

ADACOM

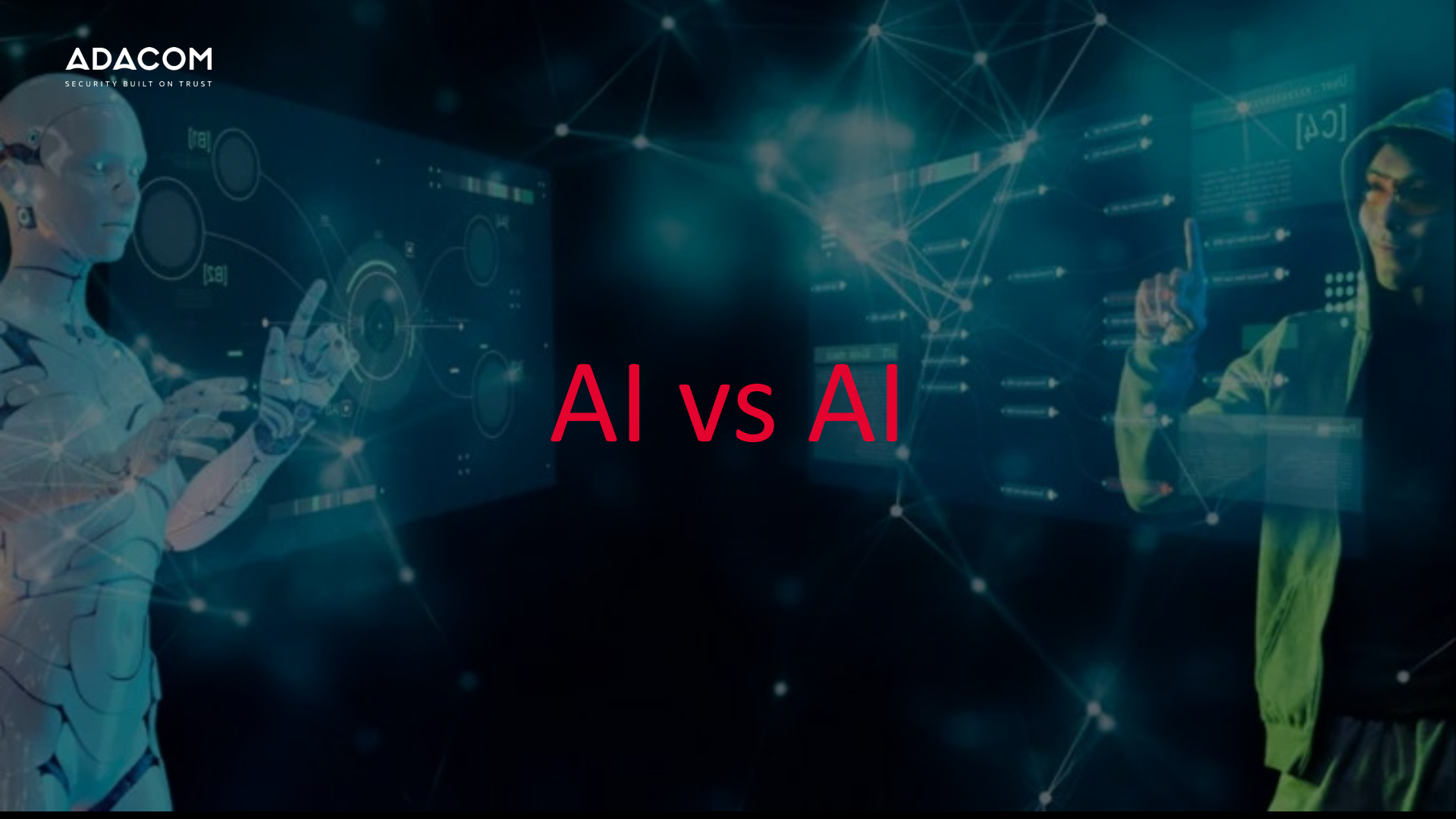
SECURITY
BUILT ON TRUST



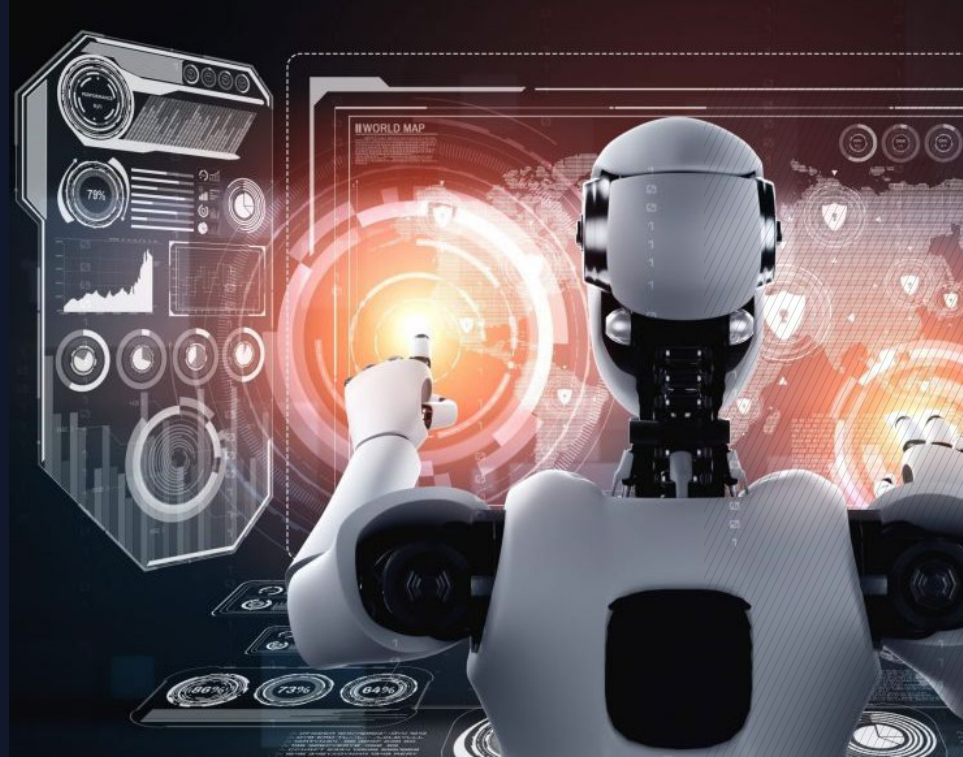
