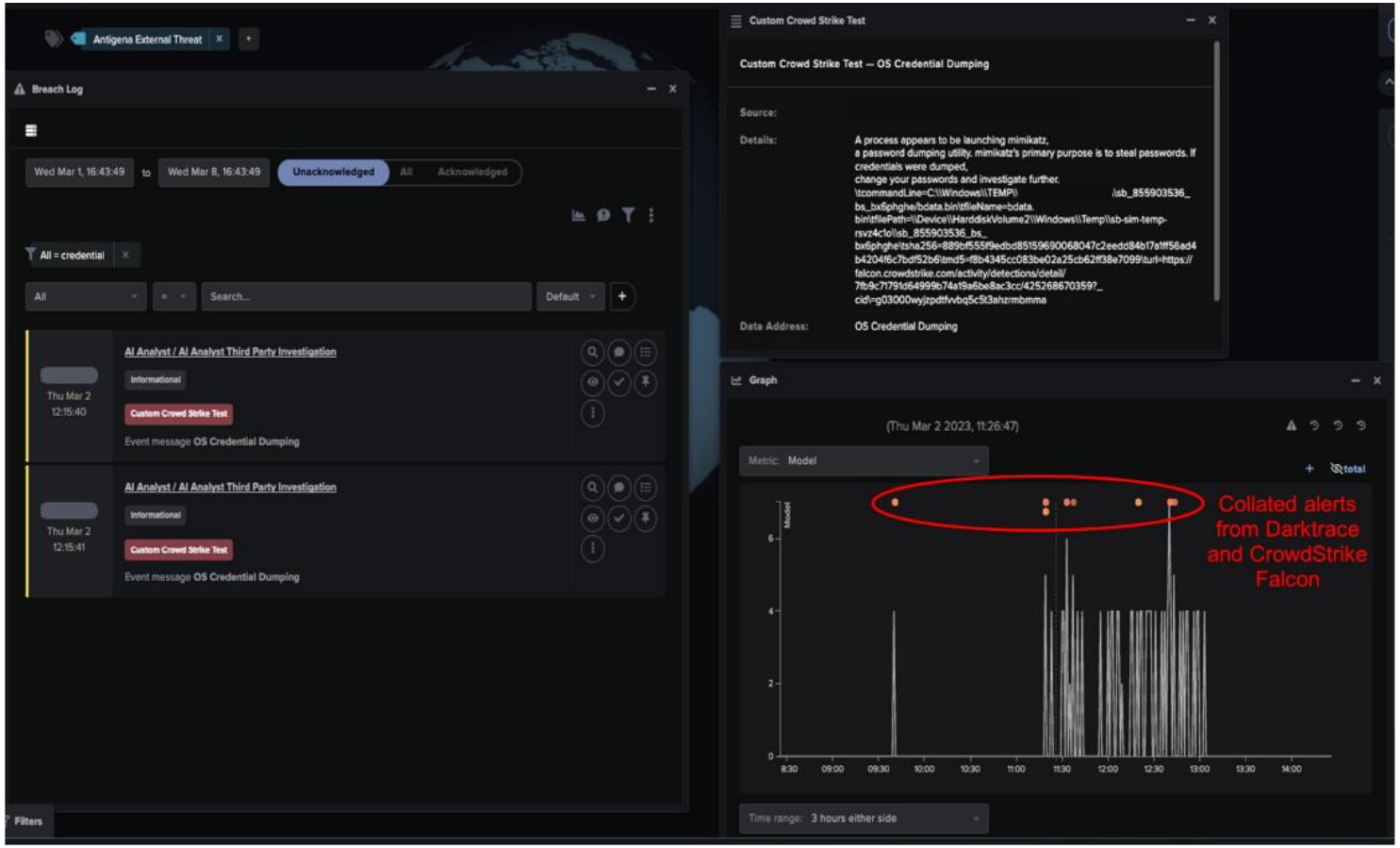
## IT + OT + EMAIL + NDR + XDR VISIBILITY

### What are we trying to accomplish?

- Reduce alert fatigue
- Detect attacks earlier
- Respond efficiently

### How does this Darktrace/CrowdStrike integration work?

- Darktrace ingests endpoint telemetry from CrowdStrike
- This telemetry data enriches AI investigations with endpoint context
- Darktrace can then invoke endpoint isolation via CrowdStrike
- Enhanced Darktrace's broader Network, Email, Identity, Cloud and OT detections




Mimikatz alerts from both Darktrace and CrowdStrike are organized in one place thanks to Darktrace Cyber AI Analyst

