NOZOMI NETWORKS | splunk> a cisco company | aws

WEBINAR

Securing Industrial and Physical AI in Manufacturing

AI in Manufacturing: A Journey

Capability and value climb across the journey. Once autonomy reaches the physical world, **the attack surface climbs with it** — securing that inflection is the new imperative.

1

Simulation, Classification & Optimization

- Digital Twins
- AR / VR
- Quality Control

2

Predictive Analytics

- Predictive Maintenance
- Predictive Quality
- Energy Management

3

Gen AI

- Industrial Copilots
- Chat Bots
- AI Assistants

4

Agentic AI

- Response to Cyberattacks
- Automated Optimizations
- Agentic AI-driven Operations

5

Physical AI

- AI-driven Robotics for Production
- Warehouse Robots
- Self-Driving Cars

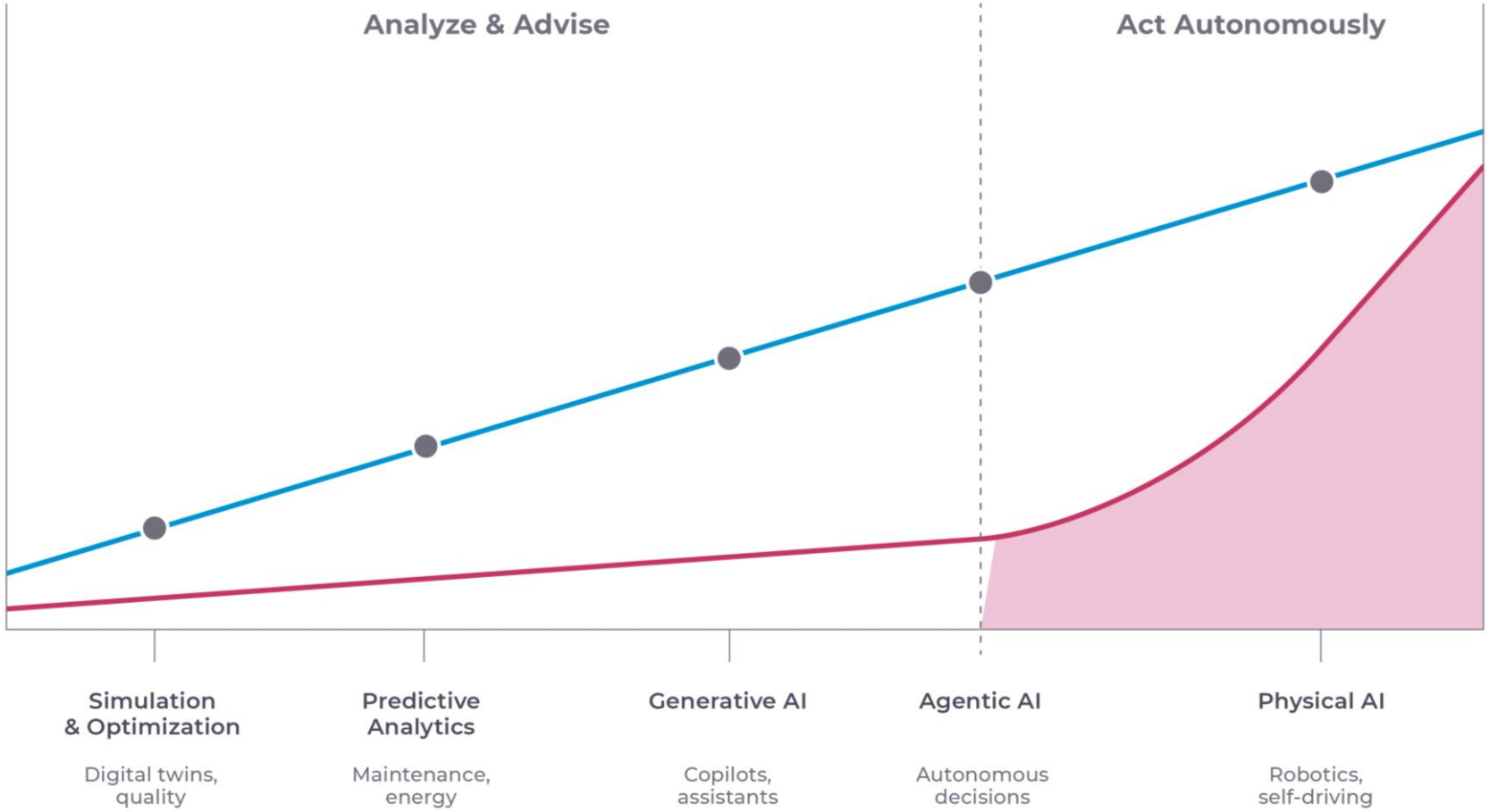
On the horizon — AI + Quantum: complex logistics & supply-chain optimization, data-center workload scheduling, new-materials discovery and large-scale simulation.