AI CyberDefense in the Edge of Tomorrow

Nikitas Kladakis – General Manager

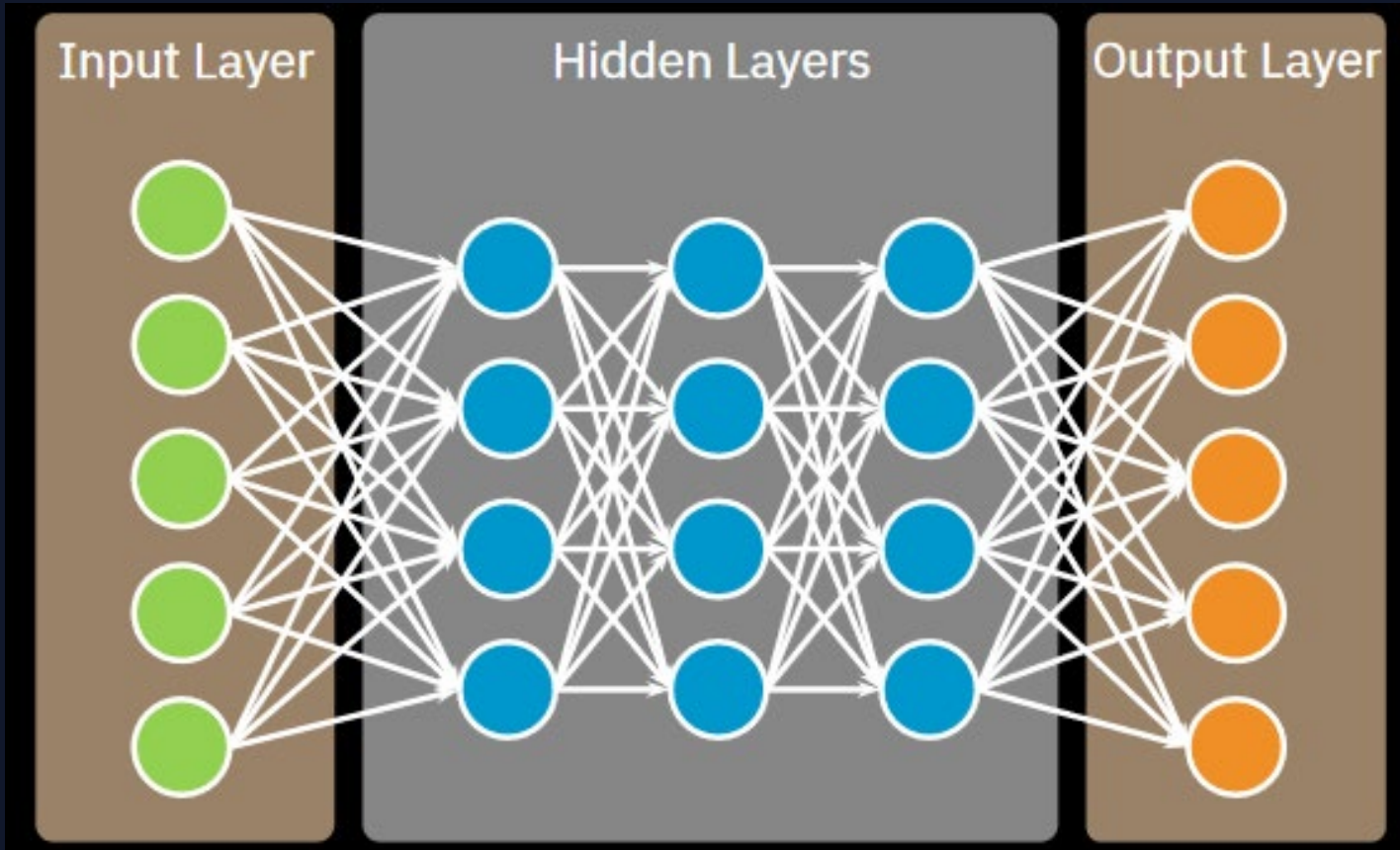
AI vs AI



