

2025 New Mexico Housing Summit

Trends in Cyber Security

Tomas Rodriguez

Assistant Director of IT for Housing New Mexico

Greg Blake

Information Officer (CIO) Idaho Housing and Finance Association



Trends in Cyber Security

AI-Driven Threat Detection – Artificial Intelligence (AI) and Machine Learning (ML) have become powerful tools in cybersecurity as they can analyze vast amounts of data, identify patterns, and detect anomalies faster than humans.

AI-Powered Cyberattacks – AI allows attackers to quickly generate harmful code, malware, with very little knowledge of coding. AI can craft highly personalized and convincing phishing emails. It is also used to create fake news, and misinformation.

Rise in Insider Threats - Insider threats can be either malicious or unintentional. Employees or trusted individuals can compromise security by accident or with malicious intent. Employee training and awareness will play a crucial role in mitigating these risks. The key is to strike a balance between trust and vigilance.

Attacks Against Cloud Services – In 2023 Garner predicts the public spending on cloud services will grow by 20.4 percent due to migration to the cloud by business. This migration is a challenge for security professionals. This growth in cloud computing has also increased cloud-based threats.



Trends in Cyber Security

Housing New Mexico Cybersecurity Tools

Darktrace:

Uses self-learning AI to detect unusual behavior across networks and endpoints and can automatically neutralize threats in real-time.

SentinelOne:

Endpoint protection that provides AI-driven protection for endpoints environments.

Cylance Aurora:

Endpoint protection that provides AI-driven protection for endpoints environments.

Mimecast:

Protects businesses from email cyber threats like spam, phishing, malware by incorporating AI-powered threat intelligence to scan every message for malicious content, links, and attachments.



Trends in Cyber Security

How they help protect from cyberattacks

Anomaly Detection

AI analyzes massive datasets to establish a baseline of normal network, user, and endpoint activity, then flags deviations that indicate a potential threat.

Autonomous Response

AI can automatically trigger actions to contain and stop threats, such as isolating infected devices or blocking malicious network traffic, without waiting for human intervention.

Threat Hunting

AI enables proactive threat hunting by automating the search for hidden threats across the enterprise, shifting from a reactive to a more proactive defense posture.

Fraud Detection

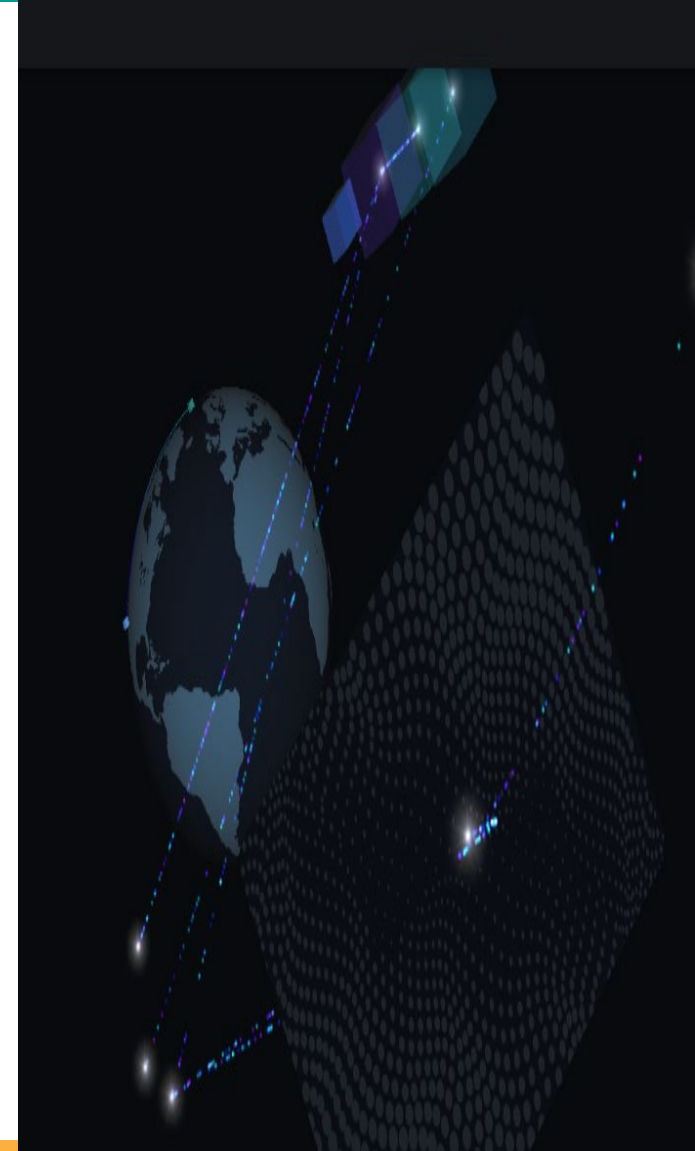
By analyzing user behavior, AI can detect suspicious activities, such as unauthorized access attempts or fraudulent transactions, helping to prevent breaches and financial losses.

