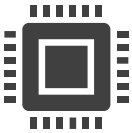
Honeywell | Cyber Proactive Defense

HOW CYBER PROACTIVE DEFENSE (CPD) ELEVATES YOUR CYBERSECURITY

AI-Powered Alert Rationalization & Correlation

- CPD unifies fragmented signals from multiple tools (SIEM, EDR, OT monitoring) into a single, high-fidelity alert.
- Reduces alert fatigue and accelerates triage by filtering out false positives.



Embedded OT Process Knowledge

- Purpose-built for industrial environments, CPD understands operational workflows and threats unique to OT systems.
- Ensures tailored detection and mitigation aligned with industrial context.

Intelligent Incident Grouping & Prioritization

- Groups related alerts into actionable incidents and assigns relevancy scores.
- Enables SOC teams to focus on the most critical threats first, improving efficiency and decision-making.

AI-Powered Response Playbooks

- Automates containment and remediation steps with structured, customizable workflows.
- Reduces incident response time from hours to minutes, minimizing operational downtime.

Integrated Threat Intelligence & Behavioral Baselines

- Combines Honeywell and Google Threat Intelligence with third-party feeds for up-to-date threat context.
- Establishes behavioural baselines to detect anomalies and early signs of malicious activity.

Scalable Force Multiplier for SOC Teams

- Acts as a digital SOC analyst, automating repetitive tasks and augmenting human expertise.
- Scales security operations across distributed environments without adding headcount.

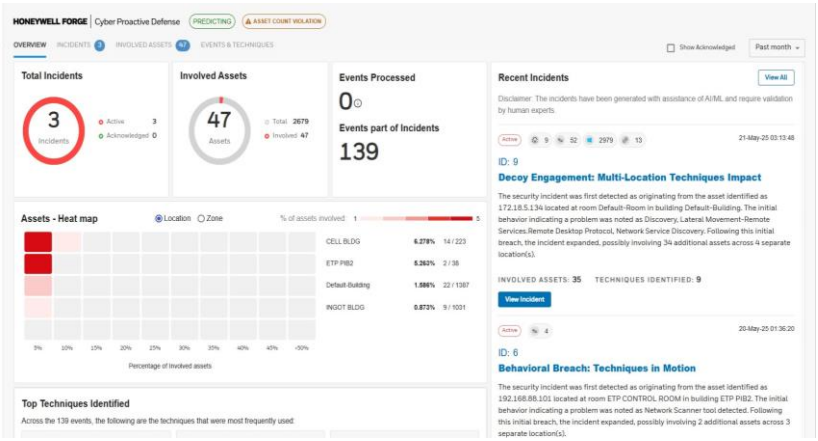
Honeywell Cyber Proactive Defense (CPD) is a forward-looking AI-powered cybersecurity solution purpose built for the unique demands of Operational Technology (OT) environments and AI-enabled cyber threats. By unifying alert rationalization, cross-tool correlation, and intelligent incident grouping, it transforms fragmented signals into actionable insights. Acting as a digital SOC analyst, CPD enriches and correlates data across your industrial environment to proactively identify, prioritize, and mitigate risks before they escalate into full-scale attacks.

The result is reduced noise, faster triage, and a holistic view of industrial risk, empowering defenders to focus on what truly matters: protecting critical operations, ensuring safety, and driving resilience in the face of evolving cyber threats.

CPD PRODUCT HIGHLIGHTS

- **Empowers SOC Analysts:** 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 collection and correlation, freeing up analysts for in-depth investigations and strategic threat hunting.
- **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.
- **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.

By integrating AI-driven behavioural analytics and leveraging the Honeywell Cyber Threat Intelligence platform, powered by products such as Google Threat Intelligence (GTI), CPD delivers enriched, near real-time insights and advanced analytics tailored to the unique demands of OT systems. CPD supports a wide range of integrations to enhance incident correlation and response readiness.



CPD can ingest telemetry from a variety of sources including deception technology, with strategically deployed OT honeypots to enrich visibility, suspicious surface activity, and divert attackers away from critical assets. Additionally, AI powered incident response playbooks enrich response efforts by offering structured intelligent guidance for addressing threats, minimizing downtime, and accelerating recovery.

By embedding deep process knowledge into cyber analysis and aligning with industrial workflows, CPD empowers organizations to adopt a proactive, intelligence-driven approach to cybersecurity, fortifying critical infrastructure against both current and emerging threats.