From Analyzing to Acting

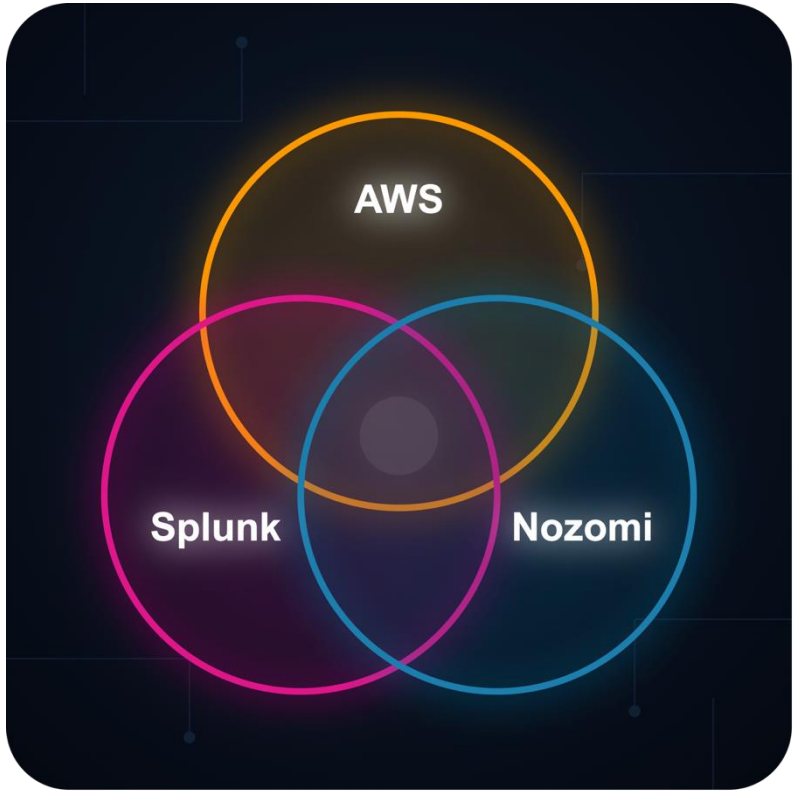
The security imperative behind manufacturing's AI journey

When AI stops advising and starts acting on machines, the cost of being wrong becomes physical.

Capability and value climb across the journey. Once autonomy reaches the physical world, the attack surface climbs with it. Securing that inflection is the new imperative.



The Partnership Opportunity



Splunk — Enterprise SIEM Layer

Enterprise Security platform with dedicated OT Security Add-on — correlating IT and OT data at scale.

Nozomi — OT Cybersecurity Core

Deep asset visibility, anomaly detection, and OT-native threat intelligence across industrial environments.

AWS — Scalable Cloud Foundation

Secure, compliant infrastructure enabling Nozomi Vantage (SaaS) and enterprise-wide data aggregation.

Cybersecurity is the #1 Barrier to Industrial AI Adoption

40%

cite cybersecurity as the **single largest obstacle** to AI adoption across manufacturing, utilities and transportation.