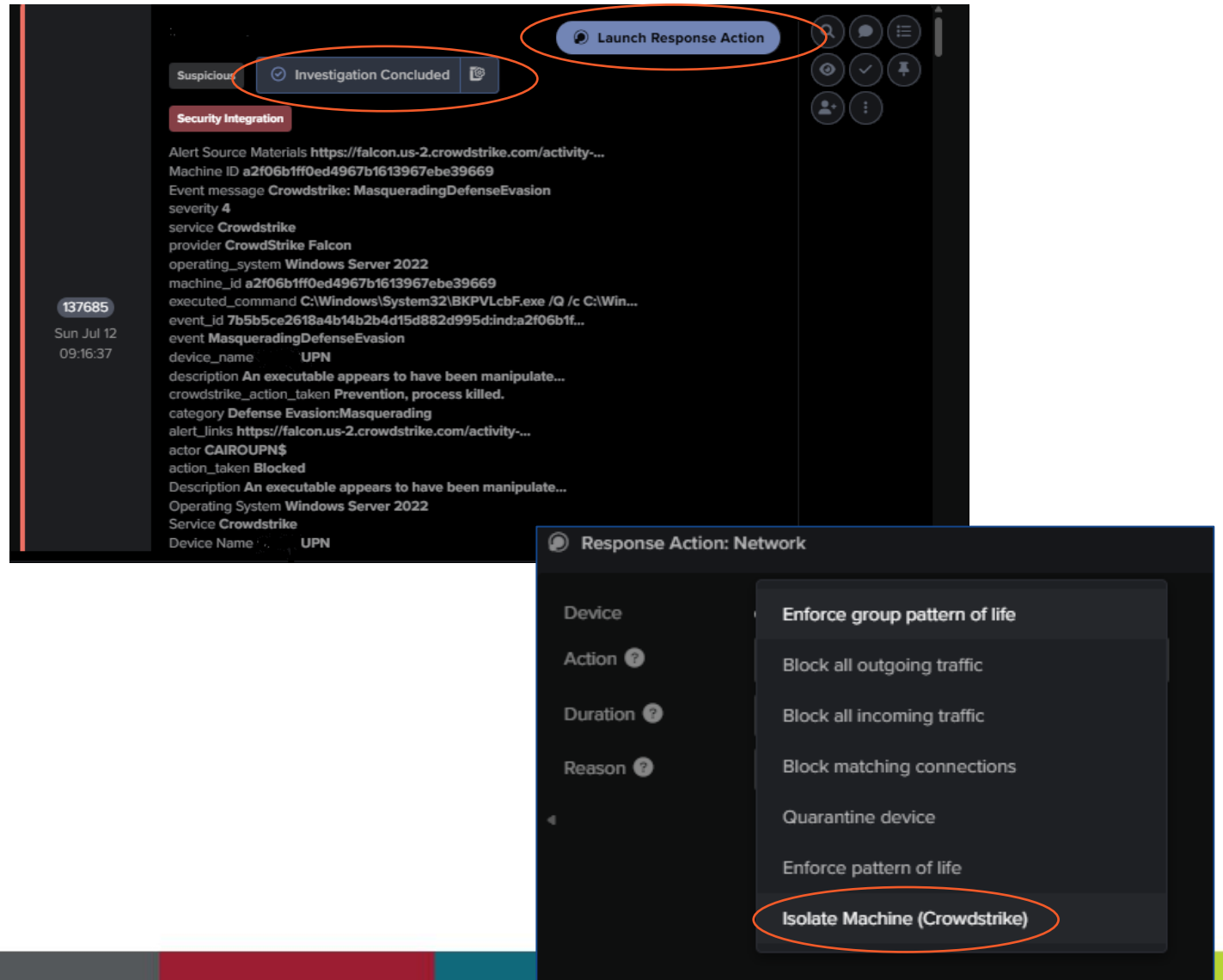
# INTEGRATION FEATURES

DARKTRACE

CROWDSTRIKE

## Key Integration Features

- Bi-directional communication between Darktrace and CrowdStrike Falcon API every 60 seconds
- Darktrace pulls CrowdStrike Falcon data for analysis in AI Analyst, triggering both Darktrace model breach and AI Analyst investigation around high-fidelity CrowdStrike alerts
- Reduces the need to switch between consoles
- Darktrace retrieves endpoint data including CVE risks for analysis via CrowdStrike Spotlight
- Darktrace can trigger CrowdStrike device quarantines within Darktrace UI via the Falcon Endpoint Protection agent




nisc

# NISC MSS

# NISC MSS



## NISC Managed Detection & Response

- **24/7 Expert Support:** NISC SOC manages triage, investigation, and escalation for comprehensive threat containment
- **Operational Excellence:** Focus on security outcomes with monthly performance reports & dedicated support
- **Comprehensive Coverage:** Get the most out of your Darktrace investments with coverage for network, cloud, OT, endpoints, and SaaS applications



## NISC Managed Threat Detection

- **Immediate Notifications:** Receive prompt alerts for incidents requiring immediate action.
- **24/7 Threat Detection:** Enhance your team's capabilities with round-the-clock monitoring
- **Expert Triage:** NISC SOC analysts prioritize high-alert incidents within your digital ecosystem