Vulnerability Monitoring

AI tools continuously monitor for vulnerabilities in networks, cloud environments, and applications, providing early warnings for potential weak points.

Automated Incident Response

AI streamlines incident response by automating the initial investigation, prioritizing alerts, and providing actionable insights to security teams, freeing up human analysts for more complex tasks.



Trends in Cyber Security

How they help protect from cyberattacks (Cont.)

Isolating a compromised device.

AI can identify a compromised device and restrict the device (quarantine) from the network.

Blocking malicious traffic.

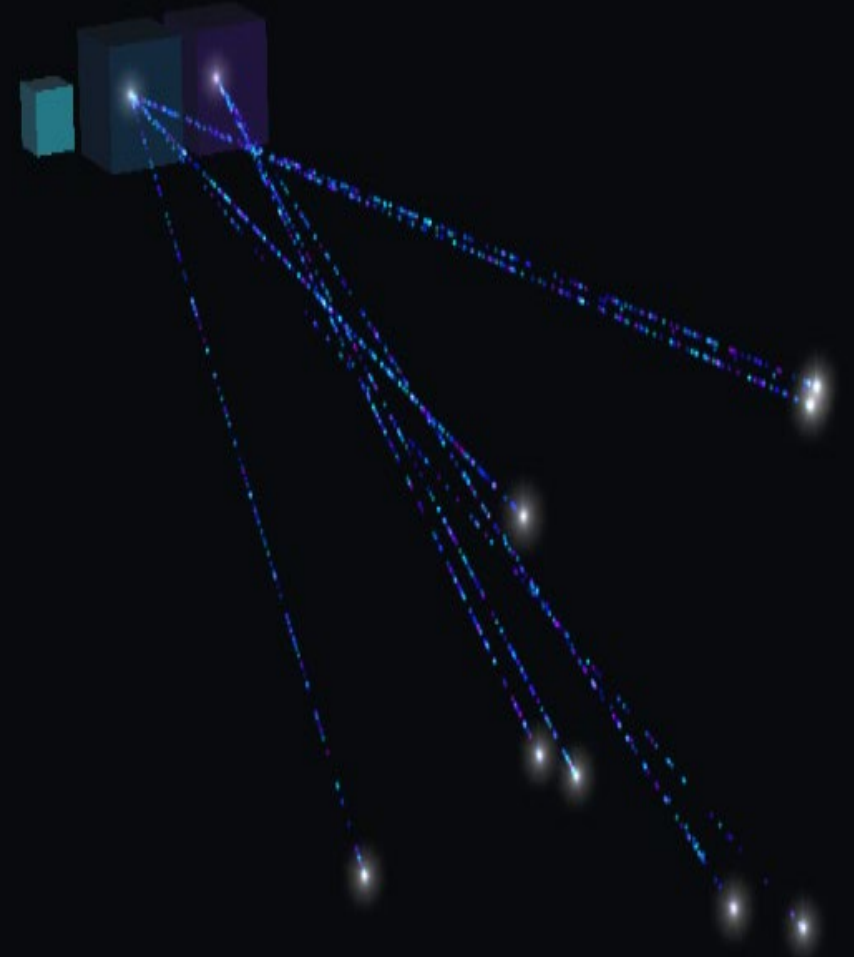
AI can monitor traffic and identify anomalies within that traffic such as network scans and stop those anomalies.

Identifying suspicious activities from within the organization.

