HONEYWELL FORGE
Cybersecurity+

HONEYWELL CYBER PROACTIVE DEFENSE

TRANSFORMING OT SECURITY FROM REACTIVE RESPONSE TO PROACTIVE RISK ANTICIPATION

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL FORGE
Cybersecurity+

THE CHALLENGE OF ANTICIPATING AND RESPONDING TO OT-TARGETED CYBER ATTACKS

OTD BİLİŞİM
GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

THE PROACTIVE DEFENSE CHALLENGE

Key Challenges in OT Cybersecurity

- **Legacy OT Infrastructure**
  Difficult to secure aging ICS/OT systems without full replacement.
- **Rapid Digital Transformation**
  Mobile, cloud, IoT, and remote work expand the attack surface, demanding stronger OT/IoT protection.
- **Advanced Persistent Threats (APTs)**
  Sophisticated, targeted attacks—often ransomware or geopolitically driven—require proactive defense.
- **Limited OT-Specific Visibility**
  Lack of insight into OT-tailored indicators of compromise (IOCs) hinders early detection and response.

MANY COMPANIES STILL LACK COMPREHENSIVE VISIBILITY INTO THEIR OT NETWORKS

HONEYWELL FORGE
Cybersecurity+

OTD BİLİŞİM
GLOBAL VAD

ARE YOUR PEOPLE, PROCESSES, AND SYSTEMS SECURE AGAINST CYBER THREATS?

QUESTIONS TO CONSIDER…

Can you detect threats across your OT systems in real time?

- Gaining continuous visibility into OT networks remains a major challenge for many organizations.
- Traditional IT security tools and practices often fail to address the unique demands of OT environments.
- Only 13% of organizations consider their OT cybersecurity posture to be very mature, highlighting a critical gap compared to IT (1).
- Honeywell Cyber Proactive Defense (CPD) helps close this gap by acting as a digital SOC analyst, enriching and correlating OT data to surface threats early, automate response, and strengthen overall visibility.

Can You Detect A Cyber Attack In Your OT Environment?

- Less than 10% of industrial companies have full-time visibility into their OT networks.
- Most organizations lack in-house expertise to manage OT cybersecurity effectively.
- OT security tools are complex, costly, and difficult to deploy without expert support.

Is Your Response Time Fast Enough?

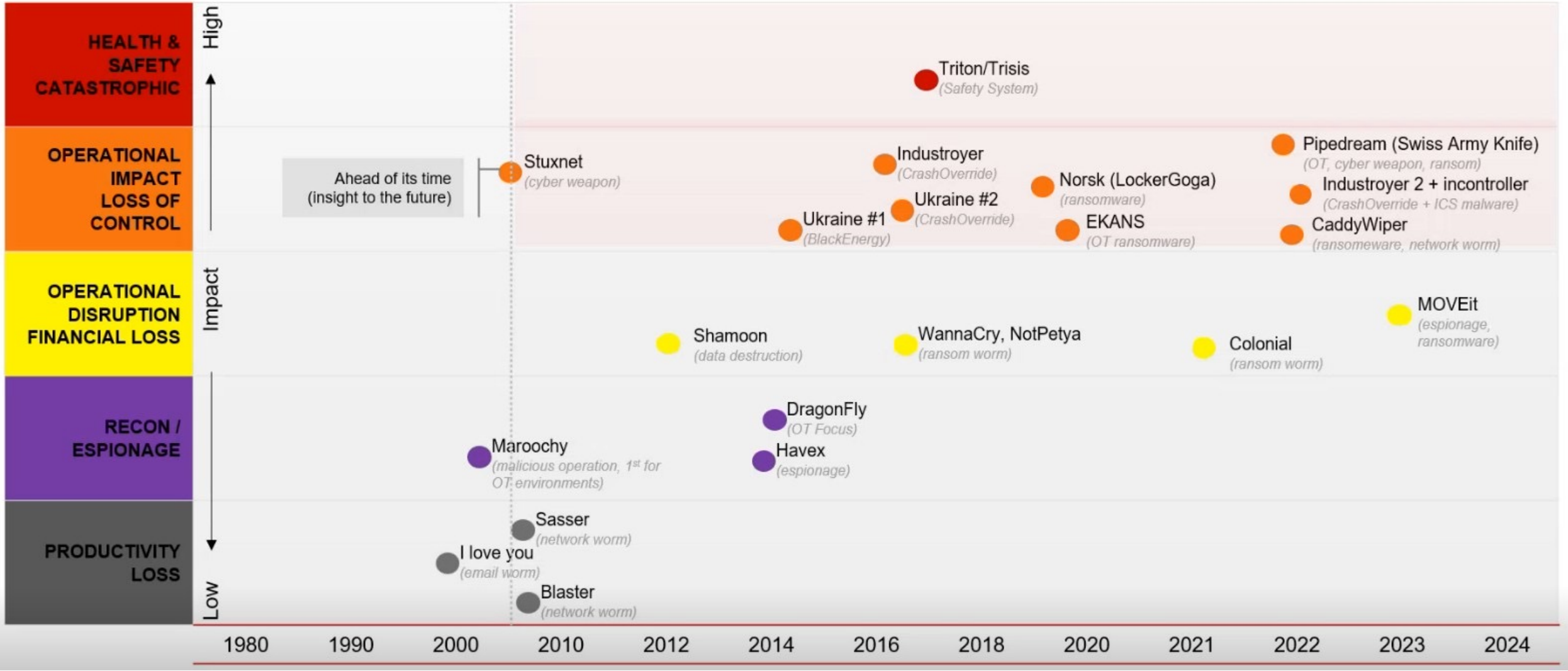
- Many organizations lack OT-specific incident response plans, leaving them unprepared during a cyberattack.
- Limited visibility into OT networks makes it difficult to detect and respond to threats in real time.
- The complexity and interdependence of OT systems hinder effective threat isolation and containment.
- Cyberattacks on OT systems can directly disrupt physical operations, unlike traditional IT breaches.