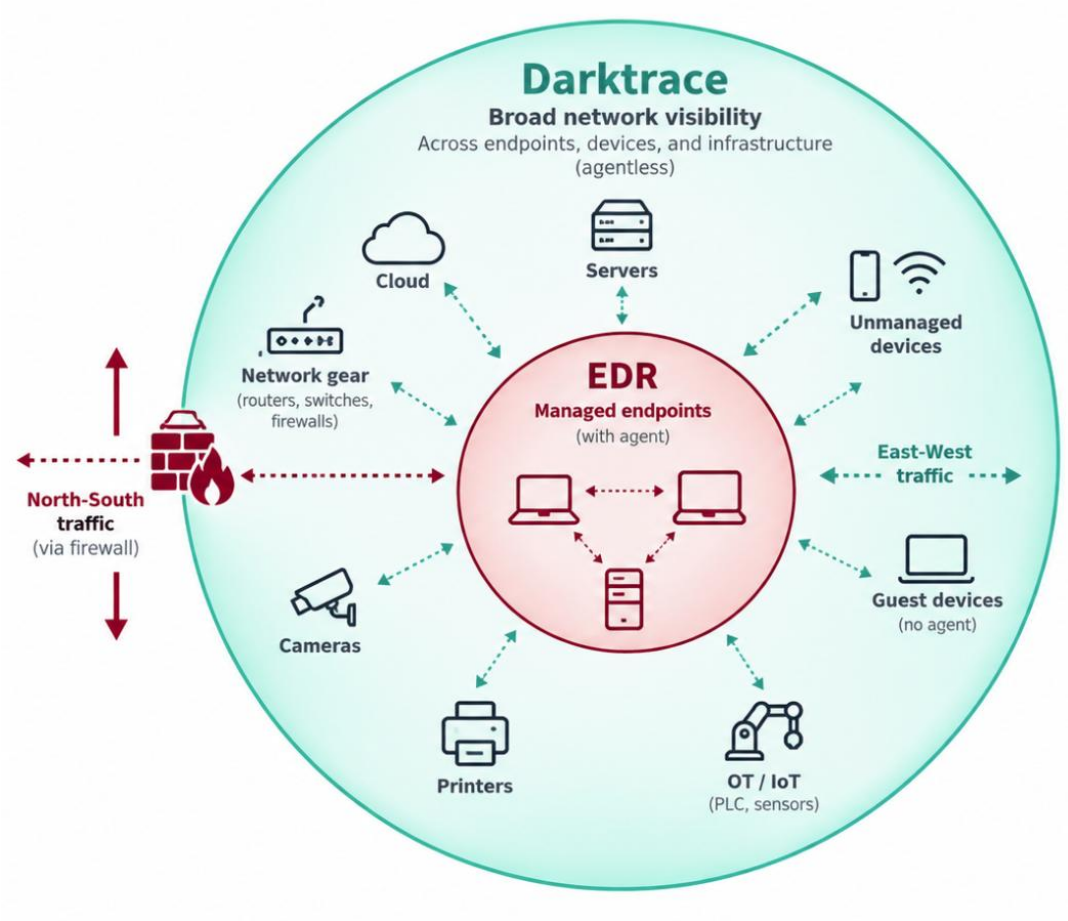
## NISC Security Operations Support

- **Live Threat Investigation Assistance:** Send queries for expert help during active threat investigations
- **Operational Support:** Collaborate with Analysts for assistance during regular security operations
- **Unlimited Queries:** Unlimited questions during live investigations or day-to-day operations

DARKTRACE

# DARKTRACE

**Darktrace** introduces additional insights into network traffic. Visibility at the edge and endpoint levels are common practice. Expanding visibility and security at the network layer is the next step to expanding cyber defenses.



# DARKTRACE NAMED A LEADER

## 2025 Gartner® Magic Quadrant for Network Detection and Response

**Darktrace** is a **Leader** in this Magic Quadrant. Its NDR, known as Darktrace / NETWORK, focuses on providing advanced threat detection and autonomous response capabilities by leveraging its core **Self-Learning AI**.




Gartner® Magic Quadrant™ for Network Detection and Response

Gartner

# DARKTRACE NAMED A LEADER

## 2025 Gartner® Magic Quadrant for Email Security

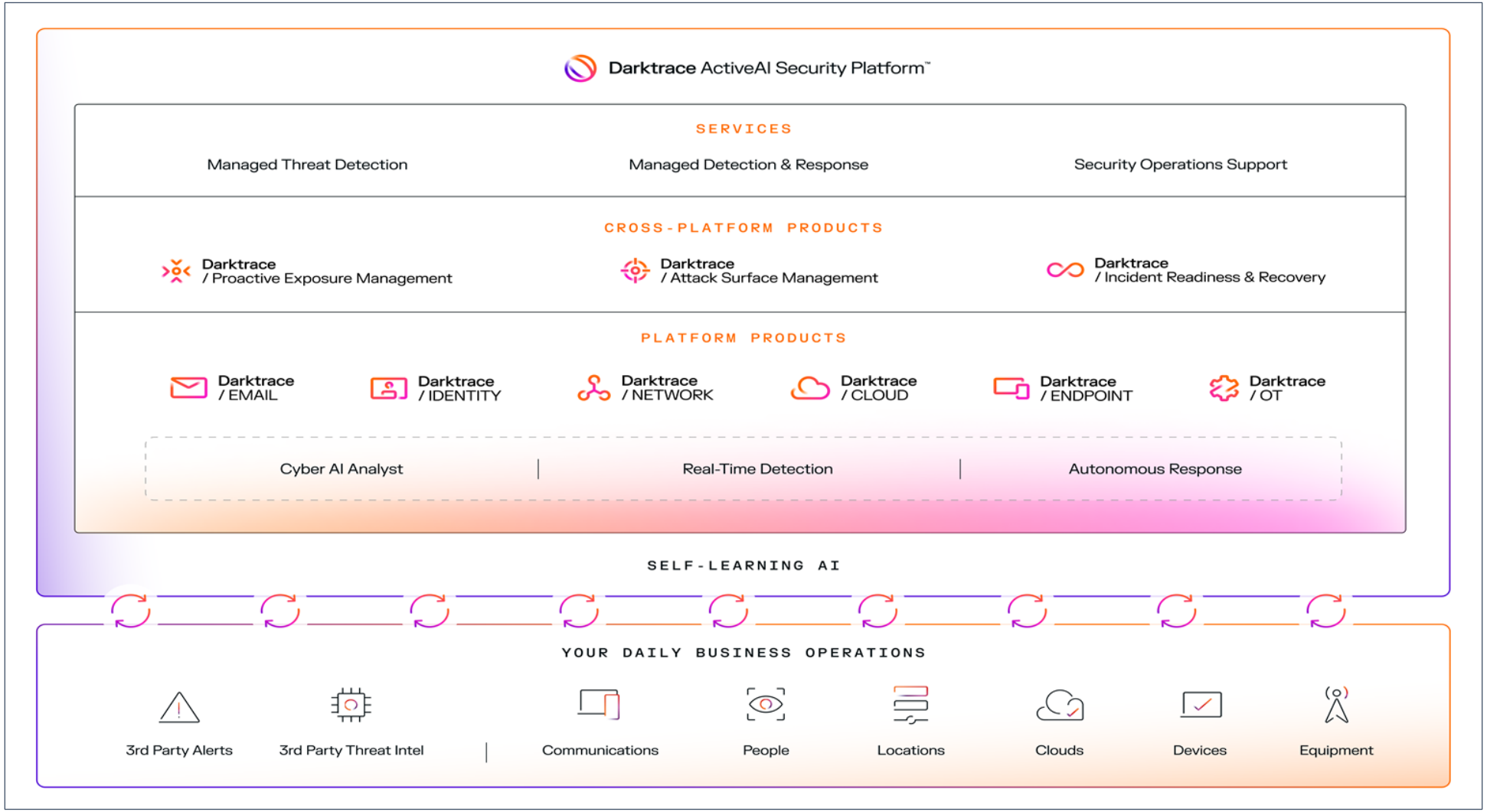
**Darktrace / EMAIL** provides a broad set of email security capabilities designed to target advanced threats. Darktrace expanded its capabilities and strategy, significantly **improving** both **vision** and **execution** potential.