GET PROACTIVE VISIBILITY FOR YOUR OT CYBERSECURITY POSTURE

Honeywell Cyber Proactive Defense is a forward-looking cybersecurity solution purpose built for the unique demands of Operational Technology (OT) environments. By unifying alert rationalization, cross-tool correlation, and intelligent incident grouping, it transforms fragmented signals into actionable insights. The result is reduced noise, faster triage, and a holistic view of industrial risk, empowering defenders to focus on what truly matters: protecting critical operations, ensuring safety, and driving resilience in the face of evolving cyber threats.

This proactive methodology is especially vital in OT settings, where legacy systems often lack native security features and where downtime can result in significant operational, financial, and safety consequences. By leveraging the Honeywell Cyber Threat Intelligence platform, powered by GTI, CPD delivers near real-time insights and advanced analytics tailored to the unique dynamics of industrial environments.

Additionally, CPD enriches cyber analysis by embedding deep process knowledge and supporting integrations such as deception technologies, various network intrusion detection systems, system logs, and many more. AI powered incident response playbooks further enrich resilience by enabling swift, structured responses to emerging threats.

Through this comprehensive and designed approach, Honeywell enhances the protection of critical infrastructure, supports operational continuity, and upholds safety in environments where even minor disruptions can have far-reaching impacts.

GENERAL USE CASES

SOC ANALYST DUTIES	HOW HONEYWELL CPD ADDRESSES IT (AUTOMATED & PREDICTIVE)
Alert Triage & Investigation: SOC analysts spend significant time reviewing thousands of daily alerts from various systems (SIEM, EDR, etc.) to distinguish real threats from false positives. This is often the primary role of a Tier 1 analyst.	**AI-Powered Monitoring & Alert Reduction:** The solution uses AI and machine learning to establish a "behavioral baseline" for the OT network. It automatically filters out benign events and correlates multiple data points to provide a single, high-fidelity alert for a potential incident, drastically reducing alert fatigue and the time spent on triage.
Threat Hunting: Experienced Tier 3 analysts proactively hunt for hidden threats that have bypassed existing defenses. This is a complex, manual process that requires deep expertise and a good understanding of attacker tactics.	**Embedded Process Knowledge:** The system's embedded process knowledge further strengthens security posture by recognizing threats unique to industrial environments, ensuring tailored detection and mitigation aligned with operational context.
Incident Response & Containment: When an incident is confirmed, analysts must quickly isolate the affected hosts, block malicious communication, and contain the threat to prevent it from spreading. This is a high-pressure, time-critical task.	**AI-Powered Response Playbooks:** The solution uses AI-powered playbooks to automate and accelerate incident response. It provides pre-defined, customizable workflows that can be used to isolate compromised devices, block C2 communications, and initiate containment procedures, reducing response time from hours to minutes.
Vulnerability Analysis: Analysts are responsible for identifying vulnerabilities in their systems and providing recommendations to patch them. This often involves manual scanning and reviewing reports.	**Threat Intelligence Integration:** The platform integrates with Honeywell's and various intel platforms including Google Threat Intelligence. This provides up-to-date threat information helping the system and the analyst to stay ahead of emerging threats and prioritize patching.

SOC ANALYST DUTIES	HOW HONEYWELL CPD ADDRESSES IT (AUTOMATED & PREDICTIVE)
Root Cause Analysis & Reporting: After an incident, analysts must perform forensic analysis, document their findings, and create detailed reports for management to understand the attack's impact and prevent future occurrences.	**Automated Data Collection & Reporting:** CPD enriches existing telemetry with contextual insights tailored for industrial environments. This augmented data stream enables comprehensive root cause analysis without duplicating monitoring efforts. By automating data correlation and surfacing relevant findings, CPD helps streamline reporting and empowers analysts to focus on strategic decision-making rather than manual data collection.

