



# Intelligent Shield: AI-driven approach for contemporary incident response strategies

Nikitas Kladakis – General Manager

# Security Challenges and Threat Landscape

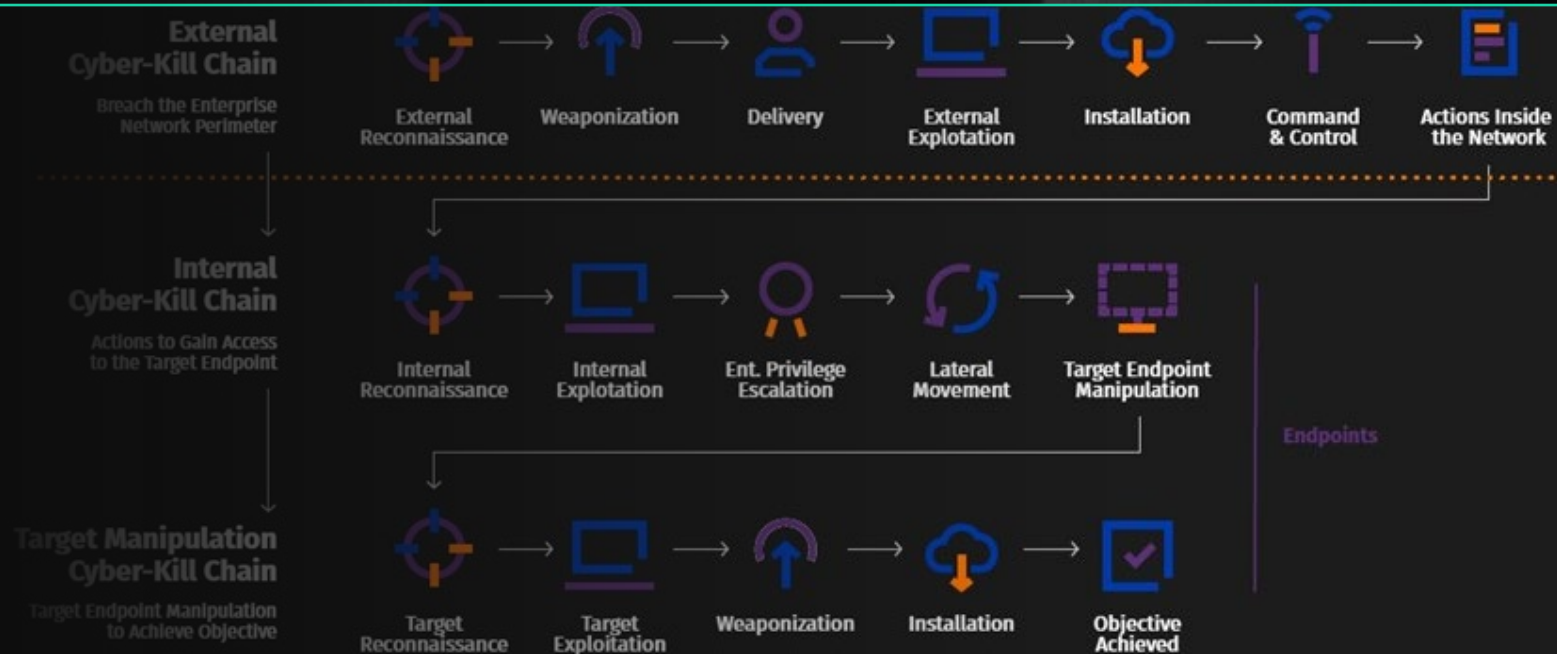


# Cybersecurity Challenges

- 🌐 **Digital transformation**
- 🌐 **Teleworking - Work from Everywhere**
- 🌐 **New Technologies (OT/IoT, 5G...)**
- 🌐 **Cloud Services**
- 🌐 **Traditional Security Controls**
- 🌐 **Legacy Systems**



# Ransomware: Stealthy Exploits and AI Battlefields






# Rise of AI-Directed Cyberattacks

Hackers will use AI to analyze attack strategies, thereby enhancing their likelihood of success. Also, they will use AI to heighten the speed, scale and scope of their activities

# Cyberattacks to Security Systems

The image is a composite graphic. On the right side, there is a silhouette of a person wearing a hooded sweatshirt, representing a hacker. The background is dark with a teal/cyan tint. On the left side, there is a complex digital network of lines and nodes. A prominent feature is a broken padlock, symbolizing a security breach. The text 'Cyberattacks to Security Systems' is overlaid on the left side in a white, sans-serif font.

