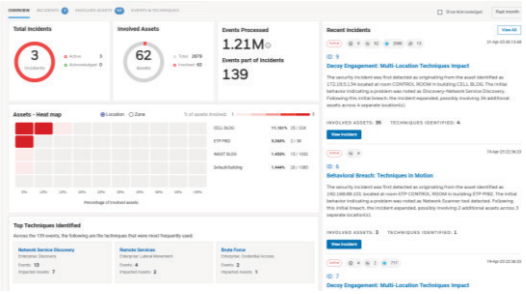
HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD

HONEYWELL CYBER PROACTIVE DEFENSE

PRODUCT INFORMATION NOTE

Honeywell Cyber Proactive Defense is a cutting-edge cybersecurity solution engineered to safeguard industrial operational technology (OT) environments against the growing landscape of sophisticated and AI-enabled cyber threats. This advanced platform proactively assists organizations to identify, prioritize, and mitigate potential risks before they escalate into full-scale attacks. By integrating AI - driven behavioral analytics and leveraging the Honeywell Cyber Threat Intelligence platform - powered by Google Threat Intelligence (GTI) - the solution delivers enriched, near real-time insights and advanced analytics tailored to the unique demands of OT systems.

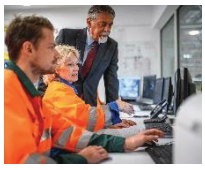


A key feature of Cyber Proactive Defense is its ability to establish a comprehensive baseline of normal system behavior, enabling the early detection of anomalies that may indicate malicious activity. The platform also incorporates deception technology, deploying strategically placed OT decoys (honeypots) within the network to mislead and divert attackers away from critical assets. Additionally, AI-powered incident response playbooks provide structured, intelligent guidance for responding to threats, minimizing downtime and ensuring rapid recovery.

By embedding deep process knowledge into cyber analysis and aligning with industrial workflows, Honeywell Cyber Proactive Defense 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 designed to protect operational technology (OT) environments by anticipating, identifying, and neutralizing cyber threats before they can disrupt operations. Unlike conventional reactive security models, Honeywell's proactive defense strategy integrates continuous monitoring, enriched threat intelligence, and AI-driven analytics to better detect anomalies and vulnerabilities early in the cyber kill chain.



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 Google Threat Intelligence (GTI) - the solution delivers near real-time insights and advanced analytics tailored to the unique dynamics of industrial environments.

Additionally, Honeywell Cyber Proactive Defense embeds deep process knowledge into cyber analysis and deploys deception technologies such as OT honeypots to mislead attackers and protect critical assets. AI-powered incident response playbooks further enhance resilience by enabling swift, structured responses to emerging threats.
Through this comprehensive and preemptive 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.

PROACTIVE DEFENSE GENERAL USE CASE

HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD

HONEYWELL CYBER PROACTIVE DEFENSE

An industrial organization operating a complex and aging operational technology (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, prioritize, 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 behavior, establishing a dynamic baseline to detect anomalies indicative of malicious activity. This early detection capability enabled the organization to identify threats before they could escalate into incidents.
The implementation also included deception technologies, such as strategically placed OT honeypots, which diverted attackers away from high-value assets and provided valuable intelligence on adversarial tactics. Furthermore, AI-powered incident response playbooks automated threat mitigation processes, significantly reducing response times and ensuring consistent, effective 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.

HONEYWELL FORGE Cybersecurity+

OTD BİLİŞİM GLOBAL VAD

HONEYWELL CYBER PROACTIVE DEFENSE

FEATURES AND BENEFITS

DECEPTION CAPABILITY

- Deploys decoys and traps within the OT network to divert attackers away from critical assets.
- Detects threats early by monitoring interactions with deceptive elements, providing early warning signals.
- Gathers threat intelligence on attacker behavior and tactics without risking exposure of systems.

ARTIFICIAL INTELLIGENCE & ML

- Identifies anomalies in network and system behavior using advanced machine learning models.
- Predicts emerging threats by analyzing patterns and correlating data across multiple sources.
- Adapts defenses in real time, continuously learning from new data to improve detection accuracy.

AI-POWERED PLAYBOOKS

- Automates incident response through predefined, customizable workflows.
- Reduces response time from hours to minutes, enabling rapid containment and mitigation.
- Ensures consistent actions across incidents, minimizing human error and improving efficiency.