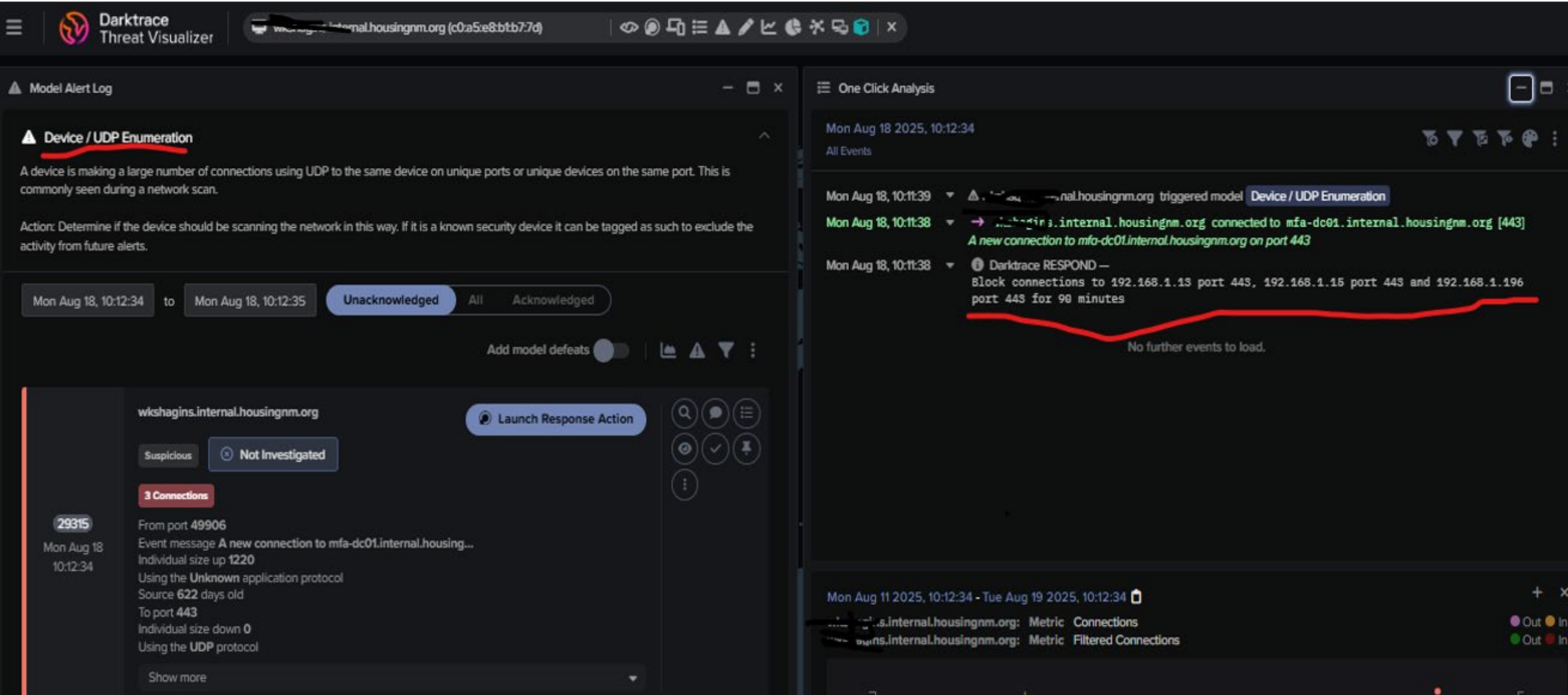
AI can identify suspicious activities such as uploading or downloading large amounts of data (DLP).

Analyzing email patterns and identifying suspicious behavior.

AI can identify suspicious activities as granular as a user creating a new email rule or allowing account access to another user.



Trends in Cyber Security



The screenshot displays the Darktrace Threat Visualizer interface. The top navigation bar includes the Darktrace logo and the title 'Darktrace Threat Visualizer'. Below this, a breadcrumb trail shows the path: 'Model Alert Log' > 'Device / UDP Enumeration'. The main content area is divided into two panels. The left panel, titled 'Model Alert Log', shows a list of alerts. The first alert is 'Device / UDP Enumeration', which is highlighted with a red box. Below the alert list, there are filters for 'Mon Aug 18, 10:12:34' to 'Mon Aug 18, 10:12:35', and buttons for 'Unacknowledged', 'All', and 'Acknowledged'. The right panel, titled 'One Click Analysis', shows a detailed view of the selected alert. It includes a timeline of events: 'Mon Aug 18, 10:11:39' - 'Device / UDP Enumeration' triggered; 'Mon Aug 18, 10:11:38' - 'A new connection to mfa-dc01.internal.housingnm.org on port 443'; and 'Mon Aug 18, 10:11:38' - 'Darktrace RESPOND - Block connections to 192.168.1.13 port 443, 192.168.1.15 port 443 and 192.168.1.196 port 443 for 90 minutes'. A red line is drawn across the bottom of the 'One Click Analysis' panel, indicating 'No further events to load.' The bottom of the interface shows a summary of the alert, including the source IP '29315', the destination IP 'wkshagins.internal.housingnm.org', and the port '443'. It also includes a 'Launch Response Action' button and a 'Show more' link.