Gartner® Magic Quadrant™ for Email Security

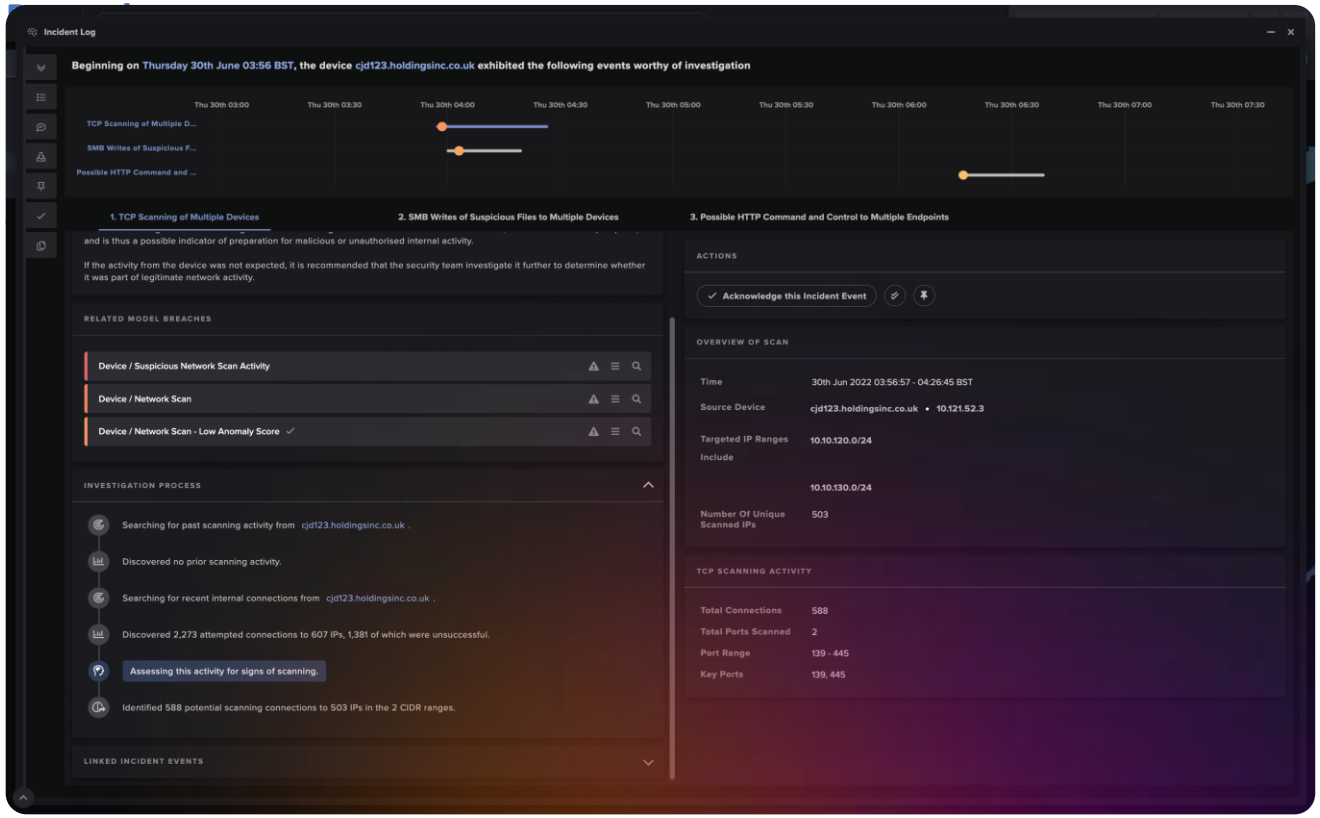
Gartner

# DARKTRACE OVERVIEW



# DARKTRACE / NETWORK

## THE INDUSTRY'S MOST ADVANCED NDR SOLUTION




### Detection

Self-Learning AI detects known and novel threats across your entire network, without relying on historical attack data.