#3 concern → **#1 blocker** | in under two years

20%	have **fully collaborative** IT/OT interworking on cybersecurity
48%	flag security as their **top networking challenge** overall
85%	believe AI is their **best tool to improve** security posture

Source: Cisco 2026 State of Industrial AI Report · base: 1,000+ industrial decision-makers across 19 countries

OT/IoT Visibility

INDUSTRIAL ENVIRONMENT

OT
PLCs · SCADA · robots · sensors

IoT
connected & edge devices

BMS
building management systems

PROTOCOLS & AI OVERLAYS

Modbus | PROFINET | DNP3 | EtherNet/IP | MQTT | AI runtimes

NOZOMI DISCOVERY

- Non-intrusive passive monitoring
- Active discovery & smart polling
- Continuous, 24/7

No operational disruption

REAL-TIME ASSET INVENTORY

Every asset, continuously, with full context:

- **Behavior & baselines**
- **Vulnerabilities**
- **Relationships & comms**

Continuously updated — **no manual audits, no blind spots.**

Baseline normal — detect anomalies early

Identify vulnerabilities across legacy + Physical AI assets

Feed clean OT telemetry to the SOC

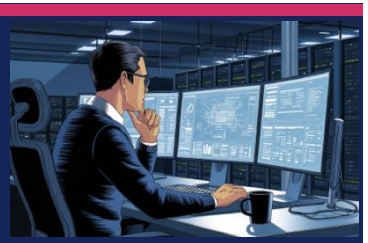
Extend visibility into BMS

Achieving OT/IoT Visibility & NIS2 Governance

Splunk + Nozomi Networks + AWS Triad - Your Competitive Weapon for NIS2 compliance

SPLUNK

Unified IT/OT Resilience Hub



NIS2 Article 23 — Incident Handling

- 24h / 72h automated incident reporting
- Risk-Based Alerting — 90% noise reduction
- Agentic SOC with AI-driven response
- Unified IT/OT correlation engine

Nozomi Networks

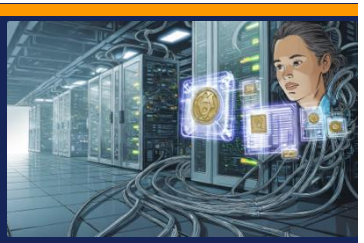
OT Security Foundation

NIS2 Article 21 — Risk Management

- 100% XIoT asset visibility
- Exposure & vulnerability management
- Virtual patching for legacy OT systems
- Purdue Levels 0–3.5 coverage

AWS

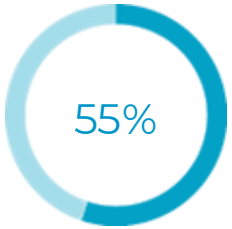
Secure Modernization Platform



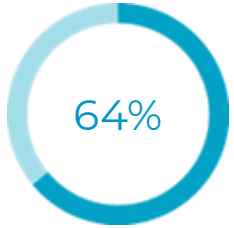
NIS2 Article 20 — Governance

- 143 security certifications
- MATM framework for OT migration
- Amazon Security Lake (OCSF)
- Marketplace bundling & procurement