Darktrace Threat Visualizer

Model Alert Log

Device / UDP Enumeration

A device is making a large number of connections using UDP to the same device on unique ports or unique devices on the same port. This is commonly seen during a network scan.

Action: Determine if the device should be scanning the network in this way. If it is a known security device it can be tagged as such to exclude the activity from future alerts.

Mon Aug 18, 10:12:34 to Mon Aug 18, 10:12:35

Unacknowledged All Acknowledged

Add model defeats

One Click Analysis

Mon Aug 18, 10:12:34

All Events

Mon Aug 18, 10:11:39 - Device / UDP Enumeration triggered model

Mon Aug 18, 10:11:38 - wkshagins.internal.housingnm.org connected to mfa-dc01.internal.housingnm.org [443]
A new connection to mfa-dc01.internal.housingnm.org on port 443

Mon Aug 18, 10:11:38 - Darktrace RESPOND -
Block connections to 192.168.1.13 port 443, 192.168.1.15 port 443 and 192.168.1.196 port 443 for 90 minutes

No further events to load.

Summary

29315

Mon Aug 18 10:12:34

From port 49906

Event message A new connection to mfa-dc01.internal.housing...

Individual size up 1220

Using the Unknown application protocol

Source 622 days old

To port 443

Individual size down 0

Using the UDP protocol

Show more

Launch Response Action

Mon Aug 11 2025, 10:12:34 - Tue Aug 19 2025, 10:12:34

Internal.housingnm.org: Metric Connections

Internal.housingnm.org: Metric Filtered Connections

Trends in Cyber Security

Darktrace Threat Visualizer

Search for a device, subnet, IP or host...