### Investigation

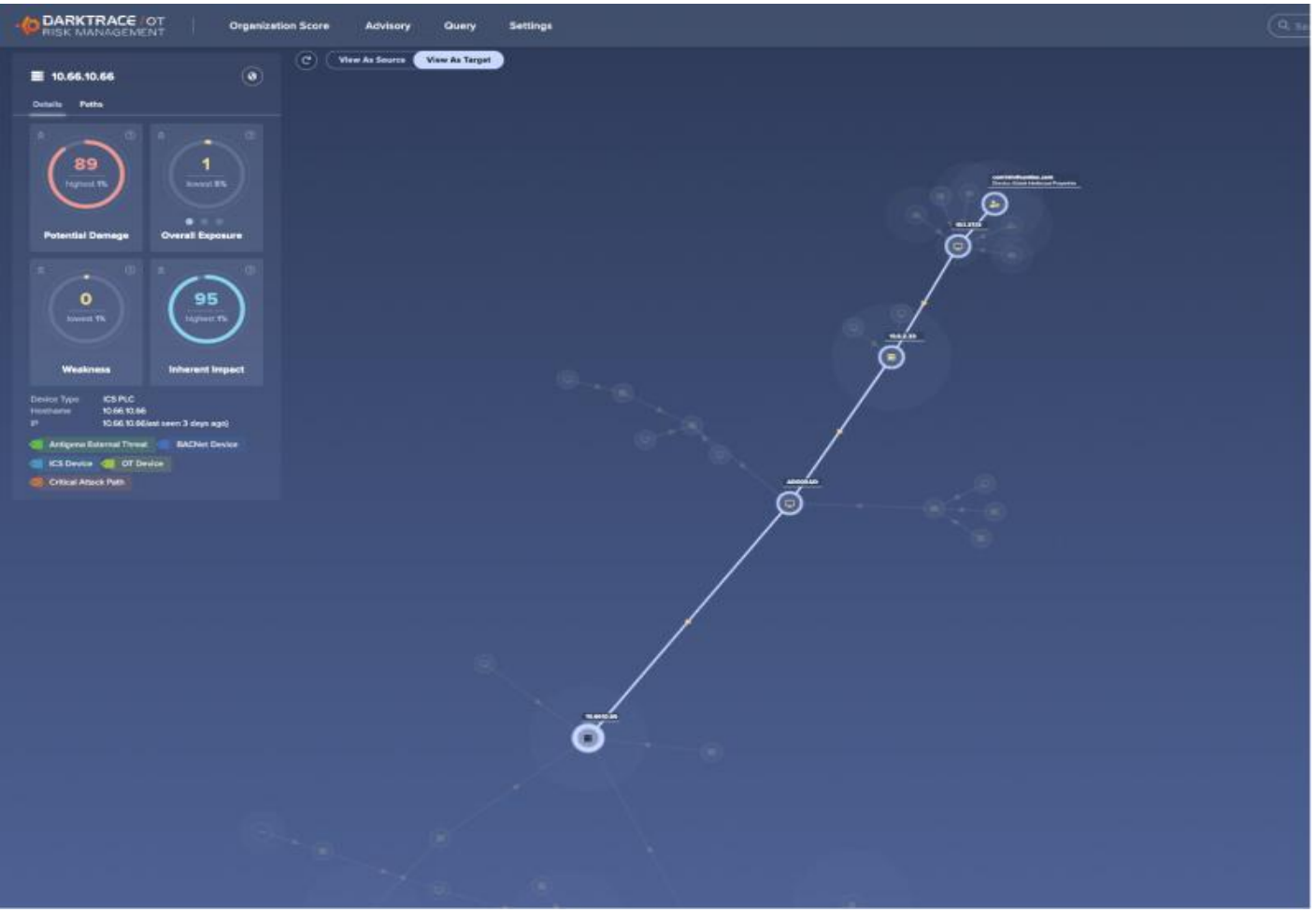
Transform your security operations and investigate all relevant alerts with the industry's first AI Analyst.

### Response

Autonomously respond to threats in real-time with precise actions to minimize business disruption.

# DARKTRACE / OT

## COMPREHENSIVE OT SECURITY FOR CRITICAL INFRASTRUCTURE




### Unified Visibility

Achieve greater visibility of OT and IT devices across every level of the Purdue Model.

### Bespoke Risk Management

The only OT-focused security solution which understands
risk in your environment, creating bespoke risk reduction recommendations and patch management plans.

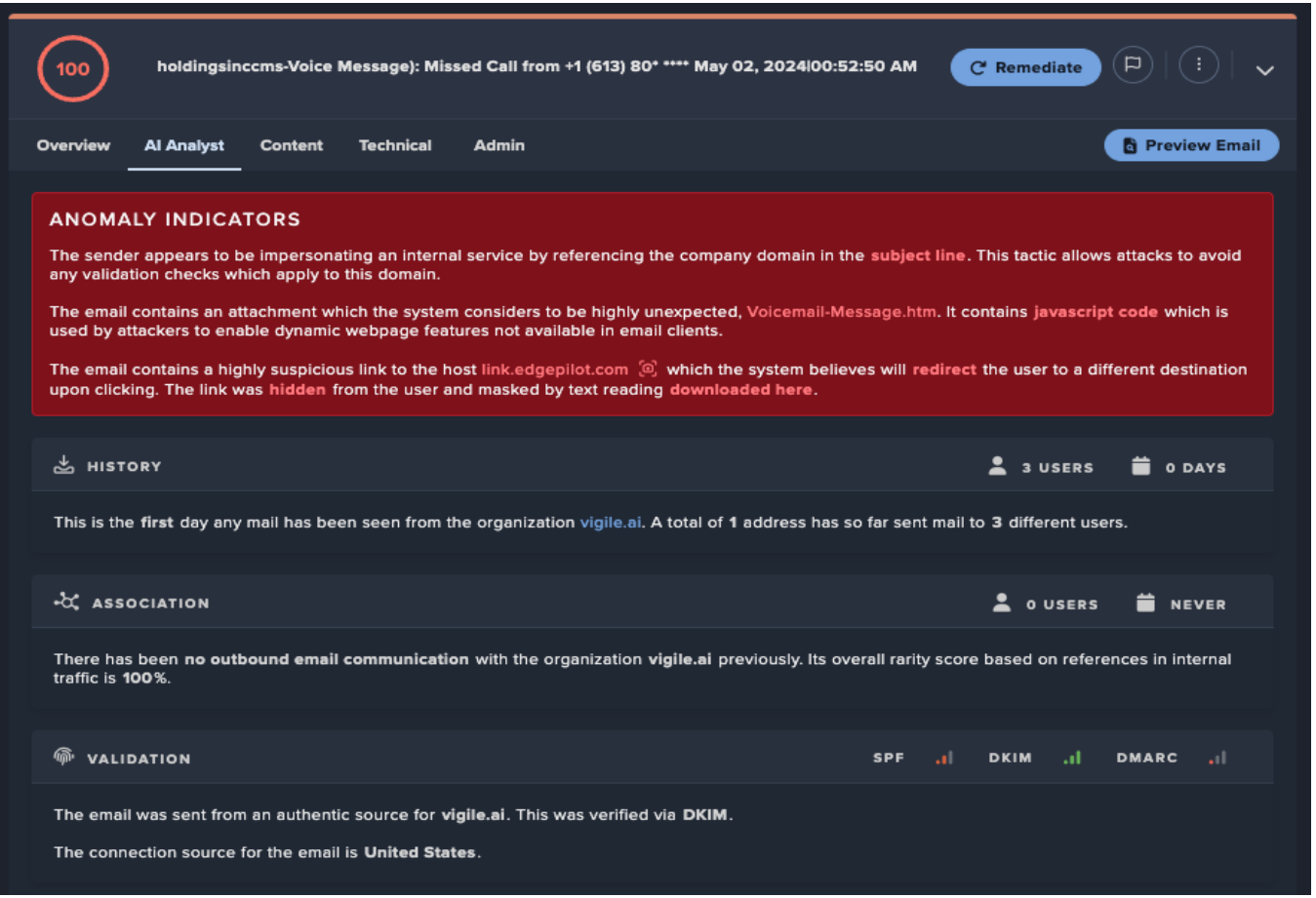
### Threat Detection & Response powered by Self-Learning AI