A hooded figure, likely representing a hacker, is shown from the chest up, holding a smartphone. The figure's face is obscured by a glowing circular interface that displays a silhouette of a man in a suit. The background is a dark blue grid with a network of white lines connecting various icons. These icons include silhouettes of people in suits and question marks, suggesting a complex network of communication or data exchange. The overall aesthetic is futuristic and digital, with a focus on cybersecurity and the theme of phishing attacks.

# Phishing attacks based on AI continue to plague businesses



# Supply Chain and Critical Infrastructure cyberattacks

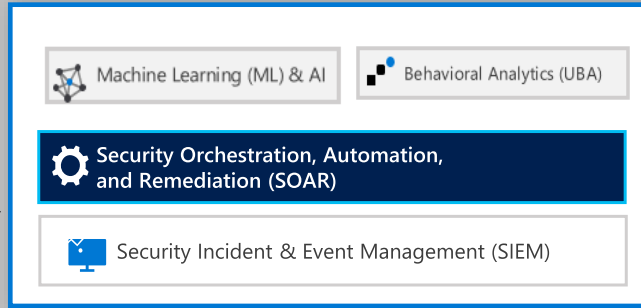


# AI-Driven Incident Investigation Technologies and Services



# AI-Driven Incident Response Operational Model

**Web Portal**  
Correlated/Unified Incident View



**Extended Threat Intelligence**

**Customer**

**Deep Insights**  
Actionable alerts from an XDR tool with deep knowledge of assets and ML

**SOCaaS (SIEM-based)**  
Provide actionable security alerts, raw logs, or both

- Carbon Black, Symantec
- FORTINET, SOPHOS
- zscaler, FIREEYE
- CYBERARK, Lookout
- Duo, Palo Alto, Check Point
- CrowdStrike, Barracuda

**AI-Driven Extended Detection and Response (XDR) (based on Microsoft XDR)**



**Infrastructure & Apps**  
Java, JBoss, .NET, php, .NET, vmware, aws, windows, etc.

**PaaS**  
Azure, AWS, etc.

**Identity & Access Management**  
LDAP, Ping, Oracle, Okta, SailPoint

**Endpoint & Mobile**  
Windows, Android, Apple

**Modern & SaaS Applications**  
Office 365, G, Salesforce, Box, etc.

**Information**  
Oracle, SQL Server, MySQL, IBM DB2, etc.

**Raw Data**  
Security & Activity Logs

Microsoft Azure
Search resources, services, and docs
admin@contoso.com  
CONTOSO

Home > Azure Sentinel
Search (Ctrl+F)
X

**Azure Sentinel - Overview**

GENERAL

- Overview
- Logs

THREAT MANAGEMENT

- Incidents
- Dashboards
- User analytics
- Hunting
- Notebooks

CONFIGURATION

- Getting started
- Data collection
- Analytics
- Playbooks
- Community
- Workspace

Last week (1/21/2018-1/27/2018)

**8.2M** ↑ 978.4K

EVENTS

**39** ↑ 6

ALERTS

**18** ↑ 4

INCIDENTS

**INCIDENTS BY STATUS**

NEW (7)
IN PROGRESS (4)
CLOSED (RESOLVED) (4)
CLOSED (DISMISSED) (3)

**Events and alerts over time**

- 89**
- 315K**
- 121K**
- 110K**
- 106K**

**Potential malicious events**

- 82K**
- 4K** ▲
- 78K** ▼

**Recent incidents**

- 9 Alerts**
- 9 Alerts**
- 8 Alerts**
- 8 Alerts**

**Most anomalous data sources**

- Azure AD
- Office
- SecurityEvents

**Democratize ML for your SecOps**

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

[Learn more >](#)

Microsoft 365 Defender

⚙️ ?