BEST-IN-CLASS COMPANIES HAVE GOOD ANSWERS TO THESE QUESTIONS

HONEYWELL FORGE Cybersecurity+

EXAMPLES: INDUSTRIAL CYBERSECURITY

ATTACK IMPACT INCREASING



TOP 6 BEHAVIORS USED IN THESE APT ATTACKS

01 **File Creation/ Modification**

Creating or modifying files on the system.

02 **Command Execution**

Executing commands using power-shell on assets.

03 **Process Creation**

Creating new processes or services on the assets.

04 **Network Traffic Flow**

Patterns, characteristics and signatures of remote activities.

05 **OS API Execution/ Module Load**

Advanced operations carried out on assets.

06 **Windows Registry Changes**

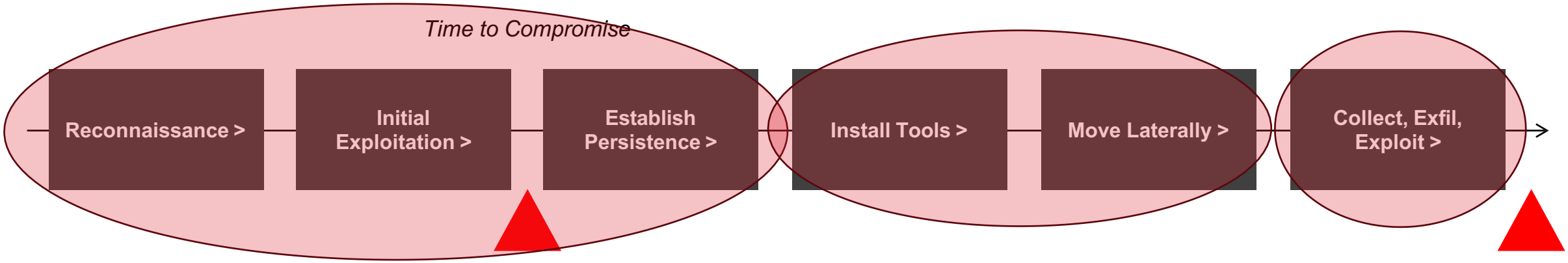
Creation, modification and deletion of entities to disrupt asset functioning

OTD BİLİŞİM
GLOBAL VAD

ANATOMY OF AN ATTACK

An attacker typically remains undetected for an average of **292 Days**[1]

DAYS- MONTHS | **MINUTES - DAYS** | **MINUTES - DAYS** | **DAYS- MONTHS**



LEARN AND LAND | LAND AND EXPAND | DAMAGE

HONEYWELL FORGE Cybersecurity+

HONEYWELL FORGE
Cybersecurity+

SHIFTING FROM REACTIVE DEFENSE TO PROACTIVE RISK ANTICIPATION

OTD BİLİŞİM
GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

BEST PRACTICES FOR ACHIEVING PROACTIVE CYBER DEFENSE

Proactive Threat Detection with CPD

- Fully automated process: from data collection to actionable recommendations
- Enriches and correlates data across OT environments for early threat identification
- Detects behavioral deviations using advanced ML models
- Goes beyond passive monitoring with deception technology (OT honeypots)
- Integrates multiple cyber tools for unified threat visibility
- Promotes early detection by grouping and correlating suspicious events
- Enhances network segmentation analysis with zone-based navigation
- Centralized incident view dashboard for streamlined triage
- Acts as a digital SOC analyst to reduce manual workloads and accelerate response

Threat Anticipation and Intelligence for OT

- Builds enriched threat intelligence tailored to OT environments by correlating data from incident feedback, SOC findings, and external cyber threat feeds.
- Surfaces actionable insights through AI-powered analysis of behavioral anomalies and attacker tactics.
- Leverages OT-specific playbooks, powered by Gen AI, to guide operators in mitigating risks and strengthening defenses against anticipated threats.
- Transforms reactive security into proactive defense, enabling earlier detection and faster response across industrial systems.