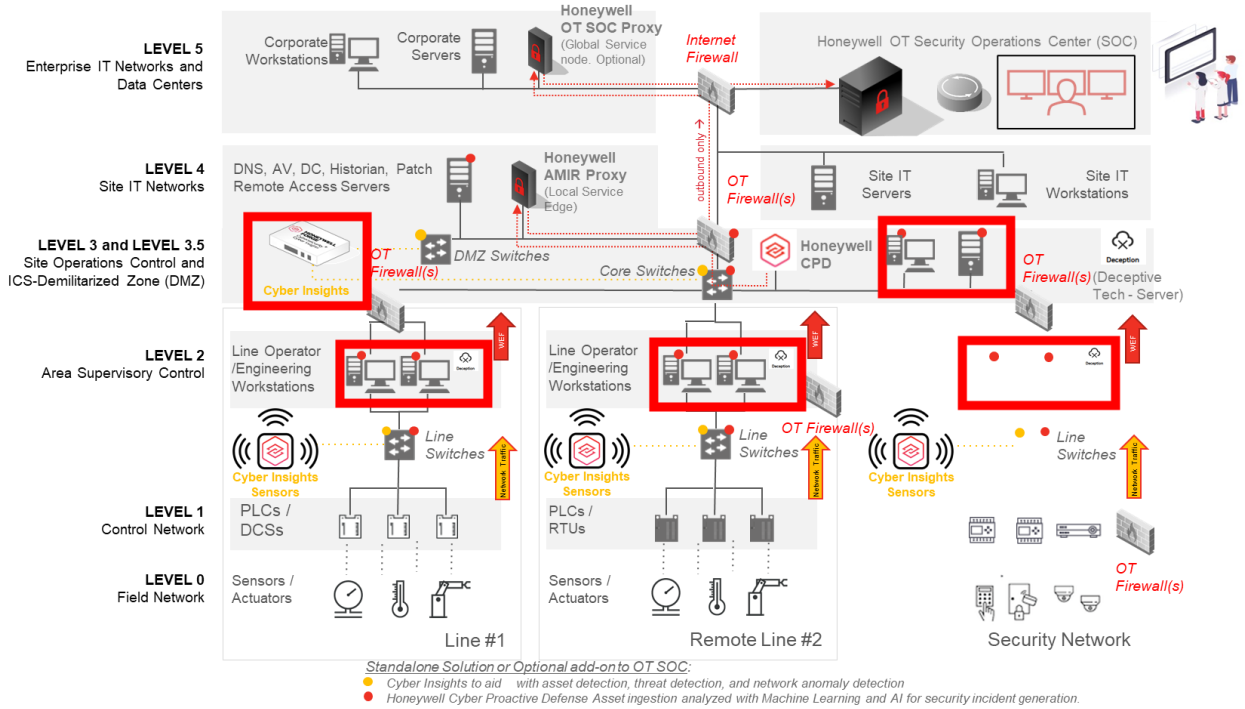
CASE EXAMPLE

An industrial organization operating a complex and aging OT infrastructure faced escalating cybersecurity threats, including targeted attacks from sophisticated adversaries. With limited cybersecurity personnel and no real-time visibility into its OT network, the organization struggled to detect, correlate, and respond to threats effectively placing critical infrastructure and operational continuity at risk.

To address these challenges, the organization deployed Honeywell Cyber Proactive Defense, a comprehensive solution designed to proactively secure OT environments. Leveraging AI and machine learning, the platform continuously monitored network behaviour, establishing a dynamic baseline to detect anomalies indicative of malicious activity. 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. AI powered incident response playbooks further strengthened resilience by automating, mitigation, and reducing response times ensuring consistent action, even with a lean security team.

As a result, the organization successfully detected and neutralized multiple cyber threats without experiencing operational disruptions. The integration of automation, real-time threat intelligence, and proactive defense mechanisms empowered the security team to maintain a strong security posture, enhance resilience, and protect critical infrastructure with limited resources.

NETWORK ARCHITECTURE



Honeywell | Cyber Proactive Defense

HOW CPD ADDRESSES SOC ANALYST DUTIES: FEATURES AND BENEFITS

CORRELATION CAPABILITY

- **Correlation Technology** in a use case such as OT honeypots (decoys) strategically within the network to mislead and divert attackers away from critical assets, reducing risk to core systems.
- **Can detect threats early** in such a use case by monitoring interactions with deceptive elements, surfacing **suspicious activity,** and providing **early warning signals** of potential intrusions.
- **Enriches and correlates threat intelligence** by observing attacker behaviour and tactics in a controlled environment, **without exposing live systems** to risk.

AI & ML

- **Identifies behavioural anomalies** across OT systems using advanced AI and machine learning models, establishing a dynamic baseline of normal activity.
- **Correlates enriched data** from multiple sources to surface suspicious patterns and provide early indicators of emerging threats, without relying on predictive models.
- **Continuously adapts defences in real time**, learning from new data to improve detection accuracy and automate first-line remediation actions.

AI-POWERED PLAYBOOKS

- **Automates incident response** using structured, AI-driven playbooks that guide operators through predefined and customizable workflows.
- **Accelerates containment and mitigation,** reducing response time from hours to minutes, even for lean security teams.
- **Ensures consistent, intelligent actions** across incidents, minimizing human error and enhancing operational efficiency.
- **Empowers SOC teams** by offloading repetitive tasks and enabling faster, more confident decision-making during active threats.

For more information
www.honeywell.com/cybersecurity

Honeywell
855 Mint St Charlotte
NC, 28202-1517
USA
www.honeywell.com

Honeywell Cyber Proactive Defense | 12/25

THE FUTURE IS WHAT WE MAKE IT

Honeywell