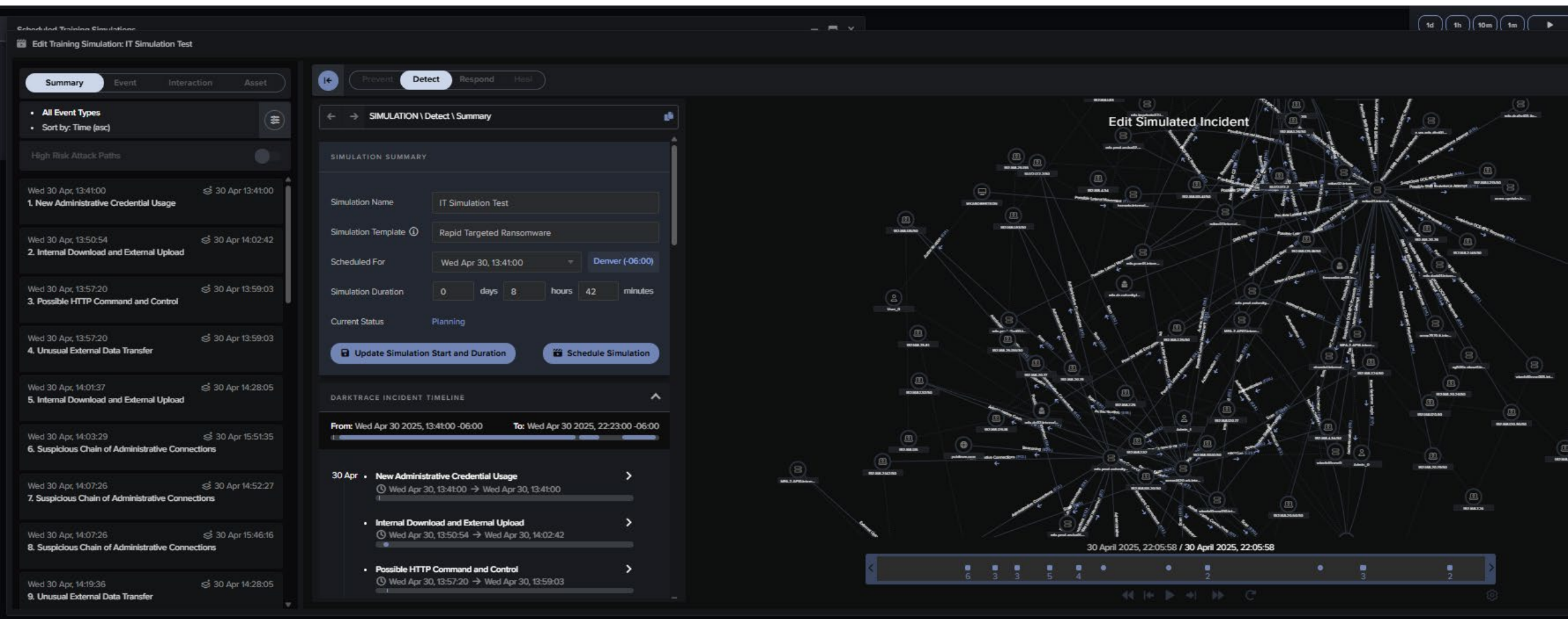
Response Actions

Network Actions Platform Actions Settings

Device	IP	Action	History	Start / Expiration	Type	Source	Actions	Current Status
WKS Vigil-LLP	192.168.2.114	Block connections to 192.168.2.35 port 161, 192.168.2.38 port 161 and 192.168.2.41 port 161	View History	<div>▶ Sat Aug 30 2025, 05:50:35 -06:00</div> <div>❑ Sat Aug 30 2025, 07:20:35 -06:00</div>	Network	Device / UDP Enumeration	Reactivate	No Message
WKS Vigil-LLP	192.168.2.114	Block connections to port 445	View History	<div>▶ Sat Aug 30 2025, 05:52:43 -06:00</div> <div>❑ Sat Aug 30 2025, 06:52:43 -06:00</div>	Network	Device / Suspicious SMB Scanning Activity_Tomas	Reactivate	No Message
WKS Vigil-LLP	192.168.2.114	Enforce pattern of life	View History	<div>▶ Sat Aug 30 2025, 05:52:43 -06:00</div> <div>❑ Sat Aug 30 2025, 06:52:43 -06:00</div>	Network	Device / Suspicious SMB Scanning Activity	Reactivate	No Message
WKS Vigil-LLP	192.168.2.114	Block connections to port 161	View History	<div>▶ Sat Aug 30 2025, 05:50:38 -06:00</div> <div>❑ Sat Aug 30 2025, 06:50:38 -06:00</div>	Network	Device / UDP Enumeration Original	Reactivate	No Message
WKS Vigil-LLP	192.168.2.114	Block connections to 192.168.2.35 port 161, 192.168.2.38 port 161 and 192.168.2.41 port 161	View History	<div>▶ Sat Aug 30 2025, 05:50:36 -06:00</div> <div>❑ Sat Aug 30 2025, 06:50:36 -06:00</div>	Network	Antigena / Network / Significant Anomaly / Antigena Significant Anomaly from Client Block	Reactivate	No Message