HONEYWELL FORGE
Cybersecurity+

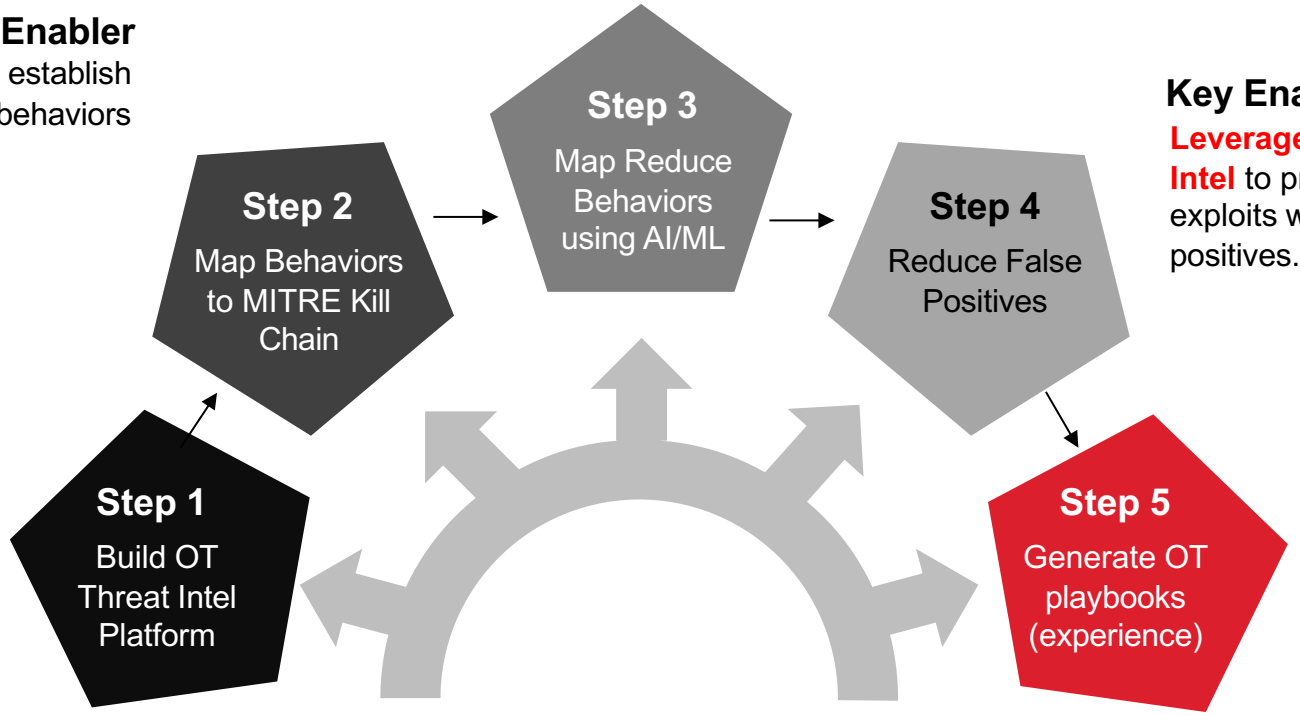
5 STEP PROCESS USING AI/ML TO BETTER ANTICIPATE CYBER ATTACKS

Key Enabler
Use **unsupervised ML models** to detect unknown threats and anomalies by identifying patterns and deviations in ICS/OT environment behavior

Key Enabler
Use AI to establish malicious behaviors

Key Enabler
Leverage OT specific Threat Intel to predict and identify exploits while reducing false positives.

Key Enabler
Use of OT specific Cyber Threat Intel feeds to enrich data



Key Enabler
Use AI and employ cyber assessments and OT expertise with partnerships to build knowledge base in Enterprise View

MOVING FROM REACTIVE TO PROACTIVE CYBERSECURITY

HONEYWELL FORGE
Cybersecurity+

INTRODUCING HONEYWELL CYBER PROACTIVE DEFENSE

OTD BİLİŞİM
GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HONEYWELL CYBER PROACTIVE DEFENSE: DESIGNED FOR PROACTIVE OT CYBERSECURITY

Honeywell Cyber Proactive Defense (CPD) is an AI-powered software solution designed to act as your digital SOC analyst, helping industrial organizations shift from reactive security to proactive risk anticipation. CPD enriches and correlates data across OT environments to detect early-stage threats, automate response, and strengthen overall cyber resilience.

