





Reaction to Readiness

Practical Resilience Strategies with Trellix (*and friends*)



BUILDING RESILIENCE

1

APT Defensive Urgency

"Defending against scary things"

2

Protect what matters

"OT systems power our lives, what do you to ensure they stay up?"

3

AI Risk and Reward

"Make your workplace and apps safe for AI adoption"

4

Next Generation Sec Ops

"Faster and more visibility will improve your readiness"

5

Your Role

"True resilience is Human-Driven"

APT Scary Trends

Living off the Land

CMD: 54%

Powershell: 49%

MITRE Techniques

Tool Transfer: 73%

Web Protocols: 77%

Malicious Files: 70%

AI MALWARE EXPLOSION

**720% increase in
general malware with
540K APT related
detections across
1200 campaigns**

Malware Sneaky Laks

1.3 Million email borne threats slipping through email security vendors each quarter

30- 50% of files analysed in cloud storage services were malicious.

Slack, Salesforce top the list for other types of applications with significant malicious detections for files and/or URLs.

UP YOUR SANDBOX GAME

Develop a multi-layer defense against malicious file transfer detection using Trellix IVX



Be Intelligence Lead by
leveraging Operational Intelligence delivered via
Trellix Insights

Supply Chain exploits on
network devices and legacy applications drive
need for NDR and application protection
schemes

Leverage AI in Defense
Trellix ML and AI based defense detected 46
Million threats

Operational Technology

The image features a central 3D illustration of a bundle of dynamite, secured with straps. A digital timer is attached to the top of the bundle, displaying '00:00'. A single wire extends from the timer. To the right of the dynamite bundle is a large, dark grey gear. The background is a dark blue-grey color, overlaid with faint, light blue line art of industrial process diagrams. These diagrams include various components such as tanks, pumps, valves, and control loops, with labels like 'PUMP', 'FIC-101', 'LIT-101', 'TI-301', and 'TID1'.

Are you ready?