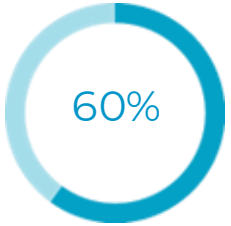
MEASURED OUTCOMES



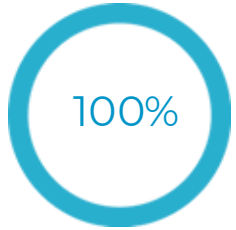
Faster Incident Detection



Greater SOC Efficiency



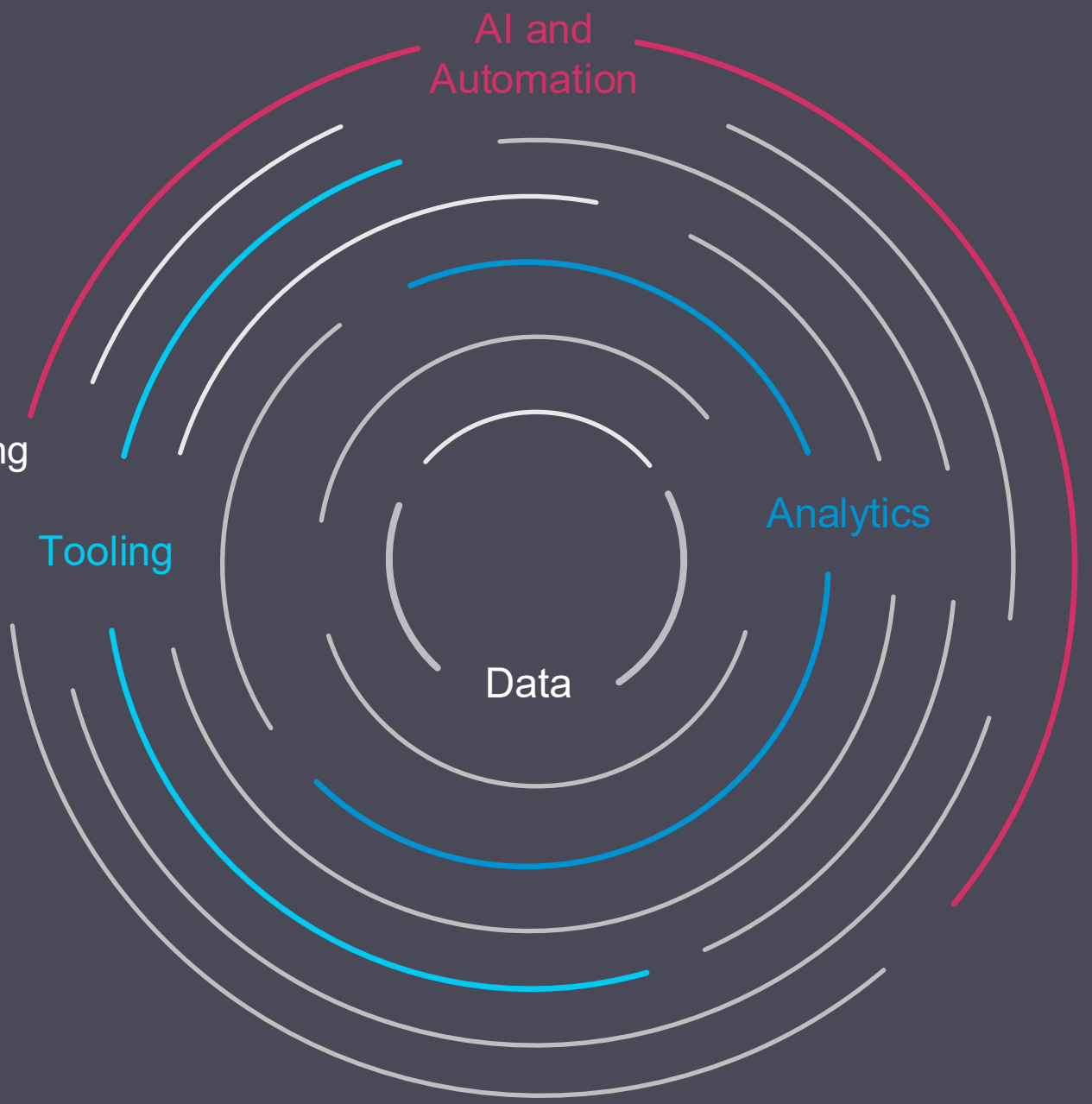
Reduction in MTTR



XIoT Visibility Levels 0–3.5

Agentic SOC

- Complete visibility
- Contextual understanding
- Intuitive analyst experience
- Machine speed & scale



