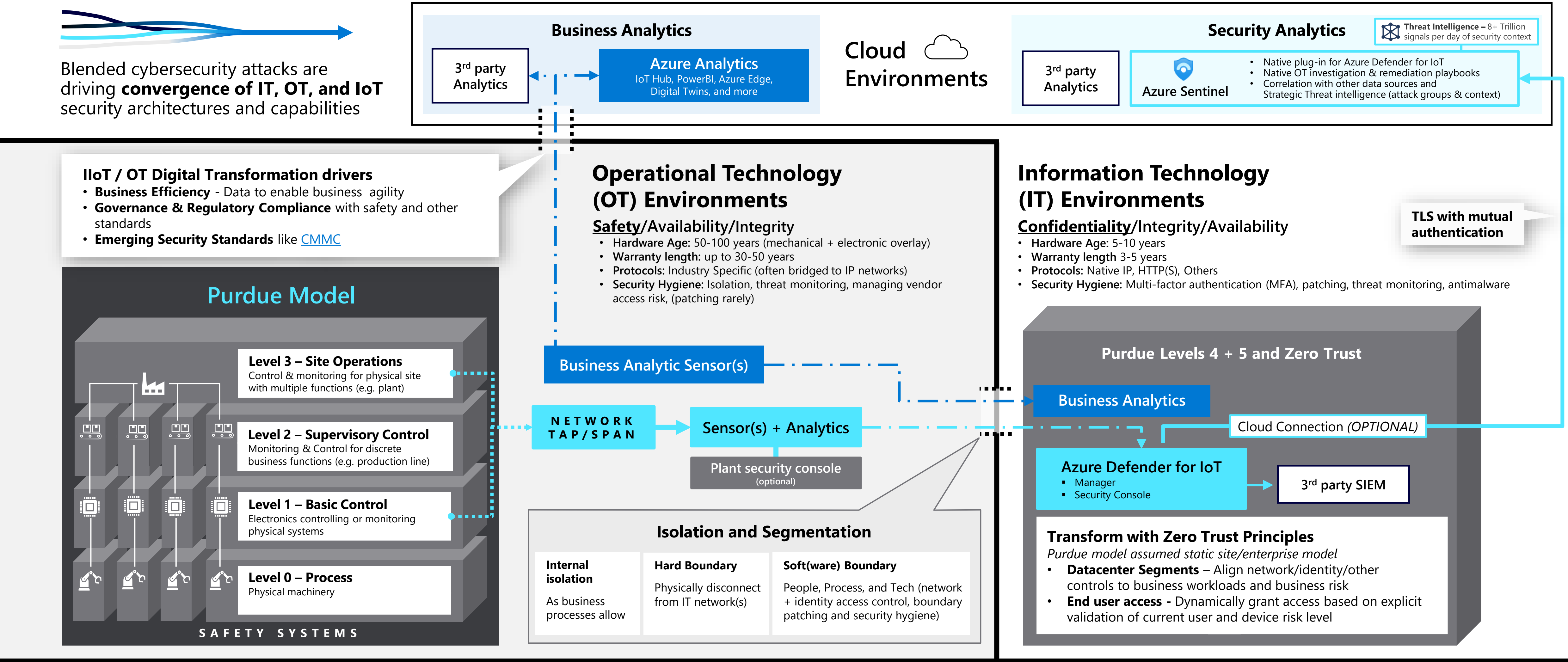
Microsoft

Defender for IoT
Zero Trust Background

Operational Technology (OT) Security Reference Architecture

Apply zero trust principles to securing OT and industrial IoT environments

November 2020 – https://aka.ms/MCRA



Blended cybersecurity attacks are driving **convergence of IT, OT, and IoT** security architectures and capabilities

Cloud Environments

Business Analytics

- 3rd party Analytics
- Azure Analytics – IoT Hub, PowerBI, Azure Edge, Digital Twins, and more

Security Analytics

Threat Intelligence – 8+ Trillion signals per day of security context

- 3rd party Analytics
- Azure Sentinel
  - Native plug-in for Azure Defender for IoT
  - Native OT investigation & remediation playbooks
  - Correlation with other data sources and Strategic Threat intelligence (attack groups & context)

IIoT / OT Digital Transformation drivers

- **Business Efficiency** - Data to enable business agility
- **Governance & Regulatory Compliance** with safety and other standards
- **Emerging Security Standards** like CMMC

Purdue Model

Level 3 – Site Operations
Control & monitoring for physical site with multiple functions (e.g. plant)

Level 2 – Supervisory Control
Monitoring & Control for discrete business functions (e.g. production line)

Level 1 – Basic Control
Electronics controlling or monitoring physical systems

Level 0 – Process
Physical machinery

SAFETY SYSTEMS

Operational Technology (OT) Environments

Safety/Availability/Integrity

- **Hardware Age:** 50-100 years (mechanical + electronic overlay)
- **Warranty length:** up to 30-50 years
- **Protocols:** Industry Specific (often bridged to IP networks)
- **Security Hygiene:** Isolation, threat monitoring, managing vendor access risk, (patching rarely)