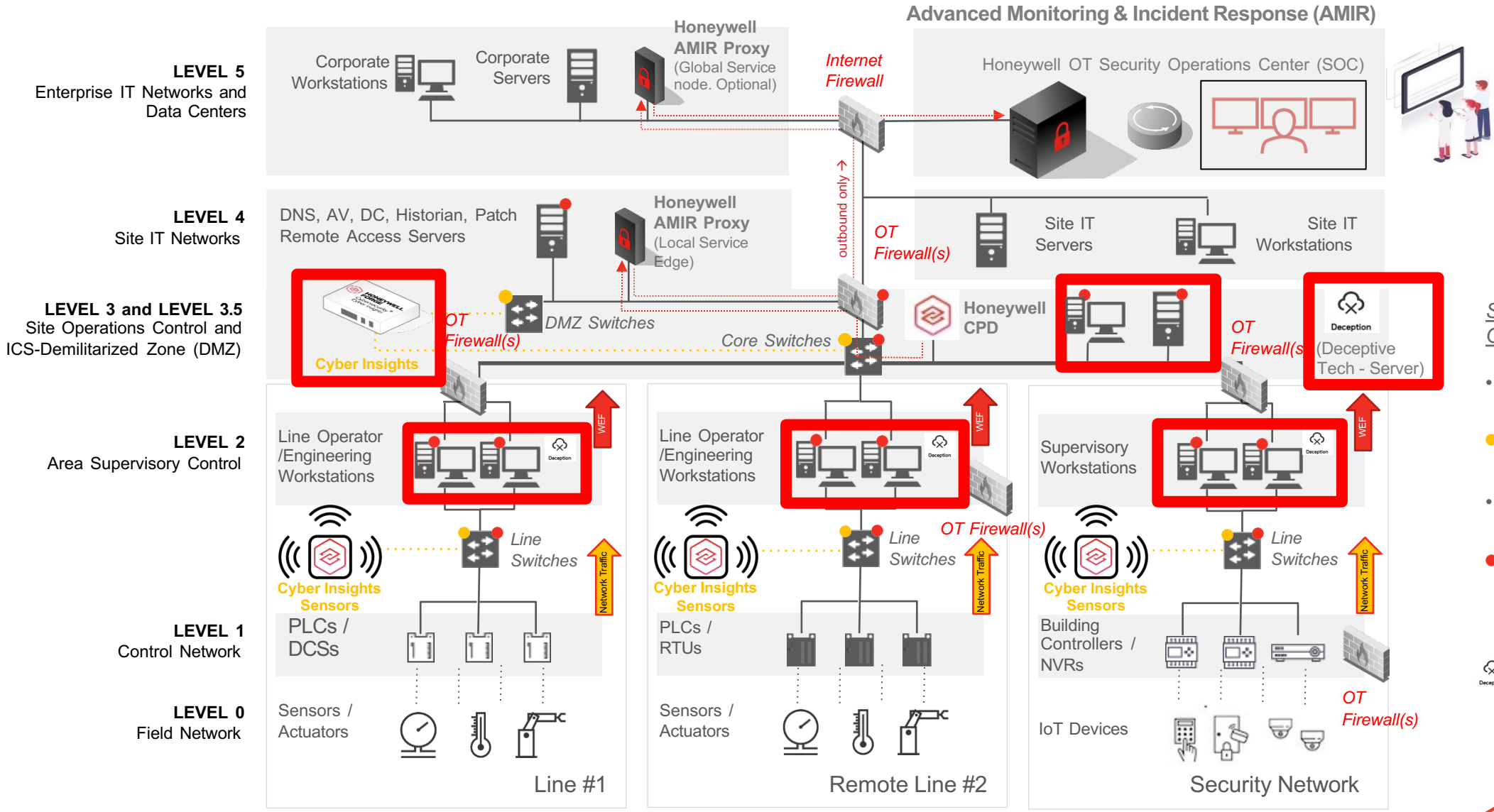
Core Capabilities

- **Process Integration-** Learn/correlate process upsets on engineering or operator assets during the cyber incident duration by integrating and embedding process data (tags and alarms/events)
- **Embedded Process Knowledge & Deception Technology** - CPD enhances threat detection through automated workflows and integrations like OT honeypots, which surface actionable intel and trigger alerts. Embedded industrial context enables tailored detection and faster response.
- **AI/ML-Driven Detection -** Identifies behavioral anomalies using machine learning and continuously adapts defenses based on enriched threat intelligence.
- **Automated Playbooks -** Guides operators with structured, AI-powered workflows that accelerate incident response and reduce human error.
- **Digital Analyst Functionality -** Automates data normalization, correlation checks, and first-line remediation—freeing up SOC teams to focus on high-value investigations.

DO MORE TO HELP IDENTIFY OT CYBER ATTACKS BEFORE THEY HAPPEN

HONEYWELL FORGE
Cybersecurity+

OT Network Design Architecture: Performance + Security

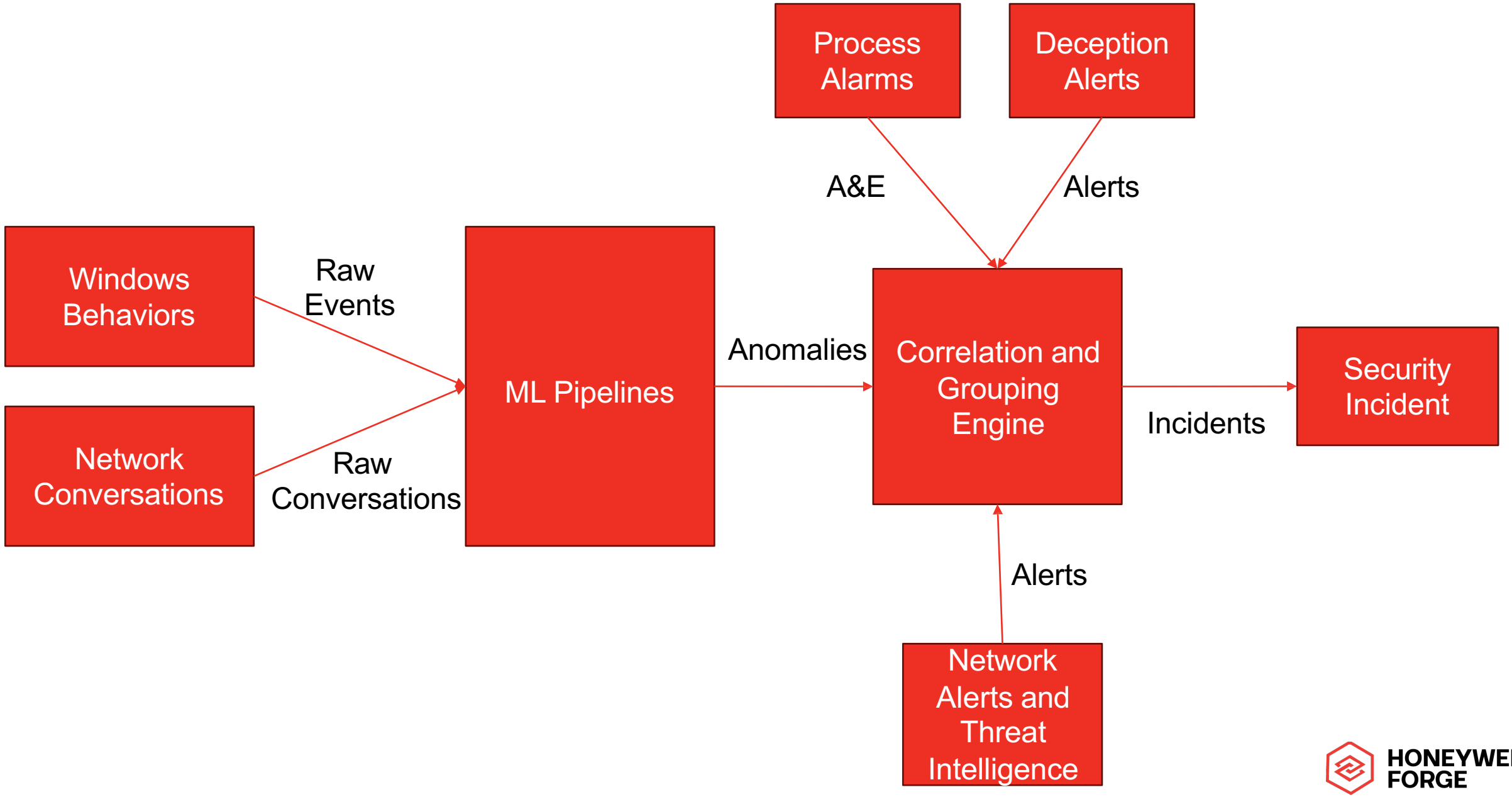


Standalone Solution or Optional add-on to AMIR:

- *Cyber Insights to aid with asset detection, threat detection, and network anomaly detection*
- *Honeywell Cyber Proactive Defense Asset ingestion analyzed with Machine learning and AI for security incident generation.*
- *Honeywell Cyber Proactive Defense (Deception Server and Sensor)*

OTD BİLİŞİM GLOBAL VAD

HONEYWELL FORGE Cybersecurity+


Process Alarms
Deception Alerts
A&E
Alerts
Windows Behaviors
Raw Events
ML Pipelines
Anomalies
Correlation and Grouping Engine
Security Incident
Network Conversations
Raw Conversations
Incidents
Alerts
Network Alerts and Threat Intelligence