A Foundation of High-Fidelity Data

Data fabric
Data management
Data pipelines

Analyzed at Machine Speed

TI enrichment & context
Correlated detections
Investigation & hunting

With Intuitive SOC Tooling

Single work surface for TDIR
Team coordination
Integrated workflows

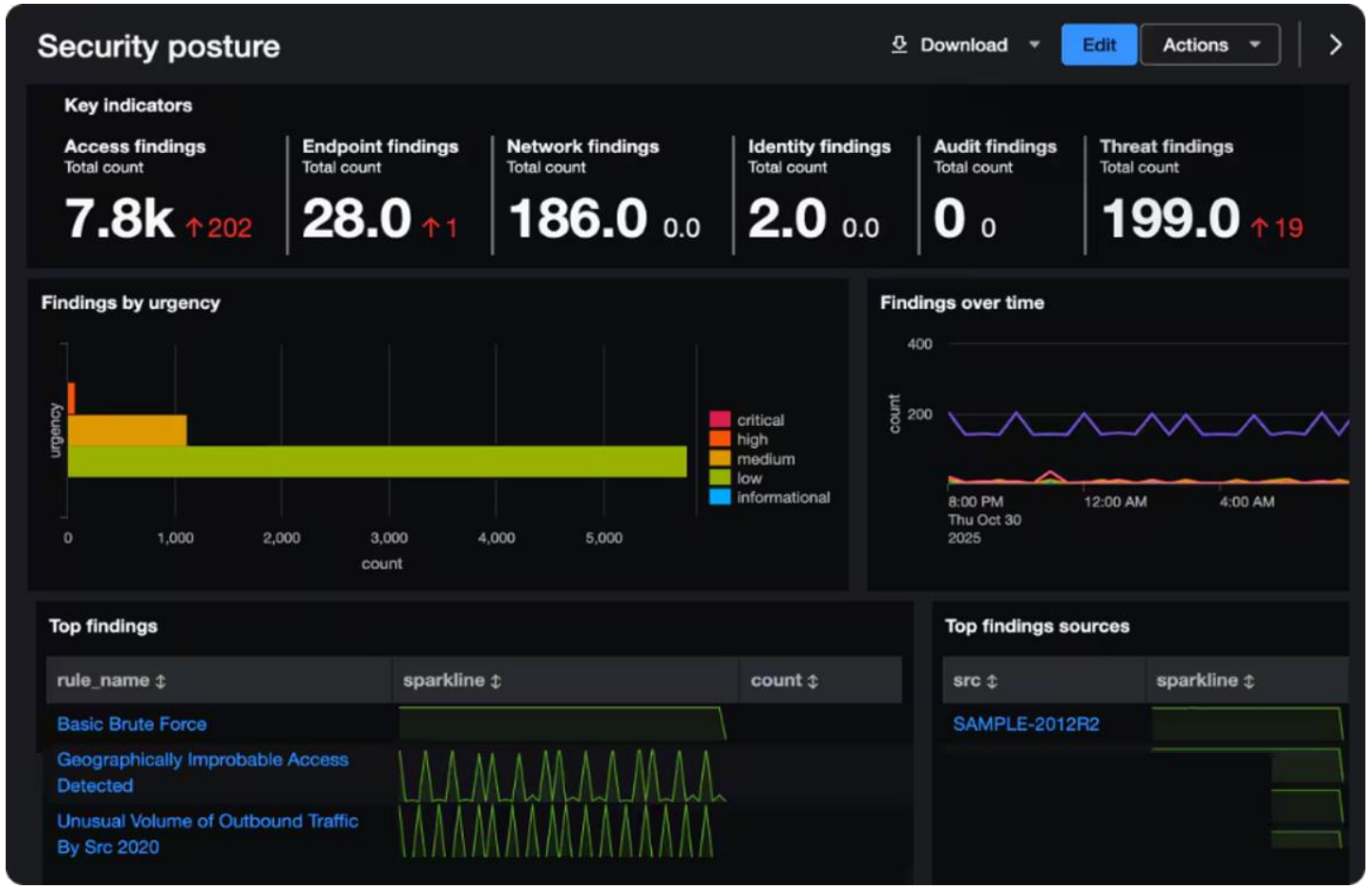
And Human-led AI & Automation

Customizable agents
Reasons and acts decisively
Prevents emerging threats

NOZOMI NETWORKS | splunk> a cisco company | aws

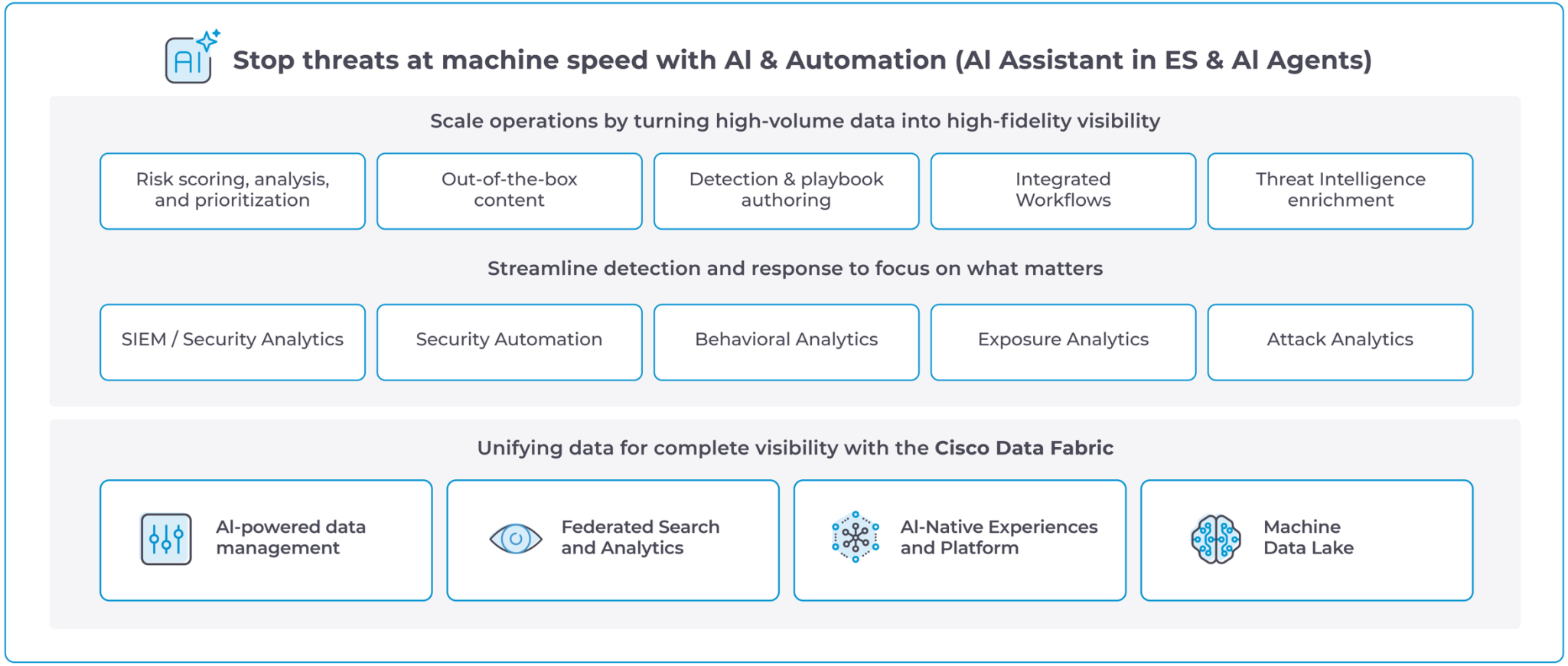
Splunk Agentic IT/OT SOC