The industry's only AI-led OT security solution that combines real-time threat detection, investigation, and response.

nisc

# EMAIL PROTECTION

## CONTEXT-AWARE EMAIL DEFENSE

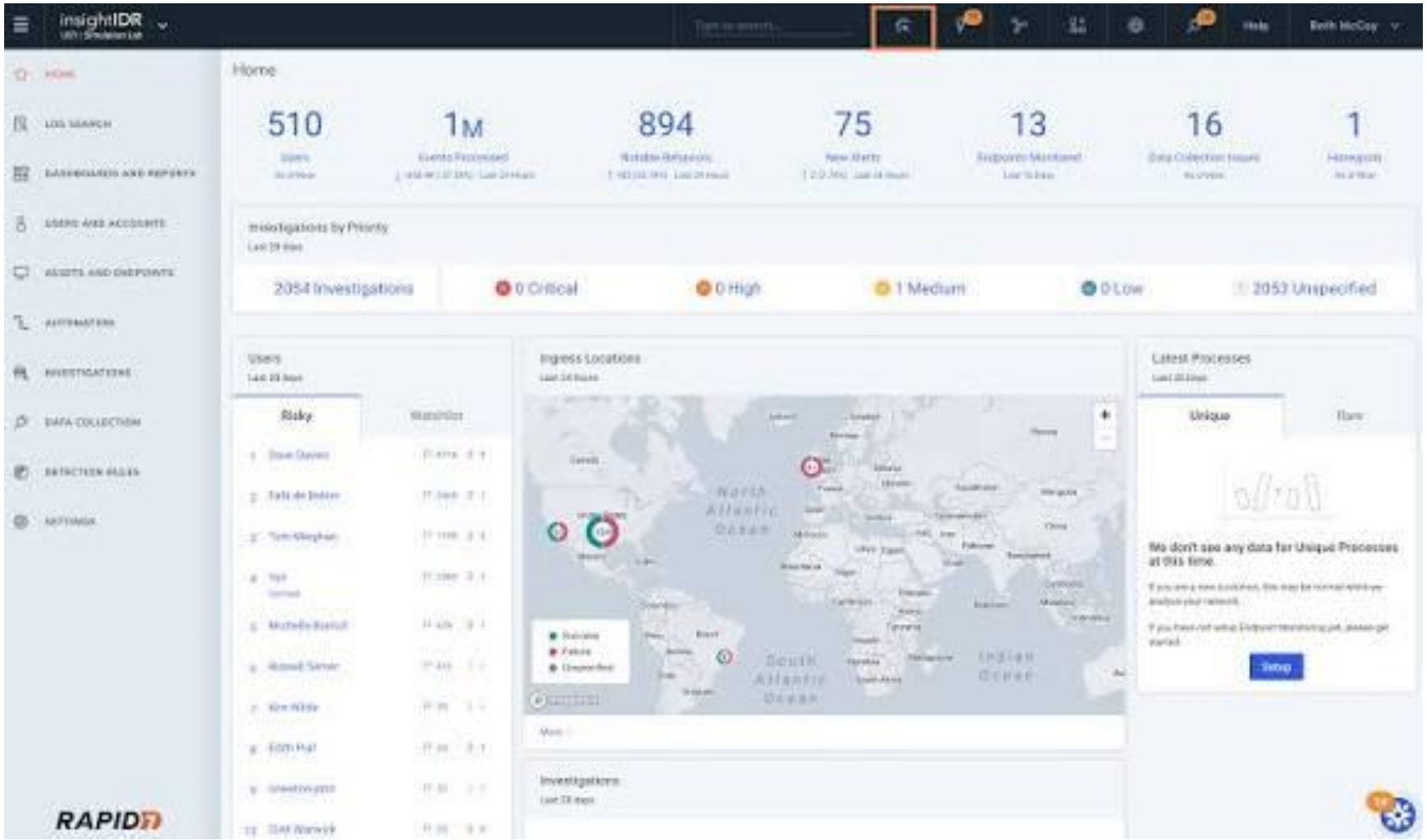



- Creates behavioral profiles for every person
- Identifies relationships between senders and receivers
- Real-time determination of email legitimacy
- Configurable actions based on threat severity

# VALUE ADD TO DARKTRACE

# RAPID7 SIEM

- Syslog ingestion
- SIEM with 1-year retention in hot cloud storage with interactive dashboards and reports



# RAPID7 IVM

- Bi-weekly and on-demand scanning
- Interactive and emailed reports
- Basic cybersecurity hygiene



# CROWDSTRIKE EPP

# CROWDSTRIKE NAMED THE LEADER

## 2025 Gartner® Magic Quadrant for Endpoint Protection Platforms

Positioned **Furthest** for Completeness of Vision and **Highest** In Ability to Execute