The Importance of what WE do

A disaster may be around the corner



37%

Industrials are the highest target for Ransomware

< 50%

Conduct IT-OT security exercises

88% APT

Target Telco, Transport and Technology

Resilience for Critical Systems

**Hardened
Endpoints
and Media**



**Trellix Endpoint
and Application
Control
validated by
OEMs**

**Network
Visibility &
Monitoring**



**Trellix NDR
now covers IT
and OT**

**Risk-Based
Vuln
Management**



**Trellix + Armis
integrate to
provide IT-OT
visibility**

**IT-OT
Sec Ops**



**Trellix Helix
Connect**

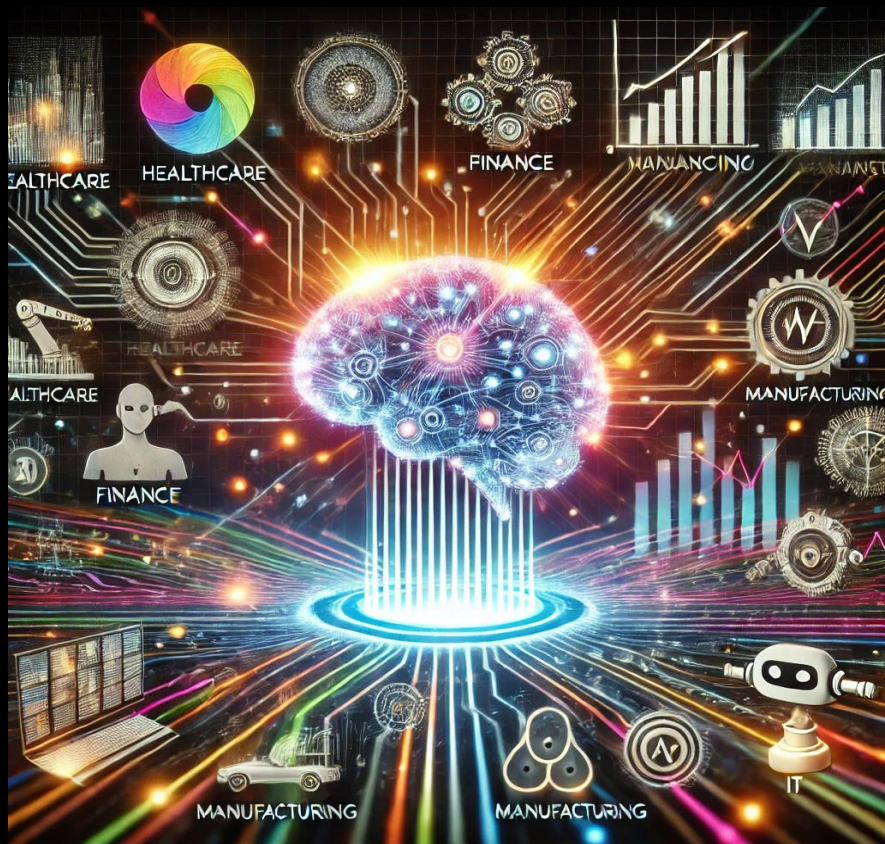
**ICS
Incident
Response**



**Trellix 360
Assurance**



**Artificial Intel,
Oh My
Are you Ready?**



Expect More 0 Days

AI Systems can generate a working exploit to a published CVE in 10-15 minutes

Trellix Global Threat Intelligence

Compliance Breach

78% of all AI Applications do not meet data security and compliance requirements

Skyhigh Threat Intelligence

Data Leaks

11% of data uploaded to Shadow AI applications have contained Sensitive Data

Skyhigh Threat Intelligence

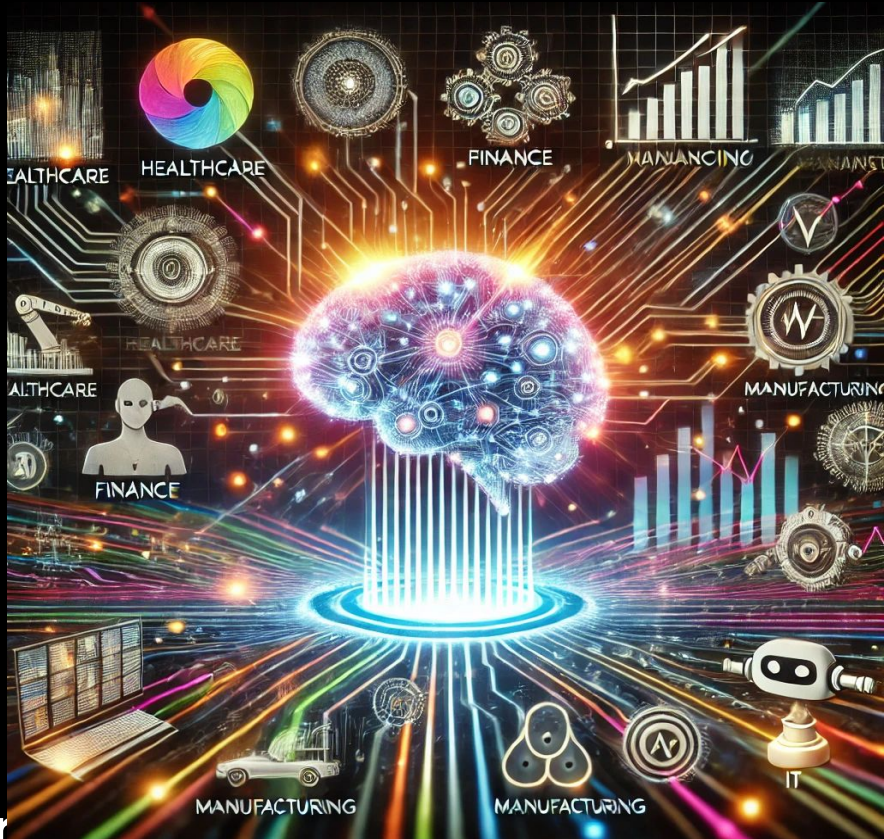
Change Behavior for True Readiness

Human Risk Management

AI-Driven Phishing
is the # 1 delivery
vehicle



Make your Workspace AI-Ready



Govern Shadow AI

Visibility and risk analysis for public GenAI user services and Models with Skyhigh

Control Sensitive Data

Trellix DLP to restrict data flow to unauthorized applications.

Observability

Monitor infrastructure, usage, detections with AI-powered XDR in Helix Connect

Make your Applications AI-Ready

Infrastructure Protection

Protect the network, workloads and storage with Trellix NDR

Data Lifecycle Protection

Control data in and out of AI Applications with Trellix DLP

Observability

Monitor infrastructure, usage, detections with Helix Connect

Trellix

400+ data formats supported by Trellix Data Loss Prevention



Generative AI is used to identify potentially sensitive data and create policies to keep it safe.

- Social Security numbers
- Employment information
- Account numbers
- Dates of birth

DATABASE PROXY

AI

Amazon Bedrock
Generative AI applications



**How to make
Sec Ops better,
faster,
stronger?**

Time Really Matters in Sec Ops



Ransomware Recovery Lessons Learned From Arnold Clark

Disruptive Data-Stealing Attackers Hit Vehicle Retail Giant Right Before Christmas

Mathew J. Schwartz (@euroinfosec) · February 25, 2025

✉ 📄 📁 ⭐ Credit Eligible

Get Permission



Image: Shutterstock

50 Million GBP Loss, 12-18 hours MTTR



2.4 Billion \$ Loss, 8-9 Days MTTD

Sec Ops Acceleration with GenAI

Analytics and Triage



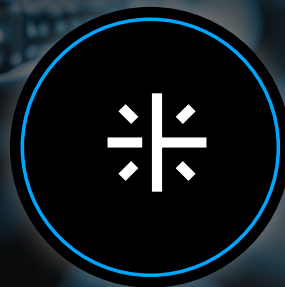
Scope, prioritize, triage, correlate, and investigate alerts and events

Threat Intel



Use natural language to hunt for patterns and anomalies; generate reports

Detection Engineering



Leverage GenAI tools to safely create parsers, rules, test code

What Defines Sec Ops Readiness?



Three Minutes



Better Sensor Grid by incorporating Email as a key sensor combined with Cloud App logs and NDR across IT-OT

Threat Hunting is no longer an option. Trellix Second Sight proactively augmenting your SOC team provides an extra layer of protection

Simulations practice your own resilience



The Importance of what *YOU* do

The background of the image is a gradient of blue and green, with a subtle ripple effect that gives it a sense of movement and depth. The word "Trellix" is centered in a bold, white, sans-serif font. The 'T' is particularly prominent, with a thick vertical stroke and a horizontal top bar. The 'r' has a distinctive shape with a small loop. The 'e' is simple and rounded. The 'l' is a straight vertical line. The 'i' has a small dot. The 'x' is composed of two intersecting diagonal lines. The overall composition is clean and modern.

Trellix