HONEYWELL OT CYBERSECURITY PORTFOLIO: A UNIFIED DEFENSE-IN-DEPTH

OTD BİLİŞİM GLOBAL VAD

Product	Core Capability	Value Proposition
Cyber Proactive Defense	AI/ML-based platform for behavioral analytics, deception technology (honeypots), and automated incident response playbooks.	Predictive Defense: Predicts and prevents unknown, zero-day, and living-off-the-land attacks to ensure operational resilience and uptime.
OT SOC / AMIR	24/7 Managed Services for centralized log collection, expert monitoring, threat hunting, and incident investigation. Provides an incident response retainer.	Expertise-as-a-Service: Provides a dedicated, world-class OT security team without the overhead, ensuring rapid and effective incident response.
Cyber Insights	Agentless asset discovery with real-time vulnerability management, passive network monitoring, and risk scoring.	Holistic Visibility: Creates a real-time, comprehensive view of all OT assets and their security posture, simplifying risk prioritization and compliance.
Secure Media Exchange (SMX)	Honeywell solution for removable media with multi-threat intel sources malware scanning, file verification, enforcement, protection against impersonating devices, firmware modification attacks and for USB device control.	Closes a Critical Attack Vector: Proactively blocks USB-borne malware, a primary entry point for threats, to protect OT networks at the physical perimeter.

Unified Defense Strategy:

The Honeywell portfolio works together as a cohesive, layered defense. SMX acts as the first line of defense at the physical perimeter. Cyber Insights provides the essential real-time context of all assets. Cyber Proactive Defense is the intelligence layer, using AI/ML to predict and detect subtle behavioral anomalies. Finally, the OT SOC and AMIR managed services provide the expert human oversight and rapid response required to neutralize threats before they can impact operations.

HONEYWELL FORGE Cybersecurity+

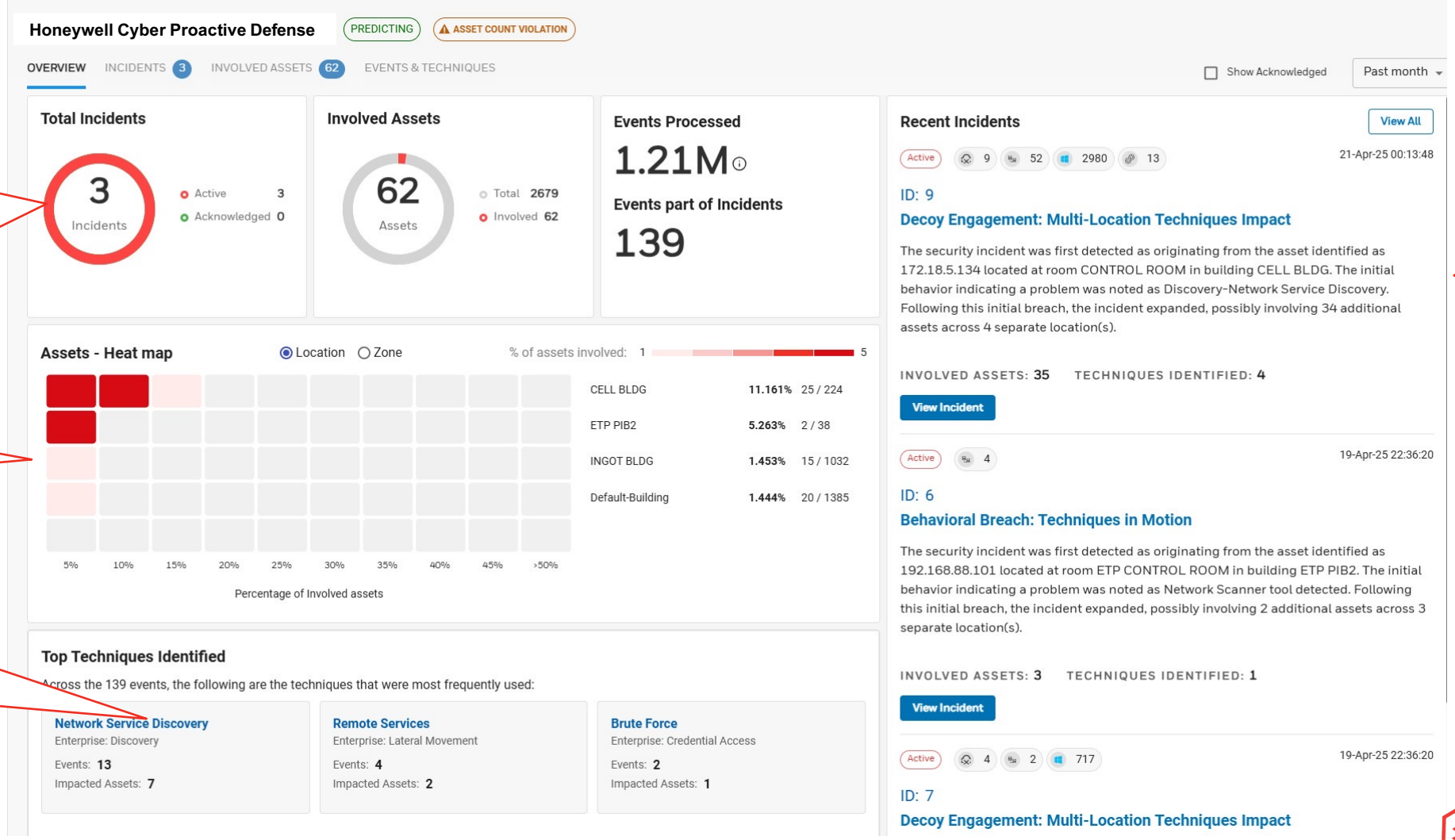
AI-POWERED CORRELATION, ENRICHED THREAT INTELLIGENCE, AND GUIDED RESPONSE

Details on security incidents within the customer environment, including their current status and resolution progress.