Trends in Cyber Security

Darktrace Attack Simulation

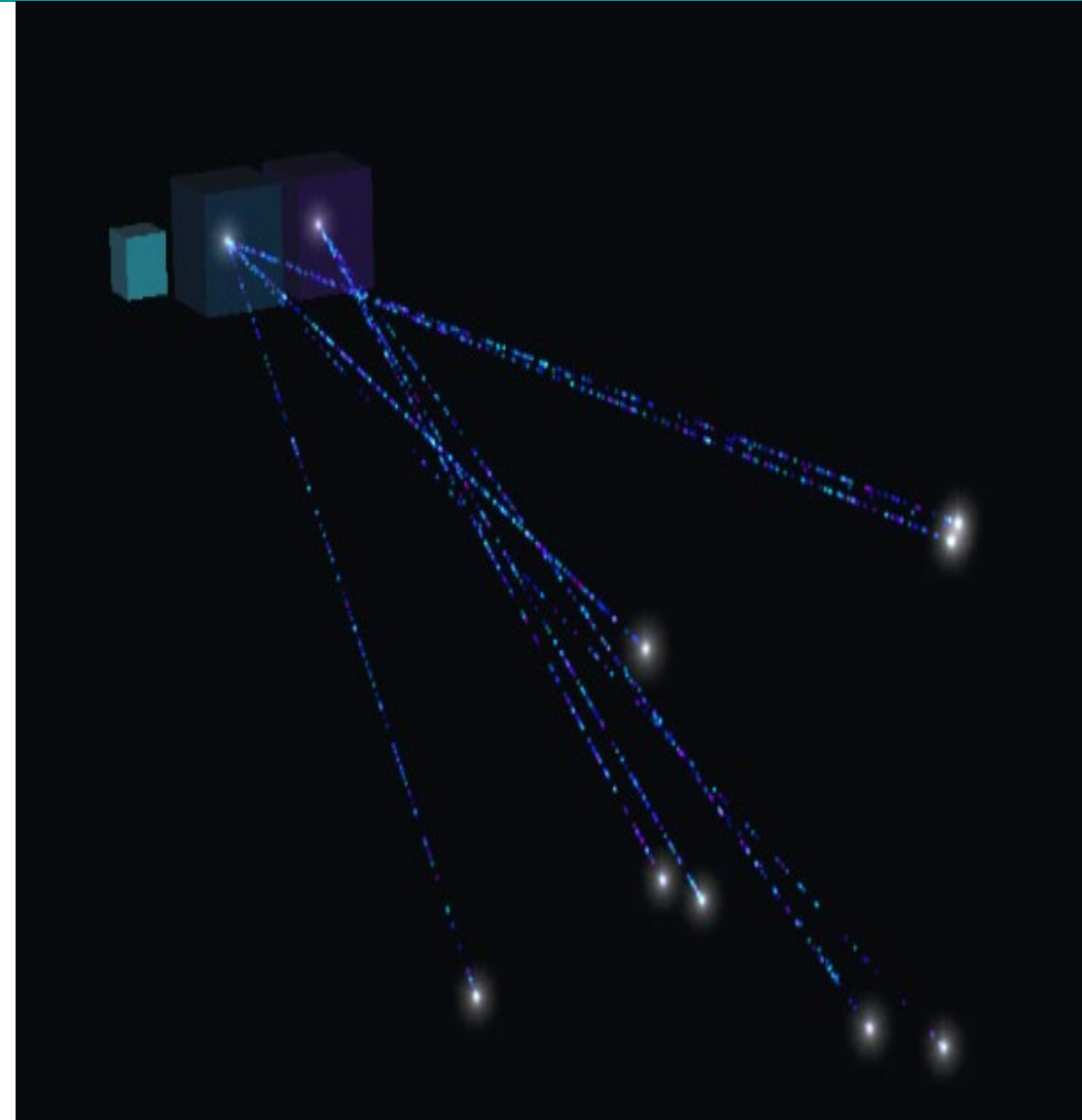


Trends in Cyber Security

Strengths of AI

- AI is great for **anomaly detection** because it can process and analyze massive amounts of data, like network traffic and user behavior, much faster than a human.
- An AI system first establishes a baseline for what "normal" activity looks like by analyzing the data in a learning mode.
- Any significant deviation from this baseline is flagged as a potential threat. This allows AI to detect even previously unknown, or zero-day, attacks.

This is a huge improvement over traditional signature-based detection, which can only identify threats based on a database of known threat patterns.



Trends in Cyber Security

Mitigate Actions Storyline Event Search

Mitigation Status Severity Classification Identified time

Benign Critical Ransomware Aug 6, 2025 10:5

Alert Status Assigned To

Resolved Tomas Rodriguez

Overview Indicators 11 Mitigation 2 Notes 0 History

Mitigation Actions

Killed 923/923

File and Process Properties

File Name Unknown file

File Path \\Unknown device\\Unknown file

Signature Verification Not Signed

Process User NMMFA

Originating Process WindowsTerminal.exe

Command Line Arguments C:\\WINDOWS\\System32\\cmd.exe

Multiple Infostealers detected

New Mexico Mortgage Finance Authority/Default site/Default Group

Mitigate Actions Storyline Event Search

Mitigation Status Severity Classification Identified time

Benign Critical Ransomware Aug 6, 2025 10:59:19 AM Aug

Alert Status Assigned To Analyst Verdict

Resolved Tomas Rodriguez False positive/

Overview Indicators 11 Mitigation 2 Notes 0 History 10 Graph

Mitigations (2)

KILL 923/923 SUCCESS

923 out of 923 actions completed successfully in under ms.