Business Analytic Sensor(s)

NETWORK TAP/SPAN → Sensor(s) + Analytics

Plant security console (optional)

Isolation and Segmentation

Internal isolation	Hard Boundary	Soft(ware) Boundary
As business processes allow	Physically disconnect from IT network(s)	People, Process, and Tech (network + identity access control, boundary patching and security hygiene)

Information Technology (IT) Environments

Confidentiality/Integrity/Availability

- **Hardware Age:** 5-10 years
- **Warranty length** 3-5 years
- **Protocols:** Native IP, HTTP(S), Others
- **Security Hygiene:** Multi-factor authentication (MFA), patching, threat monitoring, antimalware

TLS with mutual authentication

Purdue Levels 4 + 5 and Zero Trust

Business Analytics

Cloud Connection *(OPTIONAL)*

Azure Defender for IoT
- Manager
- Security Console

3rd party SIEM

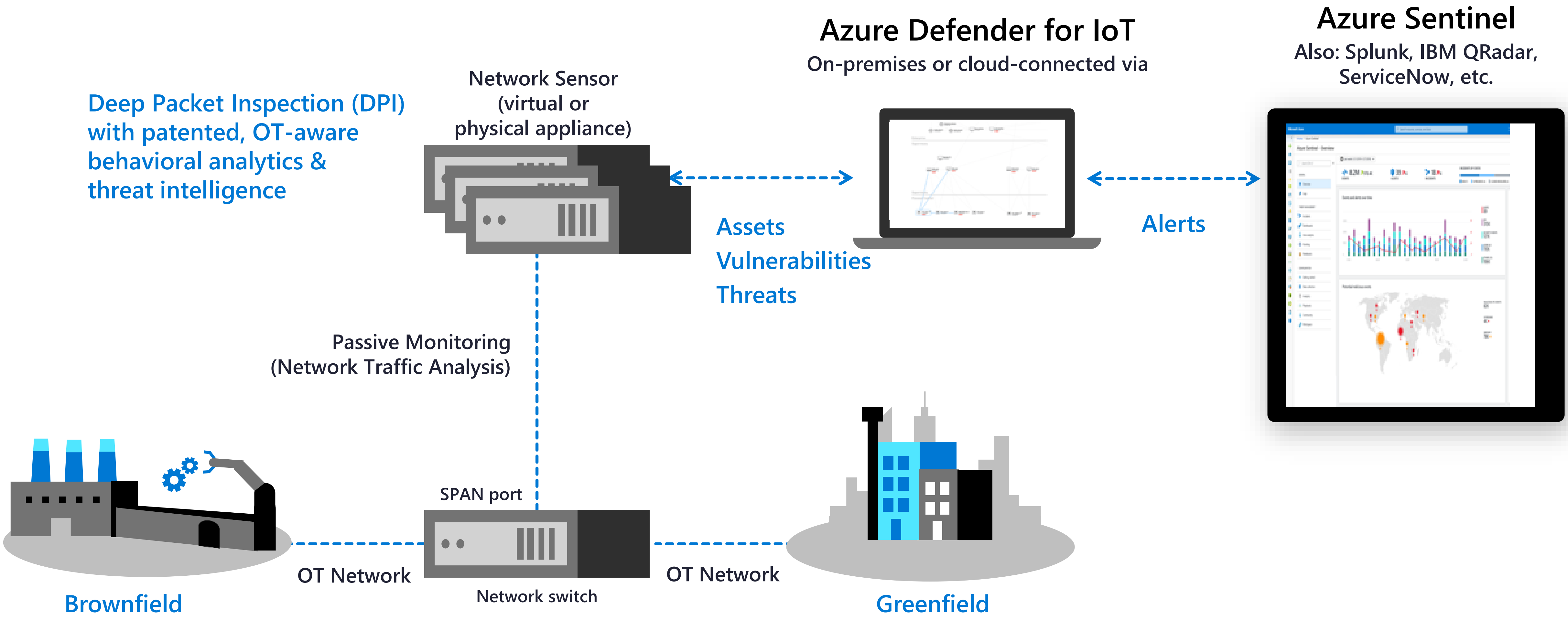
Transform with Zero Trust Principles

Purdue model assumed static site/enterprise model

- **Datacenter Segments** – Align network/identity/other controls to business workloads and business risk
- **End user access** - Dynamically grant access based on explicit validation of current user and device risk level

Zero Trust Principles - Assume breach, verify explicitly, Use least privilege access (identity and network)

Fast and frictionless deployment with zero production impact



Deep Packet Inspection (DPI) with patented, OT-aware behavioral analytics & threat intelligence

Network Sensor (virtual or physical appliance)

Azure Defender for IoT

On-premises or cloud-connected via

Azure Sentinel

Also: Splunk, IBM QRadar, ServiceNow, etc.