Asset Heat Map by Location or Zone

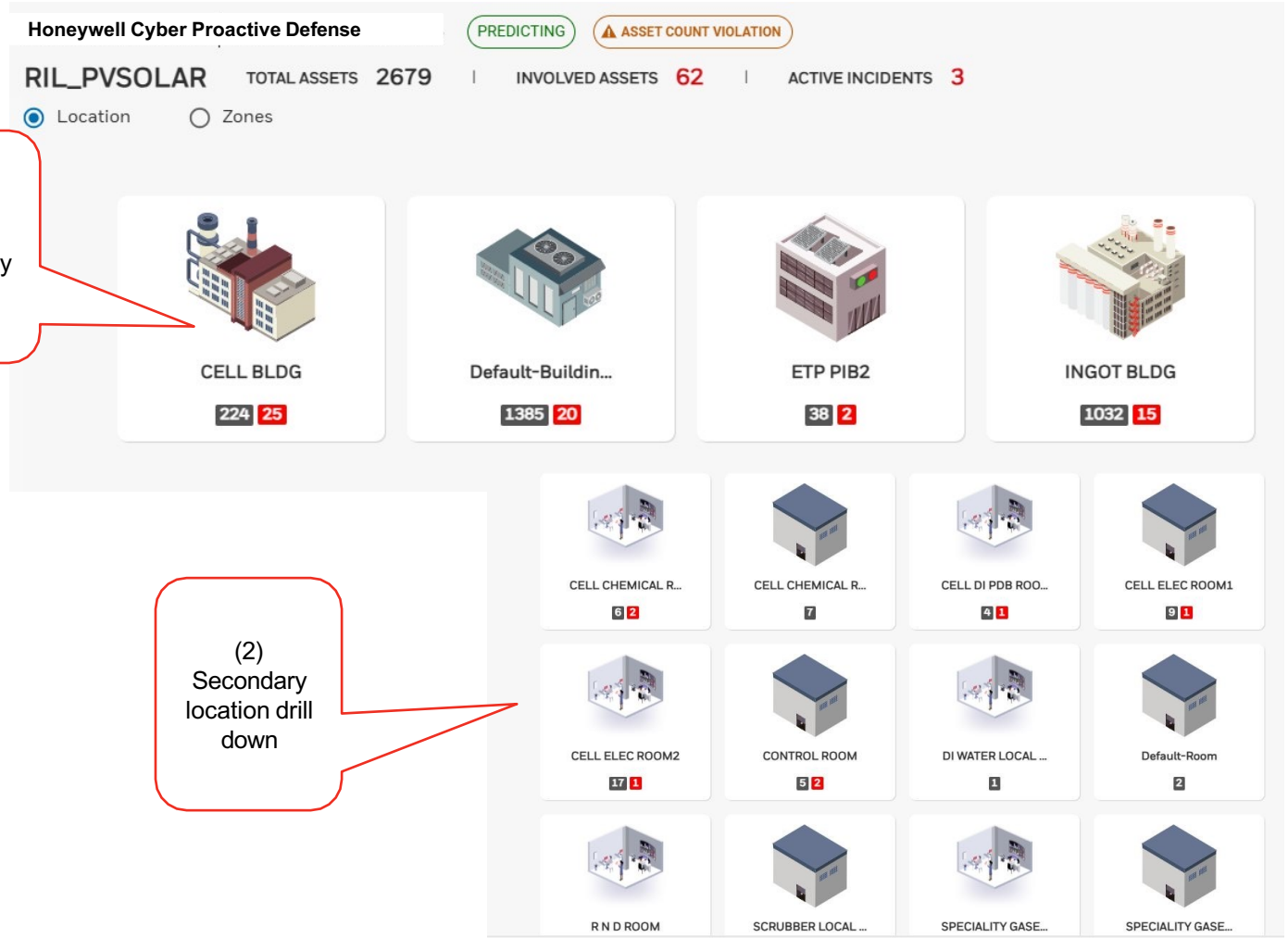
Information on Attack Tactics and Techniques