Download CSV Report

QUARANTINE 1433/1433 SUCCESS

1433 out of 1433 actions completed successfully in under ms.

Download CSV Report

Export 62%

PROCESS SUMMARY

Name: claude.exe

UID: FD61616643E57B05

ID: 56184

Command Line: --type=renderer --user-data-dir="C:\\Users\\dbaca.NMMFA\\AppData\\Roaming\\Claude" --secure-schemes=sentry-ipc --by-pass-csp-schemes=sentry-ipc --cors-schemes=sentry-ipc --fetch-schemes=sentry-ipc --app-user-model-id=com.squirrel.AnthropicClaude.claude --app-path="C:\\Users\\dbaca.NMMFA\\AppData\\Local\\AnthropicClaude\\app-0.12.5\\resources\\app.asar" --enable-sandbox --video-capture-use-gpu-memory-buffer --lang-en-US --device-scale-factor=1 --num-raster-threads=4 --enable-main-frame-before-activation --renderer-client-id=15 --time-ticks-at-unixepoch=-1753509683439748 --launch-time-ticks=992743911030 --field-trial-handle=1740,i,6013670110579839040,18424138087955261822,262144 --enable-features=PdfUseShoSaveFilePicker --disable-features=SpareRenderForSitePerProcess,WinDelaySpellcheckServiceInit --variations-seed-version --moio-ol

claude.exe Single Node

cmd.exe (npm.cmd) Events: 3

cmd.exe (npm.cmd) Events: 3

docker.exe One Child

node.exe One Child

Load more (5/40)

Trends in Cyber Security



Trends in Cyber Security

Logs

search for an email, person, domain or attachment

Actions Live

Emails

Mailbox Inspector

EMAILS

30

Housing NM BABA Presentation & Forms

Overview

AI Analyst

Content

Technical

Admin

ANOMALY INDICATORS

The user [REDACTED] has been detected emailing an unusually high volume of external recipients. The email includes an **unusual** attachment **BABA Presentation - 2025.pptx** which could indicate an attacker has control of the user's account and is targeting the recipients with a malicious attachment. In the past hour, **5** unique recipients have been contacted by the user.

HISTORY

8 USERS

30 DAYS

The recipient, [REDACTED]@dominiuminc.com, has sent and received email today. They first received an email 524 days ago.

ASSOCIATION

6 USERS

TODAY

The recipient and 20 others at the domain are known to the organization.

This recipient [REDACTED]@dominiuminc.com is well known to the organization and there is a high degree of bilateral communication patterns.

RECIPIENT > ADDRESS > METRICS > KCD

INTERNAL CORRESPONDENTS

[REDACTED]@housingnm.org

2025-08-06 18:50:55 UTC

[REDACTED]@housingnm.org

2025-08-06 18:48:12 UTC

[REDACTED]@housingnm.org

2025-08-06 17:25:45 UTC

[REDACTED]@housingnm.org

2025-08-04 16:49:28 UTC

[REDACTED]@housingnm.org

2025-07-30 15:22:07 UTC

[REDACTED]@housingnm.org

2025-07-30 13:29:12 UTC

[REDACTED]@housingnm.org

2025-07-25 17:03:36 UTC

Subject	Unlock Elite-Only Deals on Top Hunting Gear
From Display	support_at_marketing_onxmaps_com_2pv678x8k6_4136a1da@privaterelay.appleid.com
From Envelope	privaterelay.bounce.2pv678x8k6@privaterelay.appleid.com
To	ihernandez@housingnm.org
Date/Time	08 Aug 2025 - 08:25:28

Trends in Cyber Security

AI is also revolutionizing email security.

- AI can analyze linguistic patterns, sender reputation, and contextual clues, thus it can identify sophisticated **phishing attempts**.
- AI can analyze large amounts of data and find subtle patterns used in identifying anomalies in email characterizes that humans might miss.

This is particularly effective against AI-generated scams, which often bypass traditional filters because of their polished grammar and personalized content.