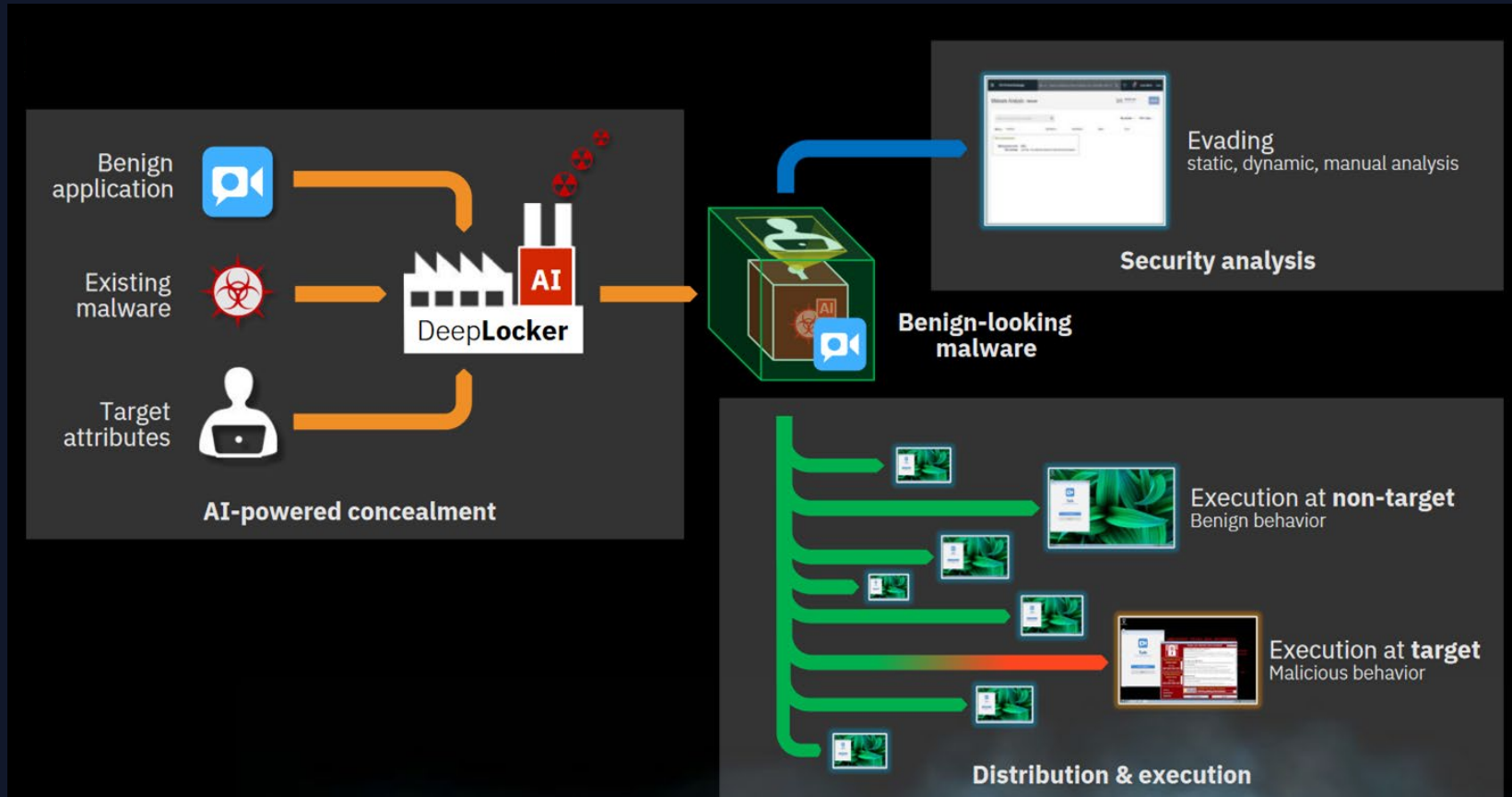
AI vs AI: DeepLocker



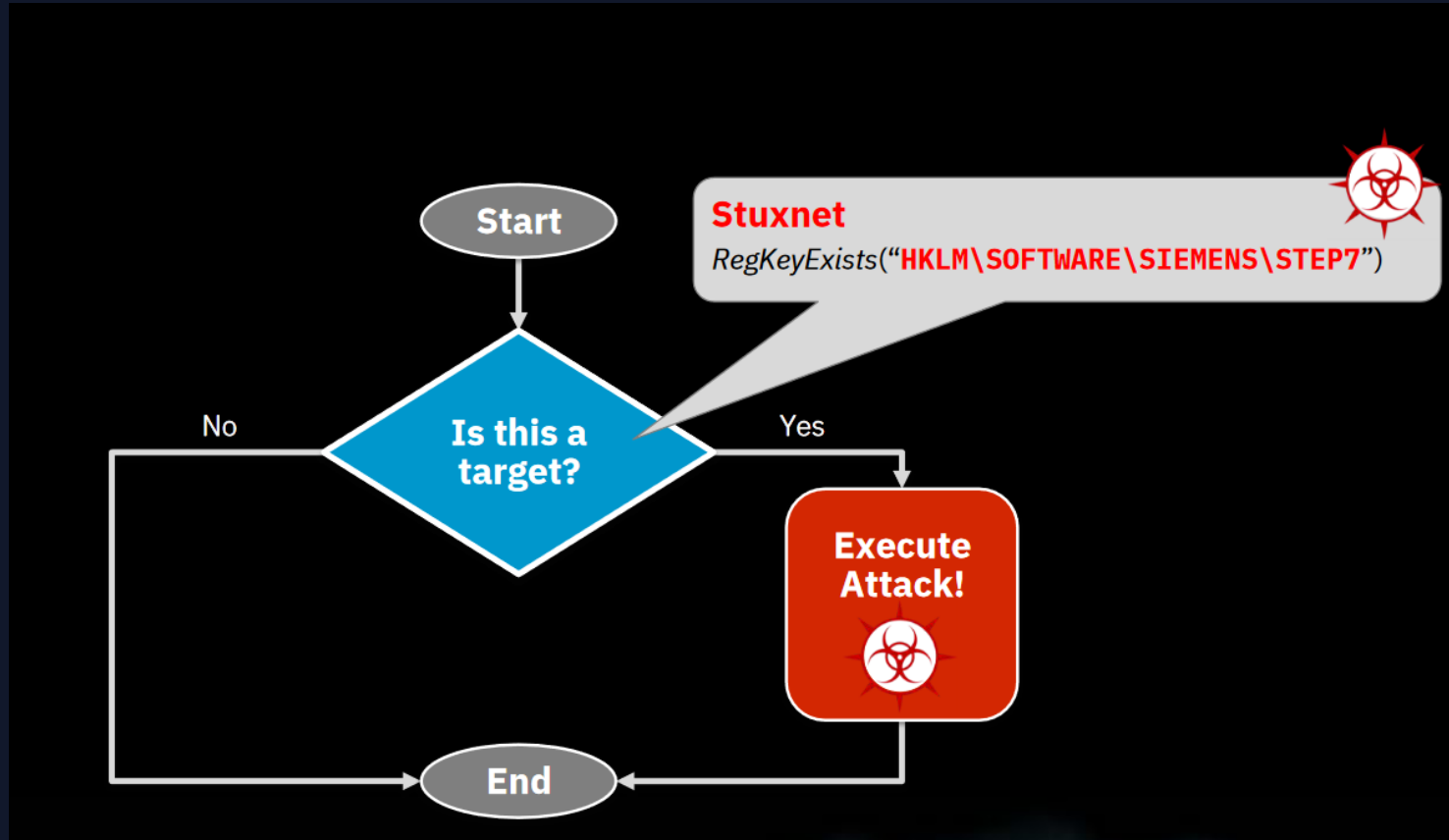
What is a Deep Neural Network (DNN)?