The Unifying Intelligence Layer

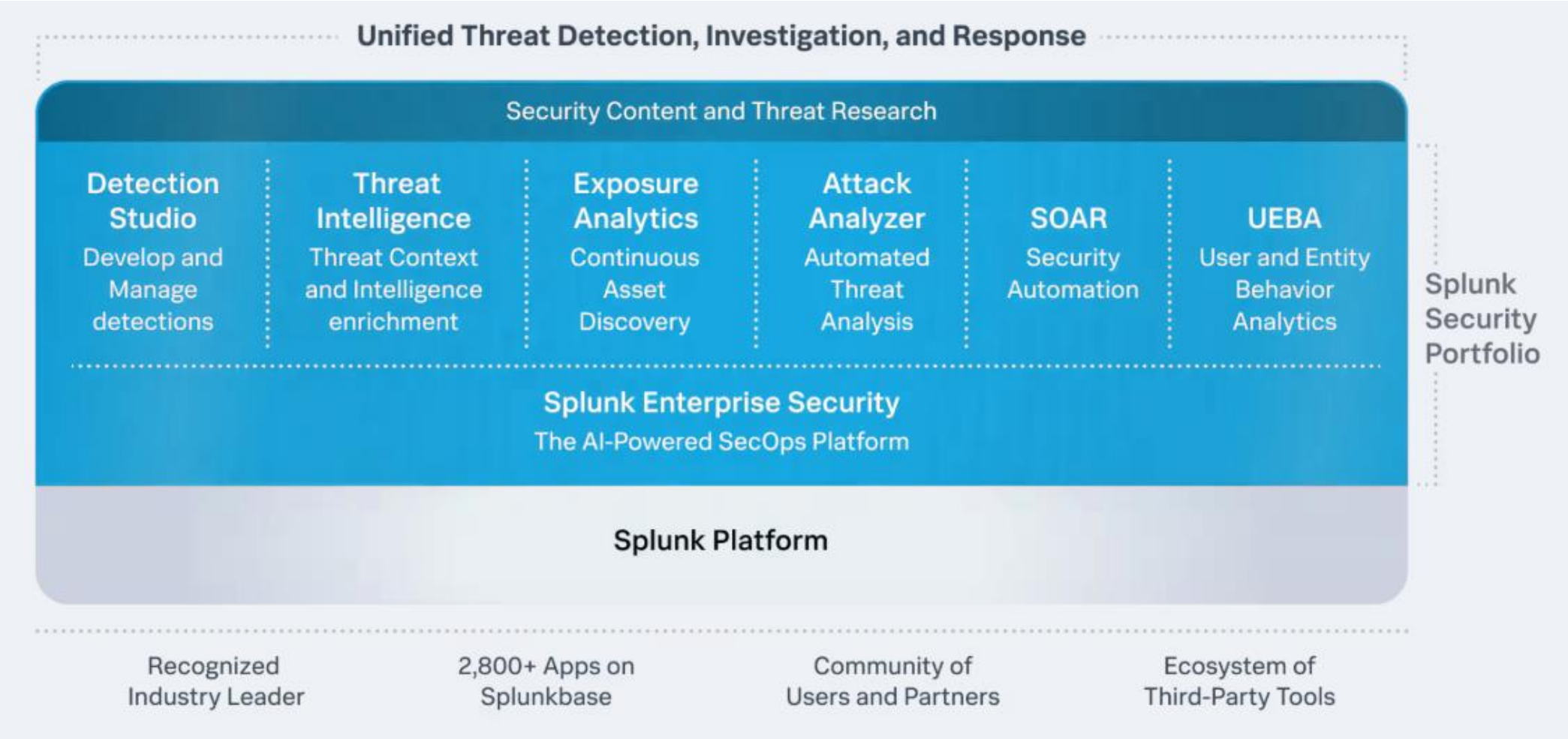


Splunk: Powering the Agentic SOC for Unified Resilience

Unify security data, analytics, tools, and AI to automate routine tasks, surface complex insights, and proactively mitigate risk