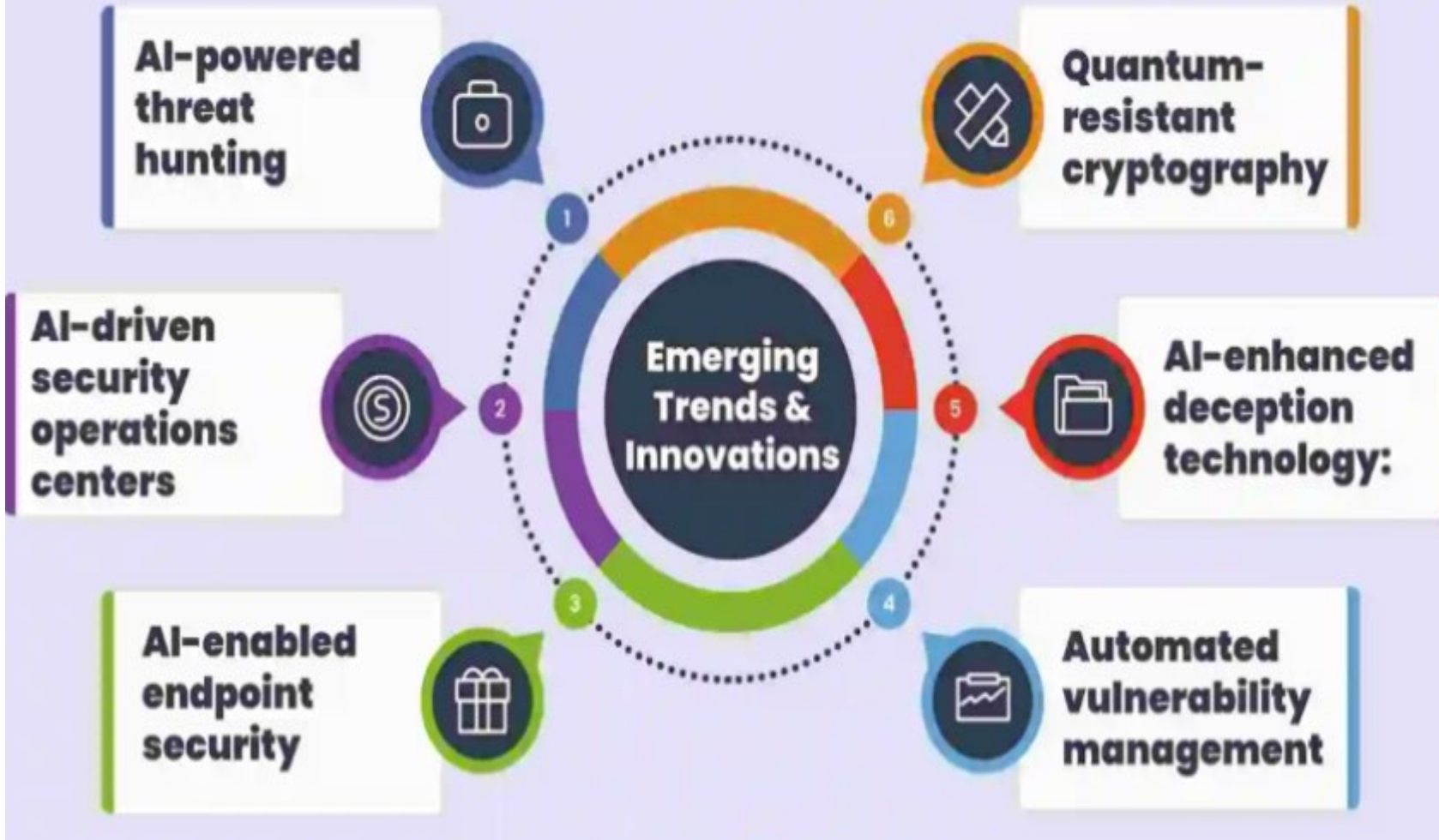
Trends in Cyber Security

AI Driven Cyber Attacks

- AI Generated Malware
 - AI is also transforming malware by creating programs that can adapt and “mutate” their own code.
 - Code mutation allows malware to get passed traditional software detection that rely on specific patterns or signature threats.
- Automated Reconnaissance
 - AI can scan networks at lightning speed to pinpoint vulnerabilities such as outdated passwords.
 - AI can search the internet and create a profile of individuals from company websites and social media sites.
 - The reconnaissance of an AI will allow attackers to craft a sophisticated social engineering attacks.
- AI attacking AI
 - AI agents can corrupt data used to train AI by injecting false information thus sabotaging the models.
 - Tampering – AI agents can embed vulnerabilities in open-source AI models setting traps once the models are deployed allowing for attackers to exploit with out detection.

Trends in Cyber Security

The Future of AI in Cybersecurity



ANY QUESTIONS