---

## Incidents

[Azure AD IP Alerts settings](#)
[Email notification](#)

Most recent incidents and alerts ▼

---

ExportCustomize columns
1 Week ▼

Filter set: [Save](#)

Severity: High, Medium, Low
✕
Add filter
Reset all

	Incident name	Incident Id	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sources
<input type="checkbox"/>	> Multi-stage incident on one endpoint reported ...	604741		■■■ High		Malware, Suspicious ac...		3/3	Endpoint, 365 Defender
<input type="checkbox"/>	> Credential access incident on one endpoint	605175	BRASS TYPHOON	■■■ High		Credential access		2/2	Endpoint
<input type="checkbox"/>	> E2E Alerts Streaming Detection Rule on one en...	606450		■■■ High		Malware		1/1	365 Defender
<input type="checkbox"/>	> Multi-stage incident involving Privilege escalati...	594464	immune +3	■■■ High	2 investigation states	Execution, Persistence, ...		629/629	Endpoint, 365 Defender
<input type="checkbox"/>	> Malware incident on one endpoint reported by ...	606966		■■■ High		Malware		2/2	Endpoint, 365 Defender
<input type="checkbox"/>	> Multi-stage incident on one endpoint reported ...	606964		■■■ High	2 investigation states	Persistence, Malware		4/4	Endpoint, 365 Defender
<input type="checkbox"/>	> E2E Mde Streaming Detection Rule on one end...	606904		■■■ High		Malware		1/1	Endpoint
<input type="checkbox"/>	> Multi-stage incident involving Persistence & Lat...	601248		■■■ High		Persistence, Defense ev...		449/449	365 Defender
<input type="checkbox"/>	> Multi-stage incident involving Privilege escalati...	590290	Ransomware +8	■■■ High	7 investigation states	Initial access, Execution...		101/129	Endpoint, 365 Defende..
<input type="checkbox"/>	> Multi-stage incident involving Privilege escalati...	588919	aA	■■■ High	2 investigation states	Execution, Persistence, ...		391/391	Endpoint, 365 Defender
<input type="checkbox"/>	> Multi-stage incident involving Privilege escalati...	598021	Defender Experts +10	■■■ High	2 investigation states	Persistence, Privilege e...		652/652	Endpoint, 365 Defender



## Extended Threat Intelligence

- Attack Surface
- Deep/Dark Web Scanning
- Threat Actor Tracking
- Threat Hunting

# AI-Driven Incident Investigation Methodology



- ↘ Initial Contact and Preparation
- ↘ Investigation
- ↘ Remediation
- ↘ Follow Up



# Initial Contact and Preparation

- Within hours of contacting ADACOM, immediate action is taken to simultaneously ensure the right next steps are taken, the correct players are engaged, and the necessary resources are assigned
- Remote IR assistance is provided to start initial analysis and deploy IR tools and Threat Analytics needed to quickly expand visibility throughout your environment.



A woman in a dark blue uniform and blue gloves is using a tool to inspect a window frame. The background is a light green wall.

# Investigation

---

- **Deep Scanning:** Assets, services affected, business impact, other attack vectors
- **Threat Hunting:**
- **Forensics Analysis:** IR Team help gain a full understanding of the threat
- **Remediation Planning:** Start planning for remediation, in parallel and in concert with the investigation



# Remediation

---

- **Secure and Validate**
- **Recover**

# Secure and Validate

---

- **Containment:** Cutting off the command and control of the threat actor
  - **Threat Actor Eviction** Evicting the threat actor from a contained network requires the orchestrated elimination of their tradecraft and resetting of compromised domains. ADACOM help validate containment actions
  - **Focused Security Hardening:** IR team guide and support tactical security control hardening efforts that will prevent re-entry by the threat actor.
- 



# Recover

---

- Restore directory services functionality and increase its security resilience to support the restoration of business
- Restore the affected systems to their pre-incident state
- Real Time Threat Monitor 24x7



# INCIDENT INVESTIGATION SUMMARY

## Follow Up

ADACOM leverage lessons learned during the incident to guide recommended response process improvements as well as strategic recommendations to help drive a security transformation roadmap

SECURITY  
BUILT ON TRUST

# Call us before you need us

---

## GREECE

25 Kreontos Str.,  
104 42, Athens  
+30 210 5193740

---

## UNITED KINGDOM

8950 Fitness Lane,  
Suite 100 Fishers, IN 46037  
+44(0) 317 588 3131

---

## CYPRUS

10 Katsoni Str.,  
1082, Nicosia  
+357 22 444 071

