Honeywell Cyber Proactive Defense - Customer FAQs

1. What is Cyber Proactive Defense?

Honeywell Cyber Proactive Defense is a software solution that helps customers defend against cyber-attacks by proactively identifying early signs of potential cyber threats in their industrial environment. It is designed to enable customers by forecasting threats before an attack occurs and then prompting them to take appropriate action to strengthen cyber defenses through playbooks provided. With the support of cyber deception technology and AI behavioral-based analytics capabilities this software is designed to help customers uncover behavioral deviations from normal operations.

2. What can Cyber Proactive Defense do for customers?

Cyber Proactive Defense helps customers reduce their cybersecurity risk, including the risk of a cyber-attack that can disrupt operations and cost $Millions in damage and lost downtime, as well as impact employee safety. The solution addresses macro trends of rising cybersecurity threats and impact, and the shortage of Operational Technology (OT) cybersecurity skills.

Value Proposition:

- Exposes cyber risk
- Prioritizes and groups alerts to increase analyst effectiveness
- Embeds process knowledge to cyber analysis
- Correlates alerts across solutions
- Continuous learnings through the capture of human action on remediations
- Improves autonomy- System recommendations/action
- De-links constraints of personal, location and cyber skills

Outcomes Supported:

- No more alerts from missed unanalyzed data
- Significant reduction in preventable cyber /cyber physical incidents
- More true positive identification and fewer false positives
- No incident without a recommendation

3. How is Cyber Proactive Defense different from competitive offerings?

Cyber Proactive Defense is designed to:
1) leverage AI behavior analytics
2) proactively identify early signs of potential cyber threats
3) enable customers to forecast and mitigate risks before an attack occurs

Key Features:

- **Proactive Threat Identification**: Detects anomalies in OT cyber behavior by establishing a comprehensive baseline of system operations.
- **Forecasting and Mitigation**: Provides actionable insights and playbooks to strengthen OT cyber defenses.

- **Cutting-edge Technologies**: Utilizes deception technology, deploying OT decoys within the network to divert attackers from valuable assets.

Cyber Proactive Defense empowers customers to take preemptive actions, ensuring robust protection against cyber-attacks.

Cyber Proactive Defense offers several unique capabilities:

- Embeds process knowledge to cyber analysis
- Cyber Proactive Defense uses curated threat intelligence to offer better accuracy and preemptive detection
- Deception technology to divert cyber-attacks to critical assets
- AI/LLM with query capability to provide accurate playbook tailored to the unique needs of industrial operations, all backed by specialized Honeywell Cyber Threat Intelligence
- Utilizes anomaly-based and behavior-based detection methods to detect malicious activity
- Enhances zone-based navigation for network segmentation analysis

4. What industry problems does Cyber Proactive Defense help solve?

- Challenge of minimizing OT cyber risk and defending against constantly changing threat landscape
- Challenge of meeting the OT cyber skills gap
- Challenge of driving cyber resiliency of business continuity in the face of growing cyber threats