ENTERPRISE-LEVEL APPROACH TO CYBERSECURITY FOR OPERATIONAL TECHNOLOGY (OT) ENVIRONMENT

A comprehensive strategy and approach to managing OT cyber risk

Honeywell

INTRODUCTION

Operational technology (OT) environments are increasingly vulnerable to cyber threats as global digitalization trends continue to expand.

A global survey in 2024 revealed that the average cost of an OT breach exceeds $5.6 million[1], highlighting the severe financial and reputational impacts of these incidents. OT environments, which include industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and building OT assets (e.g., HVAC systems, access control, video networks, etc.), are critical to the functioning of essential services such as electricity, water, transportation and manufacturing. These environments are traditionally designed for reliability and availability, often lacking the robust cybersecurity measures found in information technology (IT) systems. If these systems are compromised, it can lead to forced shutdowns and lost access to critical infrastructure and public resources. As a result, they have become attractive targets for cybercriminals and nation-state actors. Analysts predict that increasing regulations will push most companies to OT cybersecurity maturity by 2030[2], but many organizations must move into high gear or risk falling behind. A significant majority of stakeholders acknowledge OT cybersecurity as a high or top priority but may lack the internal infrastructure to properly safeguard OT environments.

As more responsibility for OT cybersecurity falls upon the CISO, many are asking pertinent questions, such as:

- What are our biggest OT cybersecurity risks today?
- What's our plan to enable operational availability, reliability and safety?
- How confident are we in our ability to assess cyber risk at a site and enterprise level?
- Do we have the right controls and capabilities to manage an attack?
- How prepared are we to address attack surface expansion driven by digitalization and ever-increasing numbers of connected assets?
- How do we demonstrate continuous compliance with evolving regulations?
- What metrics do we use to measure the effectiveness of our OT cybersecurity program?

Considering the critical nature of these challenges and the quickly evolving role of the cybersecurity professional and CISO in OT cybersecurity, this paper suggests best practices and recommendations to build mature and comprehensive OT cybersecurity security operations at a site and enterprise level.

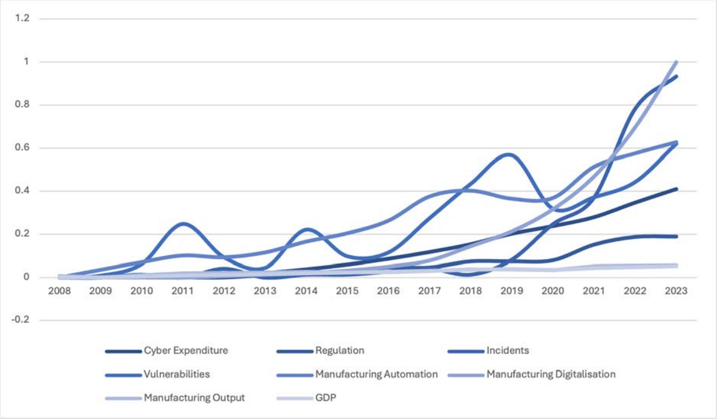
CYBERSECURITY CHALLENGES AND COMPLEXITIES: A STAKEHOLDER PERSPECTIVE

PERSPECTIVE 1: CYBERSECURITY PROFESSIONALS

ACCELERATED DIGITALIZATION

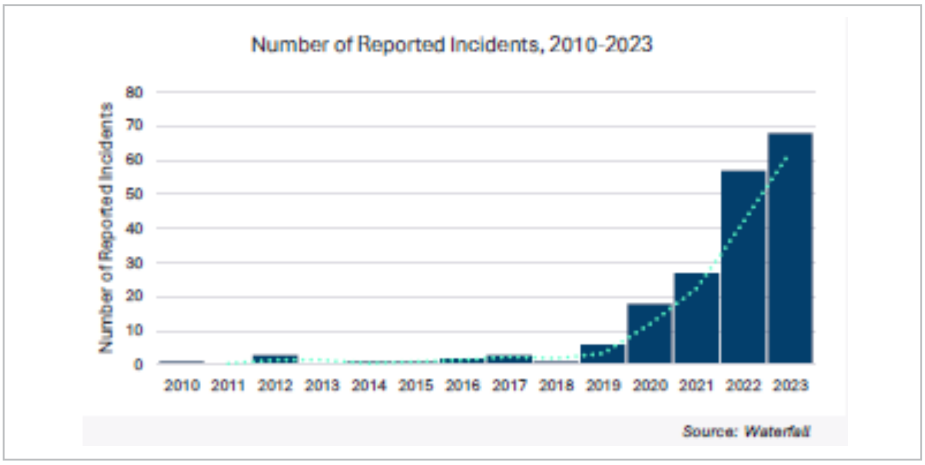
The accelerated digitalization of industrial processes – the adoption of 5G, robotics, artificial intelligence (AI), cloud, increased remote access and others – is expected to advance as asset owners seek to increase manufacturing efficiencies, reduce energy consumption, and gain competitive advantages[2].