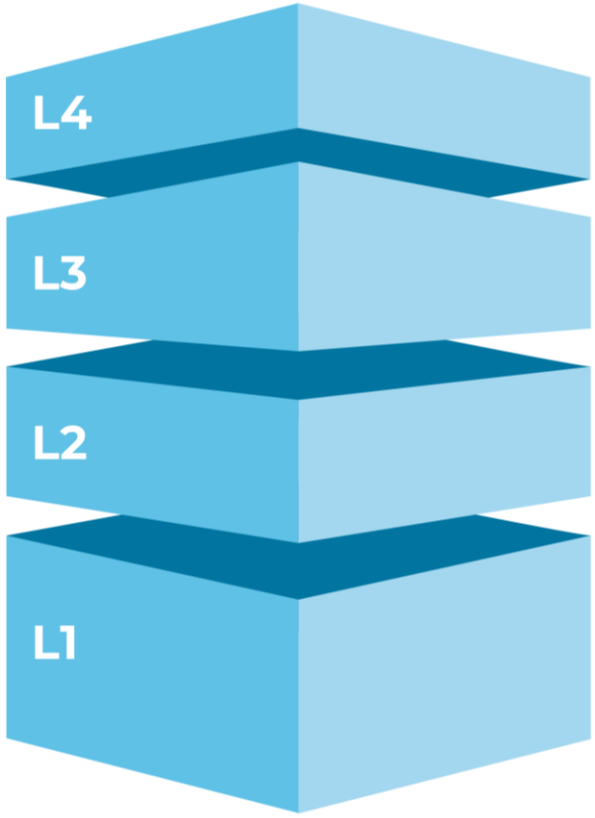


Leveraging the Power of Splunk



Cloud Infrastructure for Secure, Scalable Manufacturing

AWS Manufacturing Applications & Technology Modernization (MATM) framework structures industrial cloud security into four prerequisite layers — each enabling the next.



L4 - End Customer Enablement
OT/IIOT visibility · AI threat detection · NIS2 & IEC 62443 · Unified IT/OT SOC

L3 - AWS Enables Partner Solutions
Nozomi · Security Lake (OCSF) · Splunk ES · SOAR-driven response

L2 - AWS Enables Itself
Security Reference Architecture · Landing Zone · Multi-Account · Automated Baselines

L1 - AWS Cloud Platform Foundation
IAM · GuardDuty · Security Hub · CloudTrail · Network Firewall · VPC · KMS · Control Tower

Securing Converged IT/OT Environments

From Assessment to Enterprise Scale

VOLKSWAGEN GROUP CASE STUDY

IT/OT CONVERGENCE PROOF POINT · PRESS RELEASE

120+ factory sites

Digital Production Platform on AWS

100+ ML use cases deployed

Predictive maintenance & quality

SYNAOS robot fleet orchestration

Largest heterogeneous fleet in automotive

30%	30%	€1B
Efficiency Gain	Cost Reduction	Supply Chain Savings

This is the MATM approach at enterprise scale

ROADMAP

ASSESSMENT TO ENTERPRISE SCALE

1 Foundation

SHIP Assessment · Device identity · Passive monitoring · Data onboarding · Agent Registry for highest-risk fleet

2 Protection

Active threat detection · TLS inspection · Cedar policies · Risk-Based Alerting · Mathematical proof of isolation

3 Governance & Scale

Compliance automation · Multi-facility · Fleet orchestration security · Continuous validation & pen testing

SHARED RESPONSIBILITY

WHO OWNS WHAT

AWS

Infrastructure + AgentCore

Nozomi Networks

OT protocol analysis + XIoT discovery

Splunk

Unified detection & SOAR

Customer

Device config, access & response

Start with a Free SHIP (Security Health Improvement Program) Assessment — discover your Physical AI security gaps in 4 weeks

NOZOMI NETWORKS | splunk> a CISCO company | aws

Live Q&A

Thank You

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

nozominetworks.com