# OUTPACE AND OUTSMART THE ADVERSARY

## WITH THE MODERN ENDPOINT SECURITY LEADER



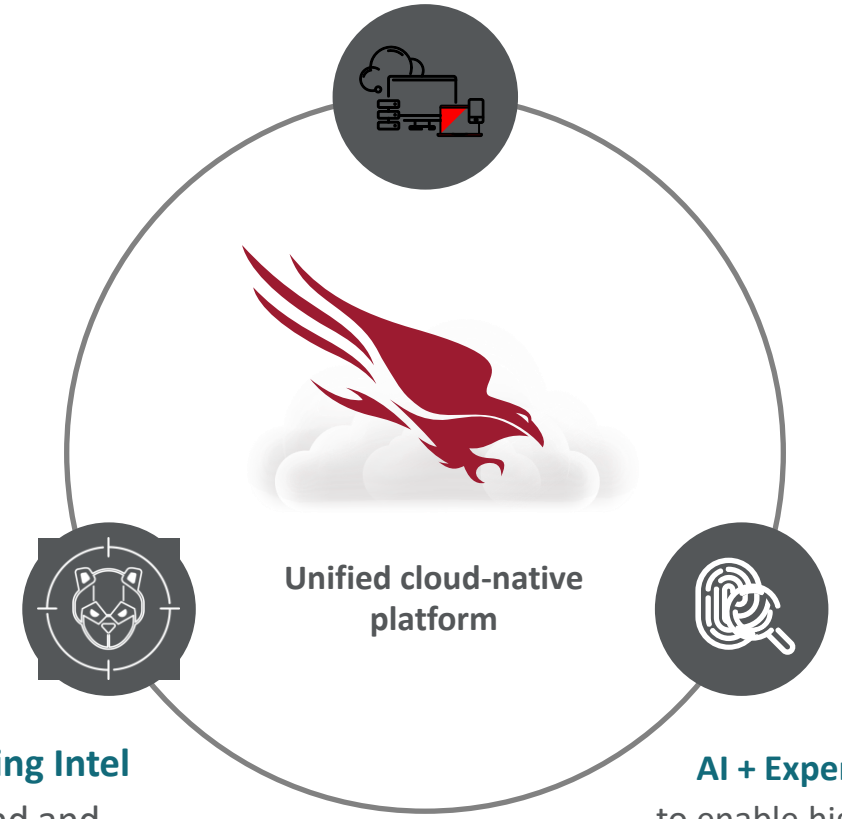
| | |
|---|---|
| **Complete visibility** | Track and stop the adversary |
| **AI-powered prevention and detection** | Stop advanced attacks with world-class AI |
| **Unified investigations** | Build comprehensive picture of an attack |
| **Integrated response** | Respond rapidly with surgical precision |
| **Easy to deploy and operate** | Deploy with ease, defend with confidence |

nisc

# NISC'S CROWDSTRIKE PARTNERSHIP

- **CrowdStrike** selected after extensive evaluation of all leading solutions (CrowdStrike, SentinelOne, MS Defender vs legacy Carbon Black)
- **CrowdStrike** was only EPP to pass 5-of-5 of ransomware and malware unit tests
- **24/7 management**, monitoring, support and escalation by **NISC SOC team** if subscribed to NISC MSS

**10+ years of EDR innovation**
to accelerate detection and response



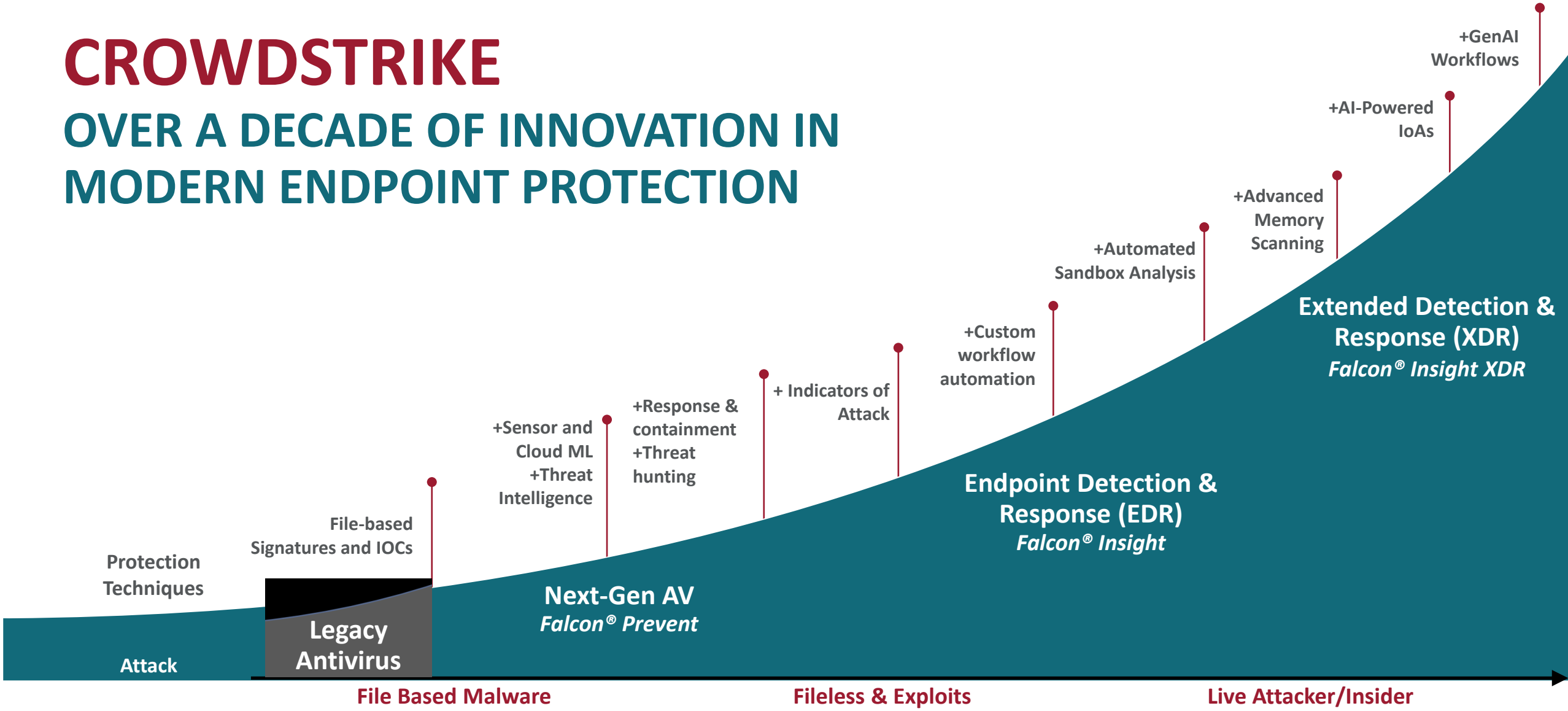

**Industry-leading Intel**
to understand and outsmart the adversary

**AI + Expert Feedback Loop**
to enable high-fidelity detection

nisc

# CROWDSTRIKE

## OVER A DECADE OF INNOVATION IN MODERN ENDPOINT PROTECTION




nisc

# INDUSTRY CHALLENGES

## AI-POWERED ATTACKS ON THE RISE

### Network Complexity

Beyond on-prem into the cloud, hybrid and virtual environments, including remote worker devices.