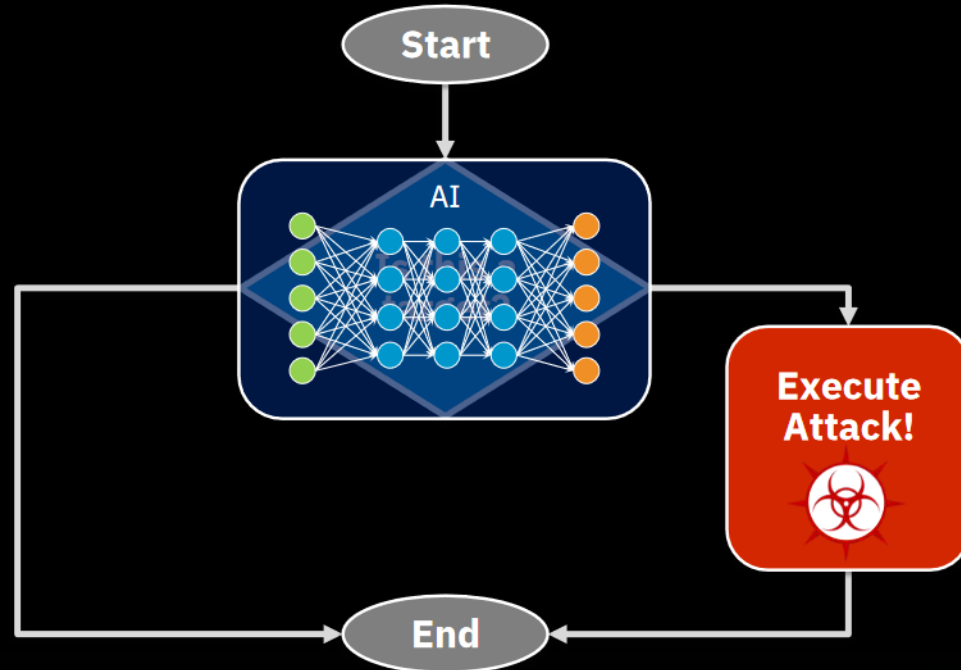


DeepLocker - Overview

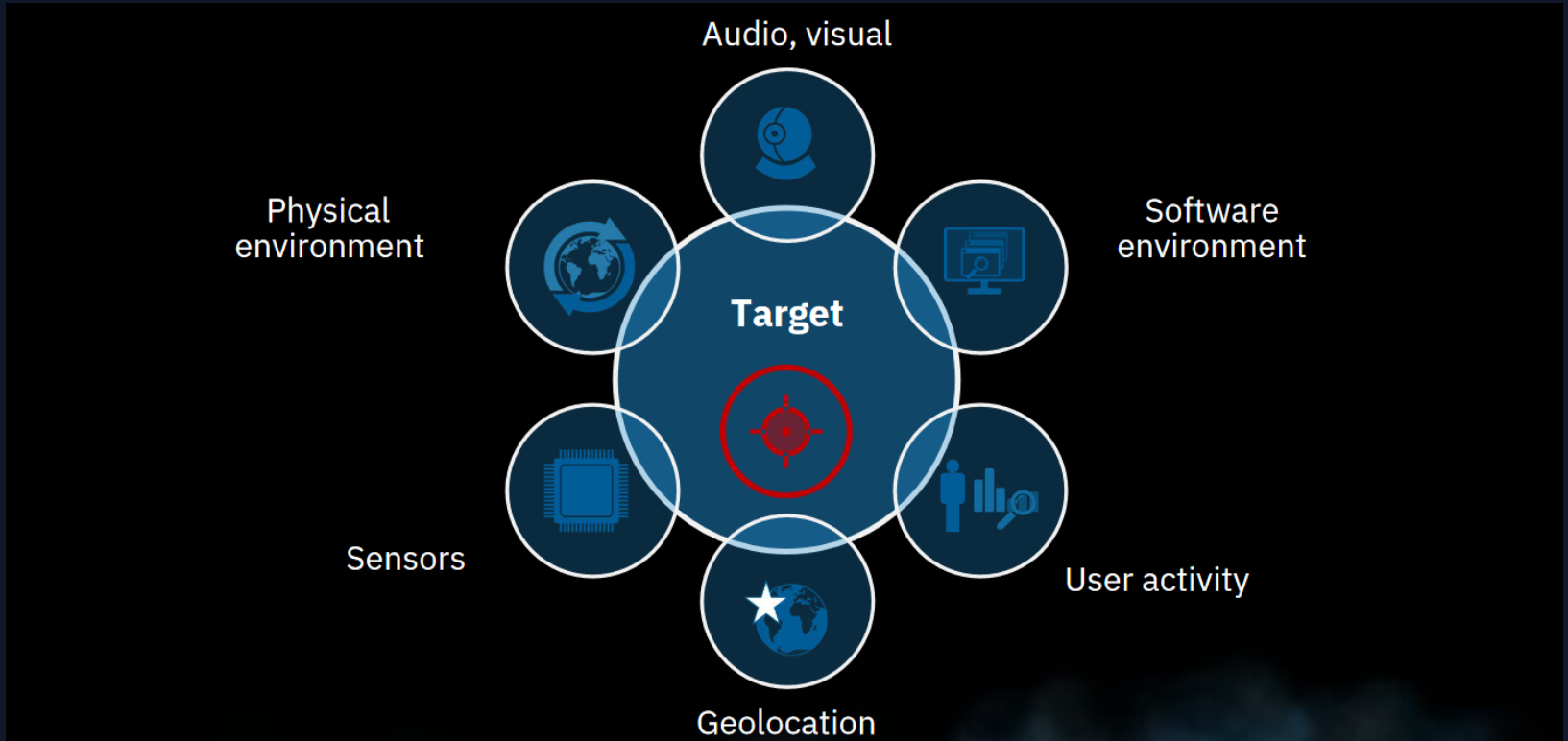


Traditional targeted attack

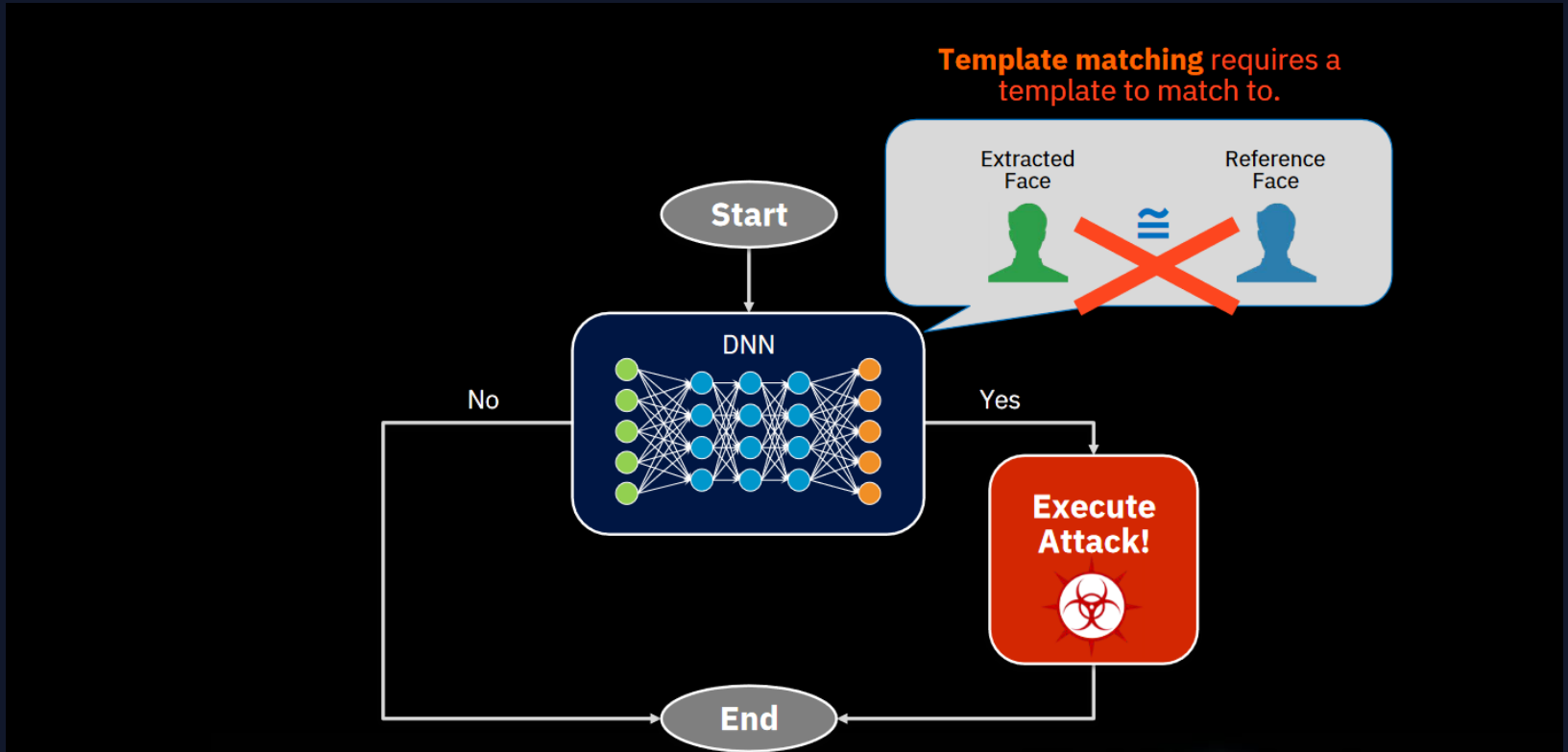




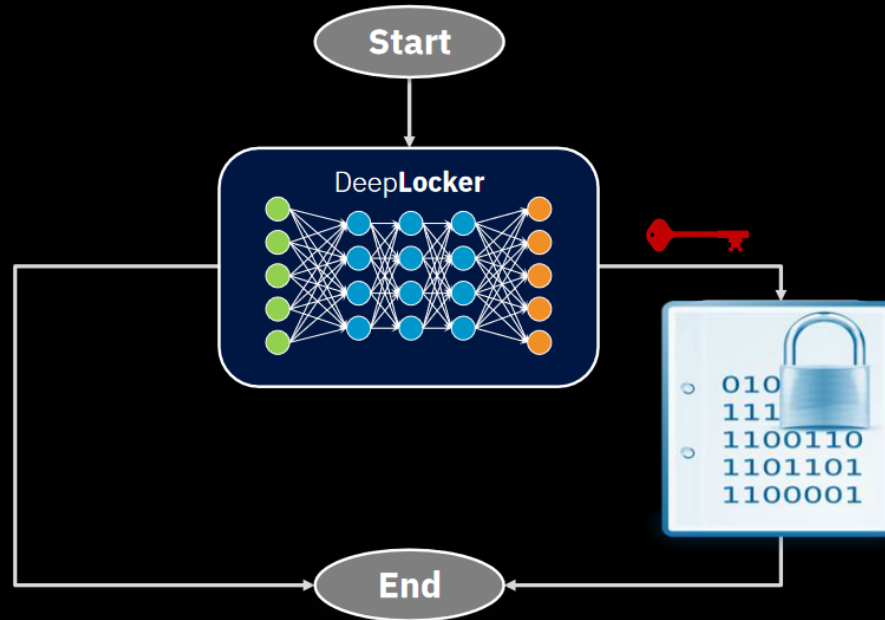
Target attributes



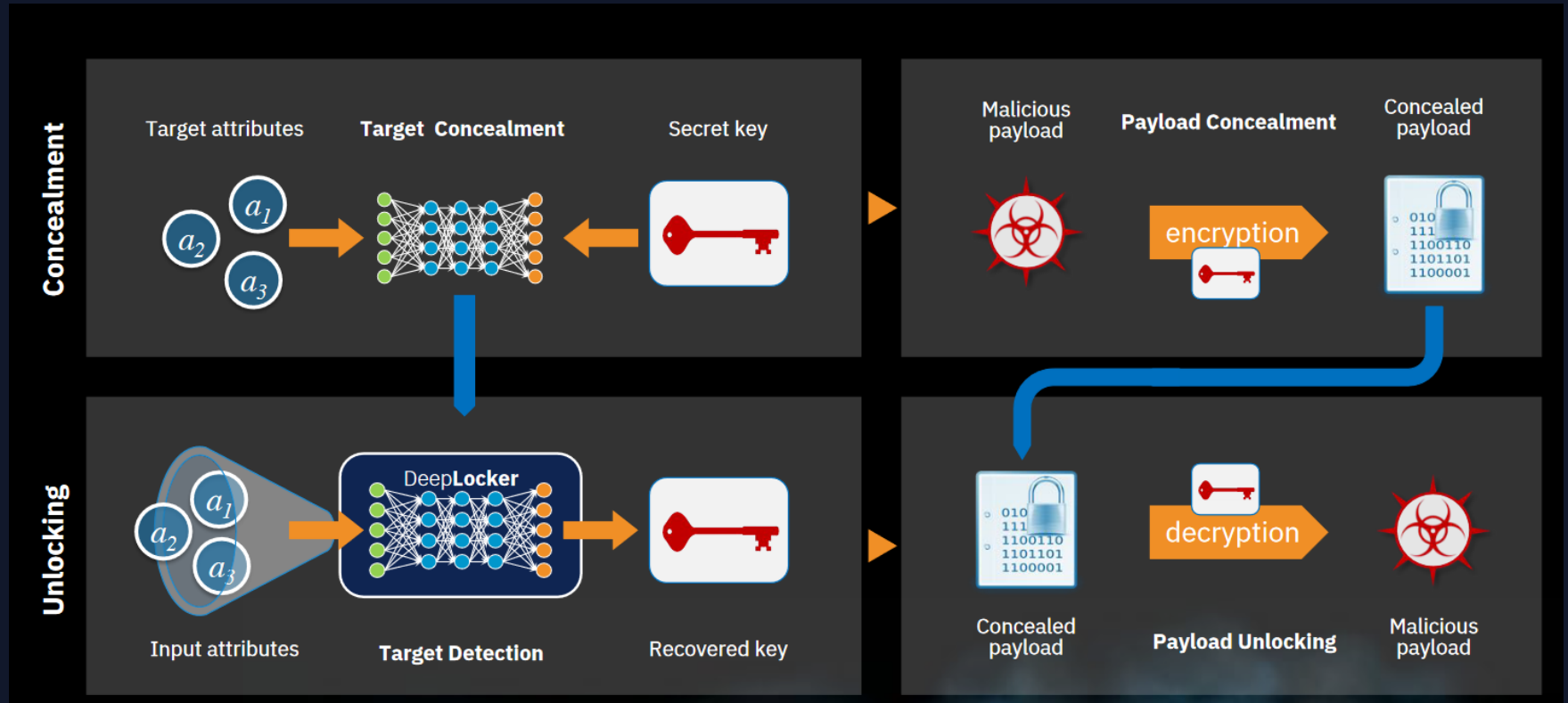
Target detection



Derivation of an unlocking key



DeepLocker – AI-powered Concealment and Unlocking

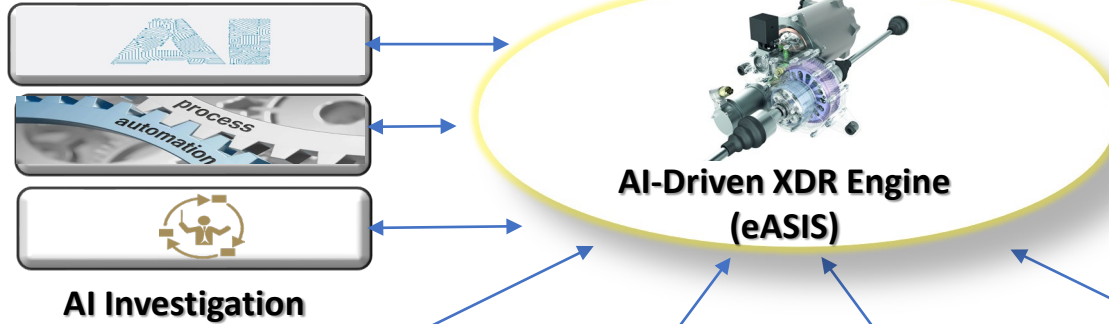


AI vs AI: NG SOC Services

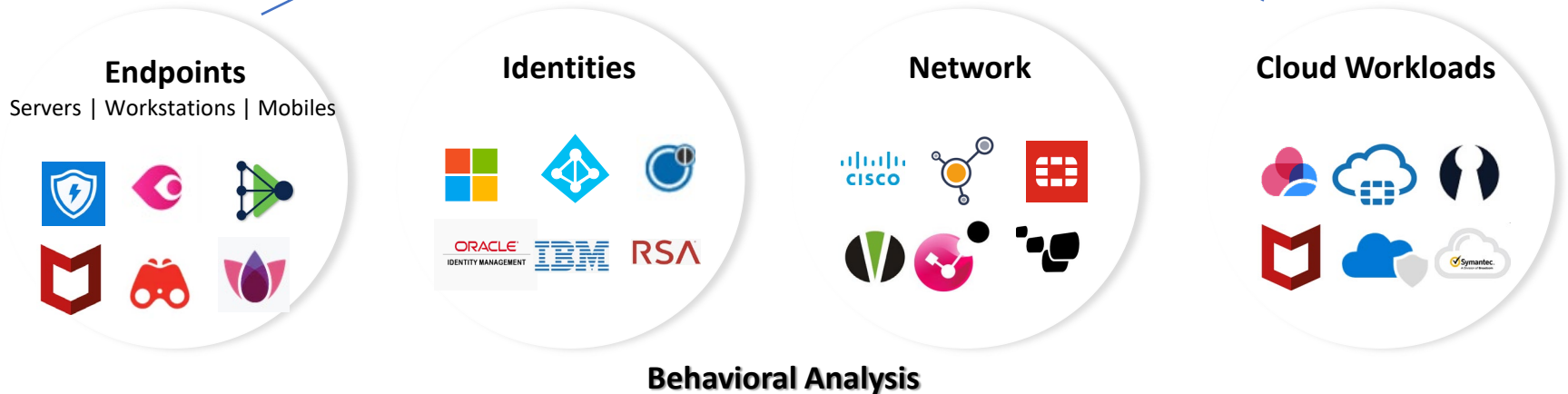


AI-Driven NG SOC Architecture

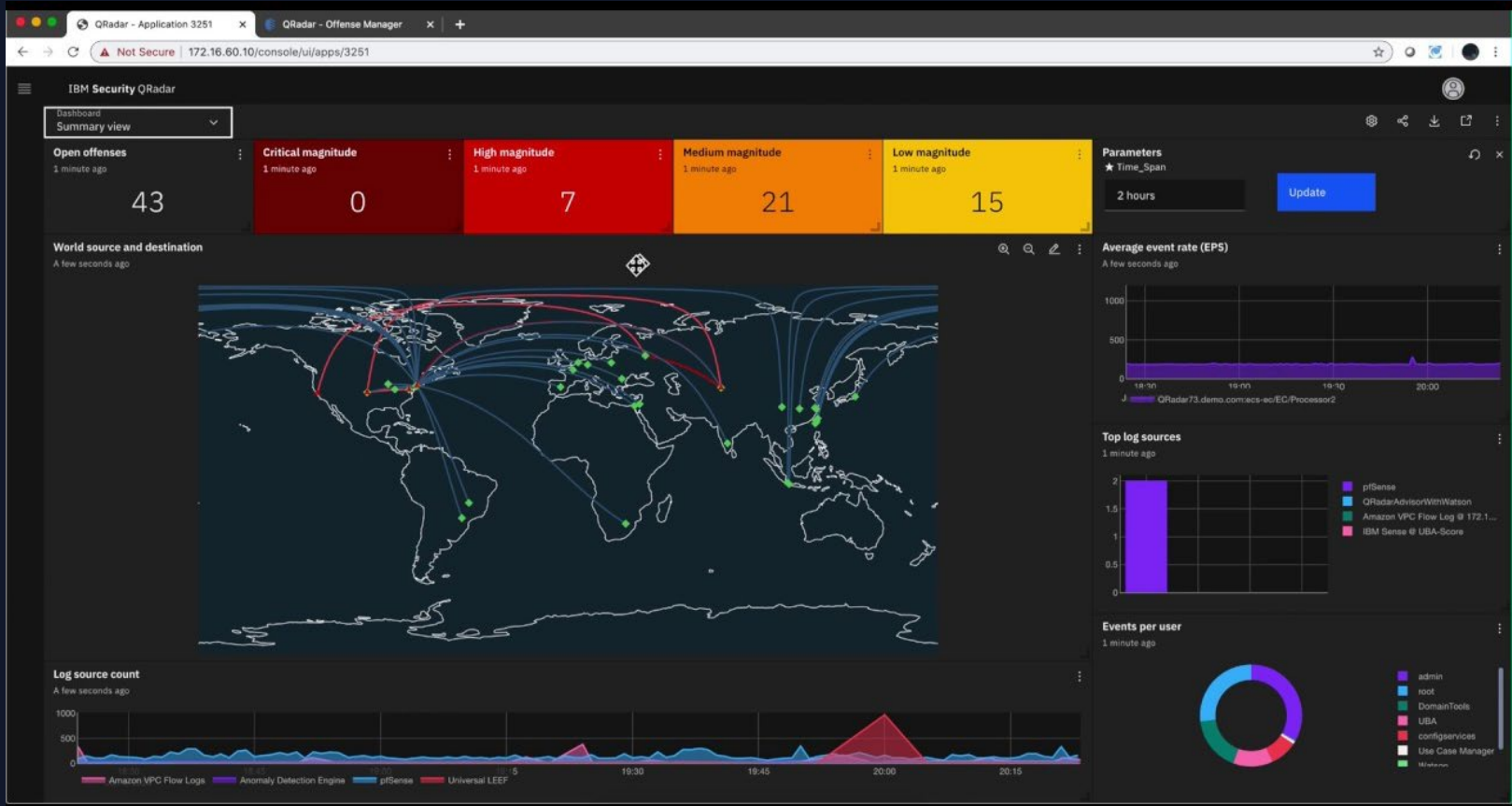
SOC Operations Layer



Detection Layer



Behavioral Analysis



Identities



IBM Security QRadar

Overview

All users

Search for users

Next refresh: 4:05

Reset

Monitored users

676

High risk users

2