AI/Machine Learning–Driven Event Prioritization and Correlation



DRILL-DOWN INSIGHTS FOR PROACTIVE THREAT MANAGEMENT

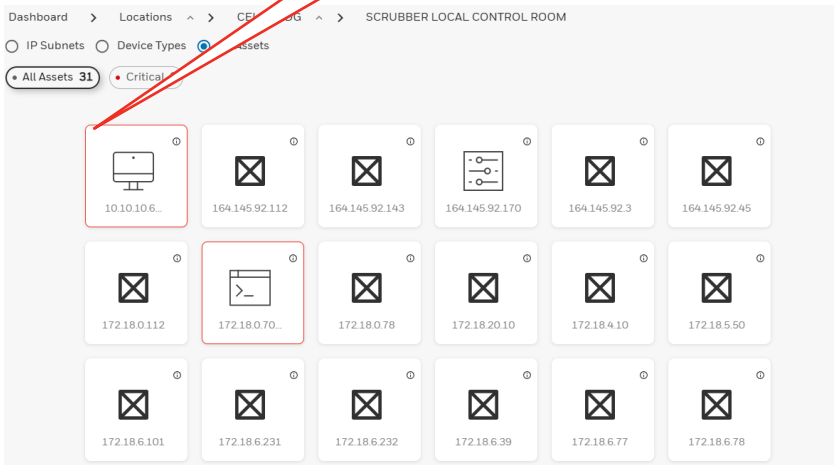
(1)
High level overview by location



(2)
Secondary location drill down

(3)
Advanced drill down by IP/device

Ex. 10.79.218.9/assets

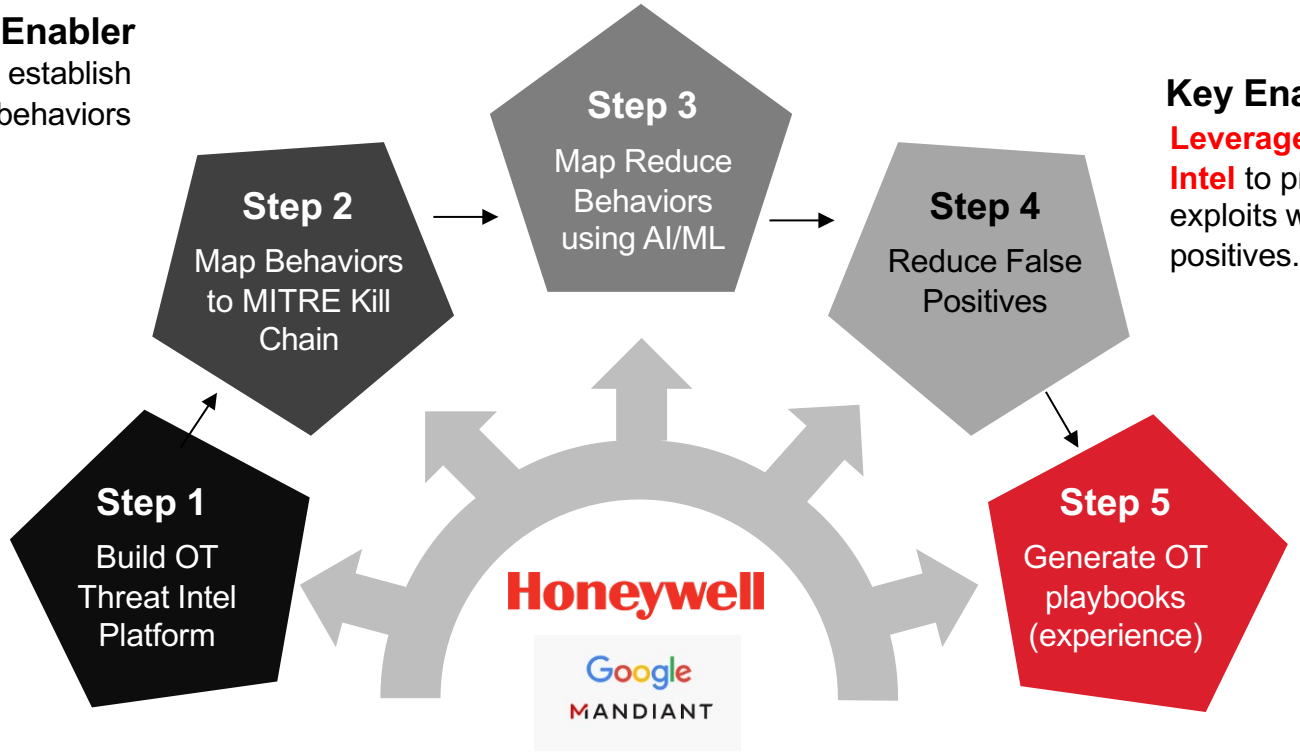


HONEYWELL'S SOLUTION FOR THE 5 STEP PROCESS USING AI/ML

Key Enabler
Use **unsupervised ML models** to detect unknown threats and anomalies by identifying patterns and deviations in ICS/OT environment behavior

Key Enabler
Use AI to establish malicious behaviors

Key Enabler
Leverage OT specific Threat Intel to predict and identify exploits while reducing false positives.



Key Enabler
Use of OT specific Cyber Threat Intel feeds to enrich data – **supported by Google Threat Intelligence along with data from preemptive cybersecurity technologies (deception)**

Key Enabler
Use AI and employ cyber assessments and OT expertise with partnerships to build knowledge base in Enterprise View

MOVING FROM REACTIVE TO PROACTIVE CYBERSECURITY

CYBER PROACTIVE DEFENSE- YOUR DIGITAL SOC ANALYST

SOC Analyst Duties	How Honeywell Cyber Proactive Defense Addresses It (Automated & Predictive)
Alert Triage & Investigation: Tier 1 analysts review high volumes of alerts from SIEM, EDR, etc., to filter false positives and identify real threats.	**AI-Powered Monitoring & Alert Reduction** Uses ML to baseline OT network behavior, filters benign events, and correlates data into high-fidelity alerts—reducing alert fatigue and triage time.
Threat Hunting: Tier 3 analysts proactively search for undetected threats using manual techniques and deep knowledge of attacker behavior	**Embedded Process Knowledge & Deception Technology** CPD enhances threat detection through automated workflows and integrations like OT honeypots, which surface actionable intel and trigger alerts. Embedded industrial context enables tailored detection and faster response.
Incident Response & Containment: Analysts isolate affected systems, block malicious traffic, and contain threats under time-critical conditions.	**AI-Powered Response Playbooks** Automates incident response with customizable workflows to isolate devices, block C2 traffic, and contain threats—cutting response time significantly.
Threat Intelligence & Analysis: Analysts identify threats and recommend actions, often using manual scans and report reviews.	**Threat Intelligence Integration** : Integrates Honeywell and Google threat feeds to stay current on emerging threats and prioritize remediation.
Root Cause Analysis & Reporting : Post-incident, analysts perform forensics, document findings, and generate reports to assess impact and prevent recurrence.	**Automated Data Collection & Reporting:** CPD enriches existing telemetry with industrial context, enabling root cause analysis without duplicating monitoring. Automated correlation streamlines reporting, allowing analysts to focus on strategic decisions.

OTD BİLİŞİM
GLOBAL VAD

HOW CPD ACTS AS YOUR DIGITAL SOC ANALYST

- **Acts as an intelligent assistant:** The platform provides enriched, real-time insights and prioritized threat alerts, enabling faster, more accurate decision-making by the SOC team.
- **Empowers SOC Analyst:** Cyber Proactive Defense is a sophisticated solution that augments the skills of SOC analysts, allowing them to focus on complex, high-impact tasks.
- **Automates the mundane:** It handles the continuous, repetitive tasks of data correlation and initial threat identification, freeing up analysts for in-depth investigations and strategic threat hunting.
- **Enhances efficiency and speed:** By automating incident response with AI-powered playbooks, it ensures a rapid and consistent reaction to threats, allowing the SOC team to operate more efficiently.
- **Scales human expertise:** It acts as a force multiplier, extending the reach and effectiveness of the human team to handle the increasing volume and sophistication of cyber threats.