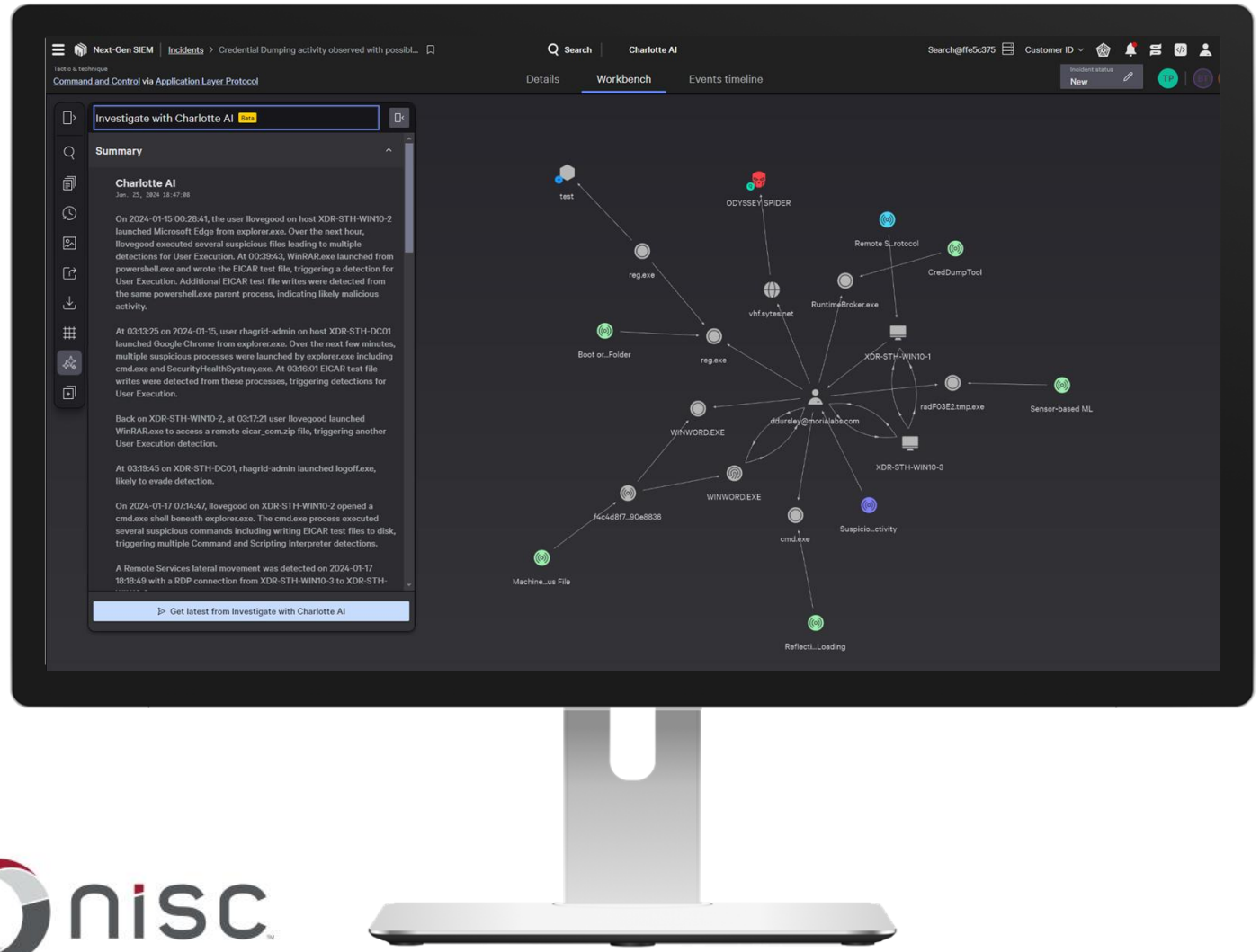
### Novel Threats

Zero days, variants of known attacks, ransomware, supply chain attacks, insider threats.

### IT Team Pressure

IT burnout, limited resources, hiring challenges, endless false positives and alert fatigue.

# UNIFY INVESTIGATIONS WITH A SINGLE COMMAND CONSOLE




Accelerate security operations across the Falcon® platform

## Rapid investigation

Instantly pivot from detections to search with easy AI-powered workflows

## Complete understanding

Visualize the full attack path and explore other potentially impacted hosts

## Full context

Integrated view with all related threat intel, context and artifact relationships

# NISC CYBERSECURITY PARTNERS

## 24/7 Managed Security Services

SIEM & HOST INTRUSION DETECTION SYSTEM

RAPID7

24/7 NDR/MONITORING

DARKTRACE

VULNERABILITY SCANNING

RAPID7 insightVM

NEXT GENERATION FIREWALL

SONICWALL

MFA

CISCO DUO

BACKUP

veeam

PENTESTING-AS-A-SERVICE (PTaaS)

HORIZON3.ai

~~TRUST BUT~~ VERIFY

CYBER AWARENESS EDUCATION

KnowBe4

Human error. Conquered.

PATCH MANAGEMENT

ninjaOne

ENDPOINT DETECTION & RESPONSE

CROWDSTRIKE

nisc

# CONNECT WITH US!


## JAY PATEL

Cybersecurity Specialist

jpatel@cemc.org

## GREG GRAY

Cybersecurity Services

greg.gray@nisc.coop