0% of monitored users

Users discovered from events

174

26% of monitored users

Users imported from directory

502

74% of monitored users

Active analytics

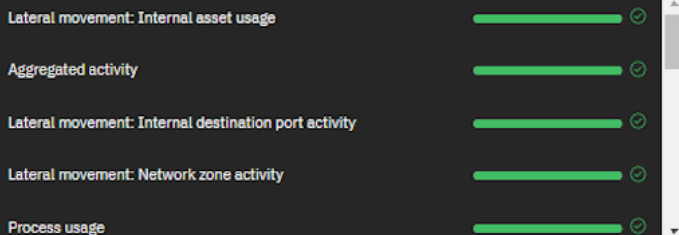
Rules: 86 of 192

Machine learning: 18

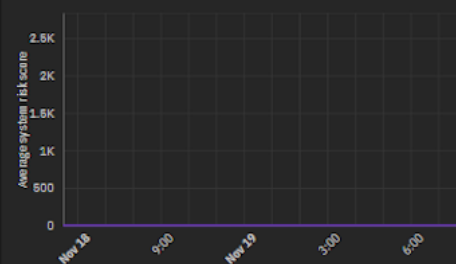
Monitored users

Username	Recent risk	Overall risk ↓
Pauline	160	499.2
Luciana	85	404.8
kitchen_sink_2	25	182.6
user2	25	167.2
kitchen_sink_1	30	166.4
kitchen_sink_3	85	153.1
kitchen_sink_4	55	126.5
e004790	15	126
qradar1	30	124.4
kitchen_sink_5	40	98.85

Status of machine learning models



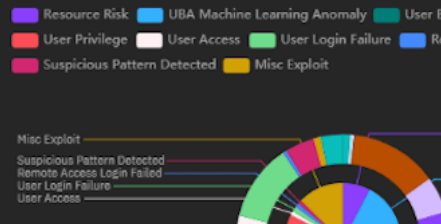
System score



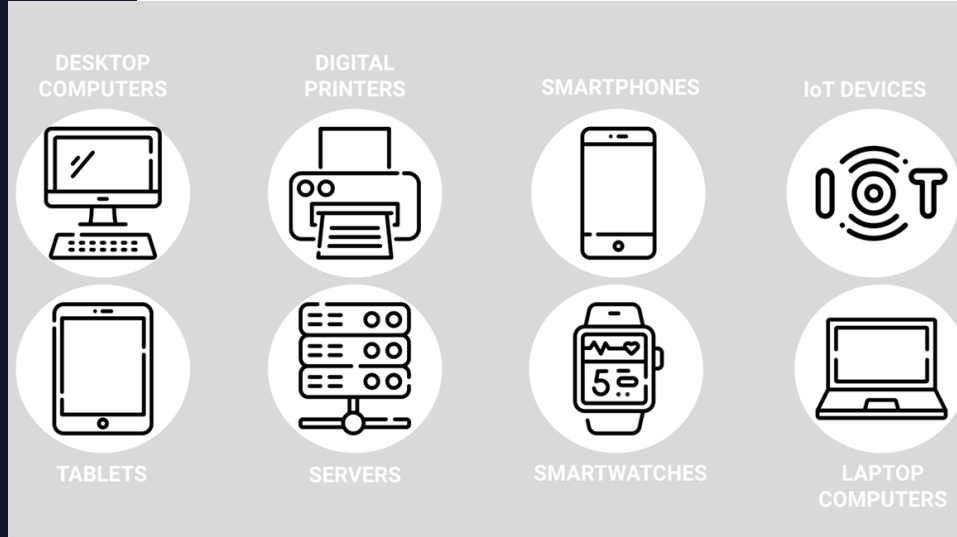
Recent offenses

- Offense #119** updated 2 hours ago
 User: sharedID-16