HONEYWELL FORGE Cybersecurity+

HONEYWELL FORGE
Cybersecurity+

USE CASE
HONEYWELL CYBER PROACTIVE DEFENSE

OTD BİLİŞİM
GLOBAL VAD

POWER GENERATION USE CASE

CHALLENGE

The utility faced escalating cyber threats targeting its operational technology (OT) network, including sophisticated intrusion attempts from advanced persistent threats (APTs). With limited OT cybersecurity staff and no real-time threat visibility, the organization struggled to respond swiftly and effectively.

Solution

- To proactively strengthen its OT cybersecurity posture, the utility deployed Honeywell Cyber Proactive Defense (CPD)—an AI-powered software solution designed to act as a digital SOC analyst. CPD:
- Enriched and correlated network data to surface behavioral anomalies before they escalated into incidents.
- Threat detection was enriched through multiple integrations, including deception technologies like strategically placed OT honeypots that surfaced suspicious activity and diverted attackers from high-value assets.
- Activated AI-driven playbooks to automate incident response, reducing reaction time from hours to minutes.

OUTCOME

- Within weeks, the utility detected and neutralized multiple intrusion attempts without operational disruption. CPD’s automated playbooks empowered the lean security team to respond efficiently, while the deception layer provided early warning and enriched intelligence—transforming reactive defense into proactive resilience.

OTD BİLİŞİM
GLOBAL VAD

SUMMARY

- Customers face growing challenges in scaling threat hunting and analysis across complex OT environments.
- Honeywell Cyber Proactive Defense (CPD) delivers a layered, proactive cybersecurity strategy to detect, deceive, and respond before threats cause harm.
- CPD enriches and correlates behavioral data using AI to identify anomalies and anticipate potential attacks.
- CPD enhances threat detection through automated workflows and integrations like OT honeypots, which surface actionable intel and trigger alerts. Embedded industrial context enables tailored detection and faster response.
- AI-powered playbooks automate and orchestrate incident response for faster, more consistent threat mitigation.
- CPD acts as a digital SOC analyst, empowering lean security teams to shift from reactive defense to proactive resilience.

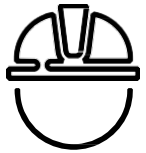
Critical Business Outcomes Enabled by Honeywell Cyber Proactive Defense

HONEYWELL FORGE
Cybersecurity+

WHY CHOOSE HONEYWELL

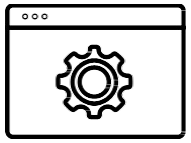
OTD BİLİŞİM
GLOBAL VAD

HONEYWELL'S OT CYBER STRENGTHS



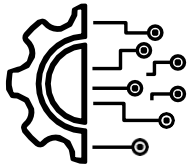
PEOPLE

- Over 25 years of experience in OT cybersecurity
- Global presence with 500+ employees dedicated to OT cybersecurity in 37 countries
- 7000+ projects delivered in 130+ countries



EXPERTISE

- Access to top experts and industry insights across Honeywell
- Global Cybersecurity Centers of Excellence and Innovation in Atlanta, Singapore and Dubai
- Global OT Managed Security Services for industry expertise
- 38 patents in OT cybersecurity



SOLUTIONS

- Products and services for a full end-to-end solutions
- Products seamlessly integrate with 3rd party solutions for effective resolution of cyber threats
- Services also complemented by partnerships with best-in-class security vendors, such as Google and Fortinet

COLLABORATION

- Industry partners (e.g., OT Cyber Coalition – founding member)
- Standards partners (e.g, ISASecure – founding member)
- Supporting government agencies (e.g. CISA, CSA Singapore)

OTD BİLİŞİM GLOBAL VAD

HONEYWELL CYBER PROACTIVE DEFENSE IS PART OF A LARGER OT CYBERSECURITY SOLUTION

★ Coming Soon

HONEYWELL OT CYBERSECURITY PLATFORM

ASSET DISCOVERY, RISK AND VULNERABILITY ANALYSIS

PROACTIVE DEFENSE THROUGH BETTER THREAT DETECTION AND RESPONSE

ACCESS OT SPECIFIC THREAT INTELLIGENCE

ENTEPRISE VIEW OF RISK, VULNERABILITIES AND COMPLIANCE

Cyber Insights*	Cyber Proactive Defense	Cyber Threat Intelligence	Cyber Governance, Risk and Compliance ★
Cyber Watch*	Secure Media Exchange		

*Single and Multi-Site

HONEYWELL OT CYBERSECURITY SERVICES

PROFESSIONAL SERVICES

- 30+ professional services supporting the full lifecycle of OT cybersecurity (assessments, remediation, architecture & design, training courses & much more)
- Cyber Care services (on-site)
- Integration of 3rd party technologies

MANAGED SECURITY SERVICES

- Secure remote access
- Patch / AV management
- Cyber Care services (remote)

OT SECURITY OPERATIONS CENTER (OT SOC)

- Provides 24x7 real-time threat monitoring and detection combined with built-in advanced security analytics, in-depth incident investigation, and orchestrated incident response

REDUCE PROBABILITY OF COMPROMISE AND SEVERITY OF IMPACT

CALL TO ACTION

- Are you confident in your visibility across all OT assets and environments?
- Do you understand your organization's cyber risk profile and exposure points?
- Would you benefit from AI-powered insights that correlate behaviors and enrich threat detection—helping you anticipate attacks before they occur?

Who are the stakeholders in reviewing your OT?

- CIO/CISO
- Corporate IT
- Plant Manager
- Engineer

- Engage with Honeywell to help your leadership transition toward Cyber Proactive Defense—a strategy designed to strengthen OT environments before threats emerge.
- Leverage OT-specific threat intelligence enriched and correlated across your industrial landscape to reduce cyber risk.
- Gain clarity into your organization's cybersecurity posture with AI-powered insights that surface behavioral anomalies and exposure points.
- Employ Honeywell’s expertise to enable advanced monitoring and automated incident response, empowering your team with digital SOC analyst capabilities.

OTD BİLİŞİM
GLOBAL VAD

THANK YOU

HONEYWELL FORGE
Cybersecurity+

OTD BİLİŞİM
GLOBAL VAD