Assets

Vulnerabilities

Threats

Alerts

Passive Monitoring (Network Traffic Analysis)

SPAN port

Network switch

OT Network

OT Network

Brownfield

Greenfield

Zero trust for IoT/OT — recommendations

Verify explicitly.

Implement least privileged access.

Assume compromise.

Apply basic hygiene.

Patch where possible.

Implement MFA.

Train employees.

Implement continuous monitoring.

Detect unauthorized & compromised devices with behavioral anomaly detection.

Implement micro-segmentation using asset discovery & network mapping.

Unify IT & IoT/OT security monitoring and governance in your SOC.

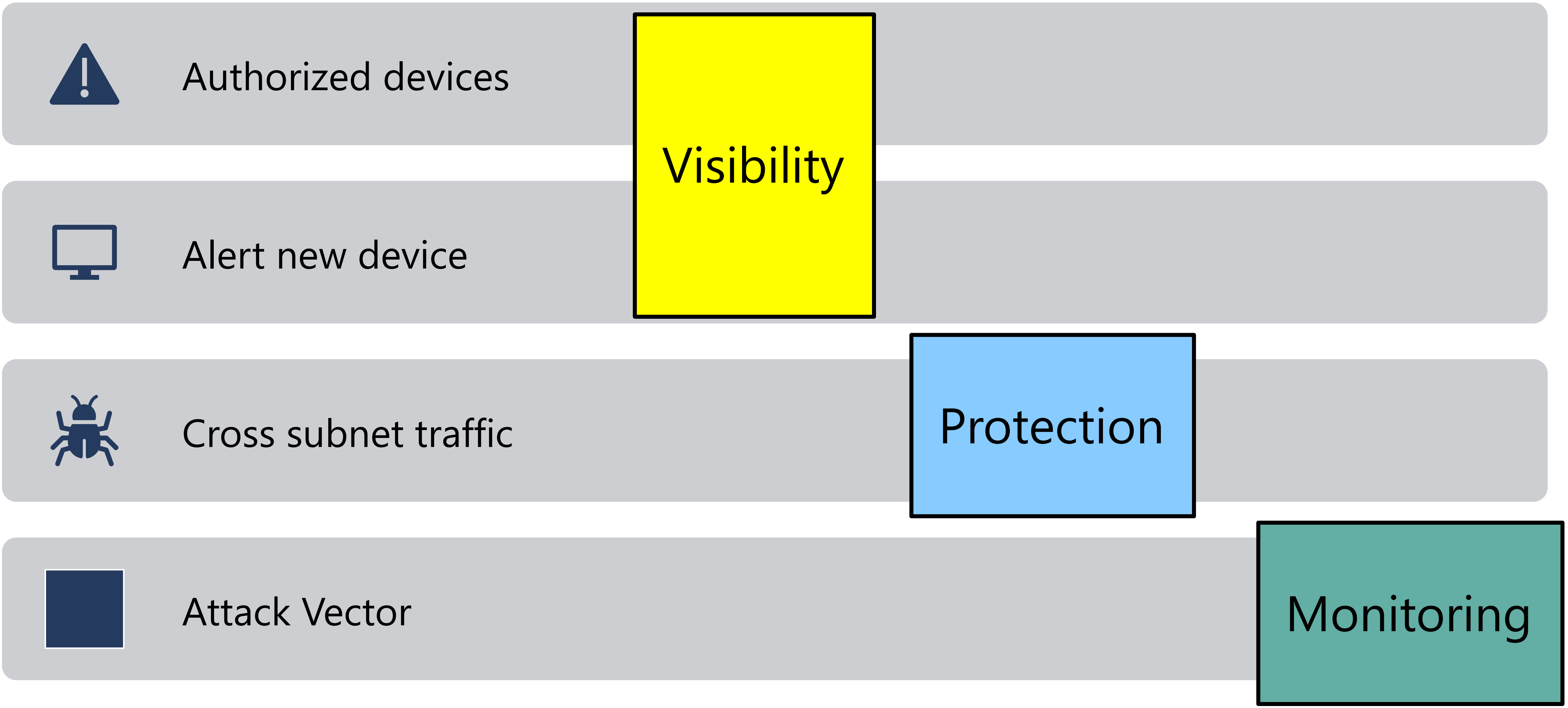
Leverage MITRE ATT*CK for ICS.

Automate incident response (SOAR).

Zero Trust for OT & IoT Environments

- **Visibility**
  - Discover and classify assets with business critical, safety, and operational/physical impact
- **Protection**
  - Isolate assets from unneeded internet/production access with static and dynamic controls
- **Monitor**
  - Unify threat detection and response processes for OT, IT, and IoT assets

Zero Trust Scenarios



- Authorized devices
- Alert new device
- Cross subnet traffic
- Attack Vector

Visibility

Protection

Monitoring