 Description: Multiple Login Failures for the Same User containing Login attempt - failed
 Event count: 12 Flow count: 0 Magnitude: 2/10
- Offense #114** updated 2 hours ago
 User: sharedID-16
 Description: Multiple Login Failures for the Same User containing Login attempt - failed

Risk category breakdown (Last hour)



Endpoints



Fortinet - Fortinet TMG x +
 https://fortiedr.console.fortidemo.com/#/event-viewer

DASHBOARD **EVENT VIEWER** FORENSICS COMMUNICATION CONTROL 101 SECURITY SETTINGS INVENTORY ADMINISTRATION 35 Protection admin

EVENTS

Showing 1-7/7 Search Event

Archive Mark As... Export Handle Event Delete Forensics Exception Manager

	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
<input checked="" type="checkbox"/>	pre-execution.exe (1 event)			Malicious		05-Aug-2020, 09:30:56	
<input checked="" type="checkbox"/>	23808	DESKTOP-C2OOS3B	pre-execution.exe	Malicious	File Read Attempt	05-Aug-2020, 09:30:56	05-Aug-2020, 09:30:56
	Certificate: Unsigned		Process path: C:\Users\singhs\Downloads\Files\malware\pre-execution.exe		Raw data items: 1		
<input type="checkbox"/>	dillhost.exe (3 events)			Malicious		31-Jul-2020, 23:16:57	
<input type="checkbox"/>	RemoteFXvGPUDisablement.exe (1 event)			Inconclusive		16-Jul-2020, 12:25:17	
<input type="checkbox"/>	WhatsAppService.exe (1 event)			Inconclusive		16-Jul-2020, 12:24:59	
<input type="checkbox"/>	setup.exe (1 event)			Inconclusive		15-Jul-2020, 11:02:47	
<input type="checkbox"/>	powershell.exe (1 event)			Malicious		25-Jun-2020, 12:19:30	
<input type="checkbox"/>	WINWORD.EXE (1 event)			Inconclusive		25-Jun-2020, 12:16:18	

CLASSIFICATION DETAILS

Malicious FORTNET

Threat name: Win32.Trojan.Aechu
 Threat family: Aechu
 Threat type: Trojan

History

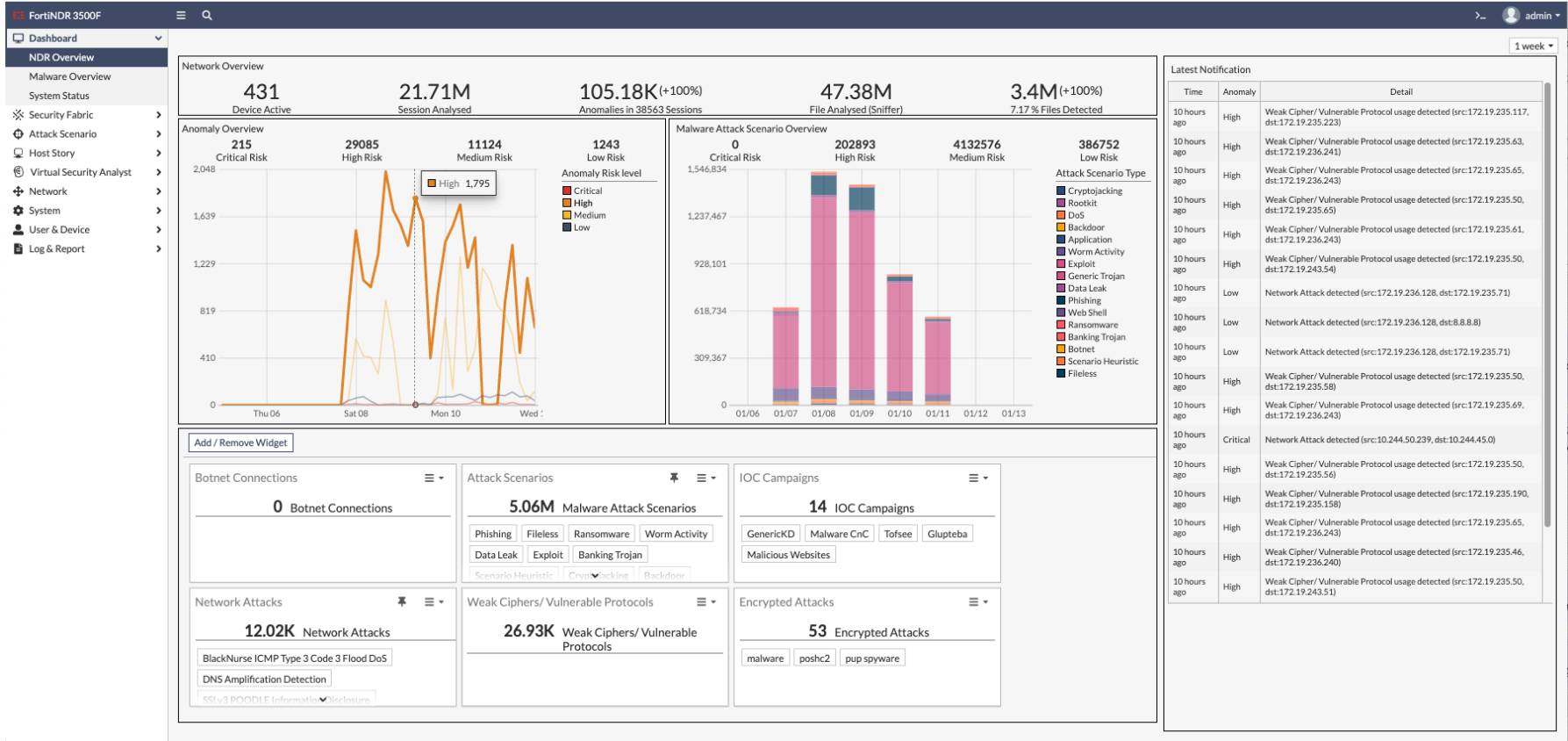
Malicious, by FortinetCloudServices, on 05-Aug-2020, 09:31:03

Triggered Rules

- Execution Prevention
 - Malicious File Detected

Network





Cloud





AI Investigation



IBM Security QRadar
👤

Watson Investigations / ID: Offense 2117

Key findings for

Source IP 10.103.22.32

Default | Investigated

Reinvestigate

Graph Relationships

Last investigation 5 days ago, on October 3, 2020, 5:51 AM

Key Observables

Critical	Threat Actors	Malware Families	High Value Assets	High Value Users
7	0	5	0	0

Compare with investigation from 5 days ago

> Filter Observables Table

Concern	Type	Description	Found Locally	Trend
Critical	📄	ad02452104dfd1eb2c91053e38332755	Yes	—
Critical	🔗	JS/TrojanDownloader.Nemucod	Yes	—
Critical	📄	ee18e36bf1cf32fac9ee006931a7a912	Yes	—
Critical	🔗	JS.Downloader	Yes	—
Critical	📄	0beb1124cbe82e4e1d3f743b5d711e5f	Yes	—
Critical	🔗	Trojan.Gen	Yes	—
Critical	📍	83.217.8.127	Yes	↘
High	📄	ad02452104dfd1eb2c91053e38332755	Yes	—
High	📄	ee18e36bf1cf32fac9ee006931a7a912	Yes	—
High	📄	0beb1124cbe82e4e1d3f743b5d711e5f	Yes	—
High	🌟	nemucod	No	—
High	🌟	locky	No	—
High	📄	8e876816e04489850f02e97b8cf8d922	No	↘

Provide your feedback to improve the accuracy of Watson evaluations. ✕

Evaluation ⓘ

Watson determined this offense is a **high priority**. Do you agree?

Yes, I agree
 No, I don't
 I'm not sure

Adding your evaluation will not close the offense.

MITRE ATT&CK Tactics & Techniques

Tactic/Technique Name <i>(Show Rules)</i>	Evidence	Confidence
Initial Access	📄	High
Execution	📄	High
Persistence	📄	High
Defense Evasion	📄	High
Credential Access	📄	High
Exfiltration	📄	Low
Automated Exfiltration	📄	Low

Offense Disposition Analysis

There are not enough recent similar offenses to provide a disposition analysis.

IBM Security QRadar

Watson Investigations / ID: Offense 2110 / Relationship Graph View Offense [Export](#)

Relationships

- Local - in offense (15)
- Watson Enriched (9)
- Local - outside offense (29)
- Local Blocked (0)
- Watson Enriched Blocked (0)

Scenarios

- Malware Executed (0)

Concern

- Critical (6)
- High (5)
- Medium (5)
- Low (24)

Observables

Important

- High Value Asset (0)

Other

- IP Address (6)
- Asset (4)
- Person (1)
- File (6)
- Hash (3)
- Filename (3)
- AV Signature (4)
- Domain (2)

The Relationship Graph displays a central yellow node representing the offense 'Offense 2110'. It is connected to various nodes representing different types of entities and their relationships. A network of green lines connects the central offense node to several other nodes, including IP addresses (e.g., IP 10.10.10.10, IP 10.10.10.11), files (e.g., file:///C:/Users/...), and other offenses (e.g., Offense 2104, Offense 2105, Offense 2106, Offense 2107, Offense 2108, Offense 2109, Offense 2111, Offense 2112). Red nodes with warning icons represent assets or domains, such as '10.10.10.10', '10.10.10.11', and '10.10.10.12'. Blue nodes represent domains like 'www.ibm.com' and 'www.ibm.com'. The graph also shows connections to various files and hashes, such as 'file:///C:/Users/...', 'file:///C:/Users/...', and 'file:///C:/Users/...'. The graph is a complex web of relationships, with the central offense node being the most prominent.

SECURITY
BUILT ON TRUST

THANK YOU

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