This will enable greater volumes of industrial data to be processed at the edge and sent to the cloud along with digital twins, machine learning and cloud analytics becoming more widely used to connect OT environments to IT systems. The use of generative AI in the manufacturing sector will also likely be widespread by 2030[2]. This increased digitalization will amplify the number of access points for cyber attacks potentially making it easier for threat actors to infiltrate under-protected OT networks.



INCREASED SOPHISTICATION AND FREQUENCY OF ATTACKS

The sophistication and frequency of attacks targeting OT-specific protocols, such as Triton and Industroyer, continues to rise, posing potential substantial risks to critical infrastructure. The number of publicly reported incidents related to OT has grown significantly in recent years. However, not all 'OT' incidents are OT attacks. Attacks on IT can have an operational impact which requires asset owners to have a good understanding of their assets, what normal looks like, and have incident response plans in place. Organizations that don't have good OT awareness may shut down operations even though the incident is IT related and not impacting OT.



Source: Waterfall

These incidents and attacks present substantial risks from both cybercriminals and nation-state actors employing advanced methods to exploit vulnerabilities in OT systems. Currently, the three most concerning types of attacks against OT are malware, ransomware and insider attacks. The threat landscape has evolved significantly from bespoke OT malware like Stuxnet aimed at specific adversaries to widely used IT-borne ransomware such as Lockbit that indiscriminately targets industrial organizations. Recently , extortion and organized crime surpassed state-sponsored cyber activities as the primary threats to industrial operators with high payouts unfortunately making attacks lucrative.[2]

INCREASINGLY COMPLEX REGULATORY LANDSCAPE

Many organizations are struggling to navigate complex regulatory frameworks, standards and guidelines which require continuous monitoring and reporting to maintain compliance and mitigate risks. This means organizations – and their respective leaderships – are under pressure to not only align with regulatory frameworks but also effectively comply with requirements across all levels of an enterprise. With these regulations, organizations must demonstrate compliant operations and products, which extends to the security of supply chains. Critically, these regulations are becoming increasingly enforceable with 18 of the most significant regulations fully enforceable by the third quarter of 2025. This may present challenges especially for asset owners who are at a nascent stage of their cybersecurity journey.

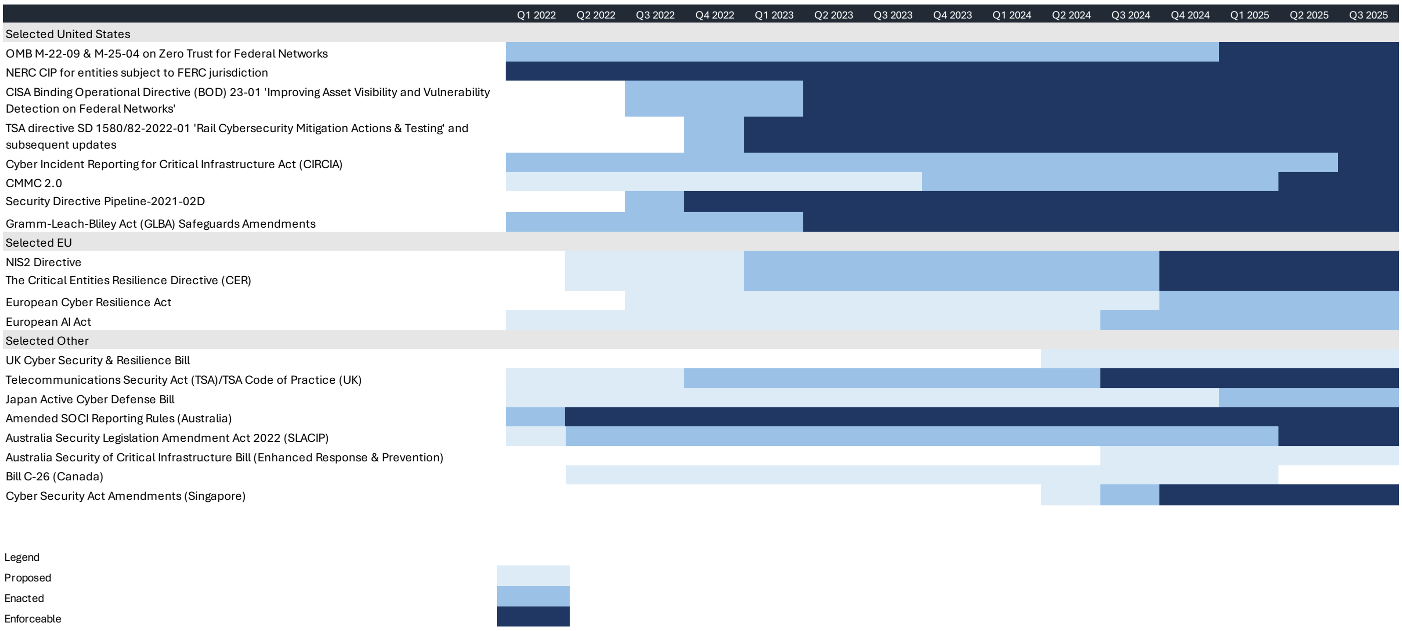
Examples of regulatory frameworks, standards and guidelines include:

- ISA/IEC 62443
- NIST CSF
- NERC CIP
- Saudi Arabia's OTCC
- TSA SD-2E for pipeline and rail
- European Union AI Act: takes effect in 2025 and will provide a comprehensive framework for regulating AI, assigning risk levels to AI systems, and more
- NIS2: NIS is also expanding its coverage from about 20% to more than 35% of the industrial base in Europe, with more organizations being drawn into regulatory frameworks
- European Cyber Resilience Act
- Security of Critical Infrastructure Act, 2018

Westlands Advisory states, "Strengthening regulation is raising the cybersecurity baseline across industries, accelerating investment in people, processes and technology to improve visibility, accountability, and resilience." These challenges affect how organizations manage their people, processes and technologies. Asset owners will need to increase investment in resilience which will include staff awareness and training, incident response and a greater focus on supply chain partners to meet these regulatory demands.

Collaboration among diverse teams, such as site operations, audit, compliance and OT cybersecurity functions, is critical. Many organizations face the dual challenge of adapting their compliance strategies to rapidly changing regulations while being in the early stages of their cybersecurity journeys, often relying on cumbersome and ineffective manual processes for compliance tracking. The key lies in formulating comprehensive strategies that navigate regulatory complexities and enhance overall cybersecurity resilience[2].

Whilst Regulation has been a contributing factor to increasing investment in cybersecurity, low enforcement has led to low adoption. New regulation aims to address previous weaknesses



LACK OF SKILLED LABOR WITH DEEP OT DOMAIN EXPERTISE

With the shortage of skilled experts with OT domain experience, resource-related challenges is often one of the largest obstacles to reducing the attack surface and creating an effective response to cyber threats. Often, organizations only have leadership in place without adequate support staff, making it difficult to effectively manage and respond to cybersecurity threats. Limited availability of skilled cybersecurity professionals can exacerbate the difficulty in implementing robust security measures, potentially leaving OT environments vulnerable to attacks, thus creating delayed response times.

PERSPECTIVE 2: CISOS

An appropriately scaled and secure OT cybersecurity environment cannot be set up quickly, especially at an enterprise level. As the OT threat landscape evolves, many CISOs may be asking themselves some hard questions:

- Where to start.
- How to stay ahead of threats, malicious actors and cyber criminals.
- How to gain executive support, investment and alignment with business processes.
- How to track regulatory changes across regions and sectors.
- How to automate tracking, reporting and stay continuously compliant.

These are all valid questions and concerns and with the ever-changing landscape, likely can't be answered just once. These questions need to be visited not just when organizations start their cybersecurity journey but also periodically as processes and protocols are reviewed and updated to stay ahead of threats and compliant with regulations and guidelines.

ENTERPRISE VISIBILITY (ASSETS & DATA)

Lack of asset visibility at the enterprise level often complicates the ability to accurately assess and mitigate cybersecurity risks. According to Honeywell internal research, approximately one-third of OT assets remain unidentified due to reliance on outdated discovery methods like paper and spreadsheets. This situation is often exacerbated by the complexity of managing assets from multiple vendors that require specialized domain expertise to accurately identify and integrate these assets into monitoring systems. Additionally, unharmonized assets and/or data can hinder the ability to pinpoint threats in a timely manner and the coordination between enterprise and sites, potentially putting organizations at risk.

AI – FRIEND OR FOE

Artificial Intelligence (AI) may present increased opportunities for malicious actors. Threat actors may more effectively identify targets, skillfully manipulate users and systems, and automate sophisticated and targeted attacks or use AI to develop new malware. Technologies such as machine translation, speech synthesis and generative AI can reduce the need for extensive customization and manual oversight in executing successful cyberattacks.

It's important to note that these same technologies can also provide an effective line of defense. Currently, numerous IT cybersecurity solutions use machine learning, heuristics and AI in various capacities including automatic patching, malware classification, threat detection and incident response. Part of the challenge with this accelerated digitalization is determining how best to extend these practices to OT cybersecurity.

OT – IT COLLABORATION & CONVERGENCE

The much-required collaboration between IT and OT causes additional complications as the traditional roles of IT focusing on enterprise-level decisions and OT focusing more on operations converge around cybersecurity. Though organizations agree that some level of centralization must occur, many are unsure of the best approach.

KEY FOCUS	**IT** - Information security and data protection **OT** - Operational safety, physical process integrity, and preventing catastrophic disruption.
AVAILABILITY	**IT** - Downtime is disruptive, but rarely causes immediate physical harm **OT** -Operational continuity is paramount; system faitures can threaten lives and critical processes
THREATS	**IT** - Data theft, ransomware, malware **OT** -Advanced targeted attacks, disruptions intended to sabotage operations or equipment.

A fragmented approach to cybersecurity is ineffective for both IT and OT regardless of the quality of solutions implemented, potentially leading to the ongoing OT asset vulnerability. Despite distinct needs in IT and OT cybersecurity, a coordinated decision-making process is essential. This requires communication between the two teams: IT must focus on appropriate countermeasures to mitigate threats while OT must address the specific limitations and constraints of OT assets.

The slow convergence can largely be attributed to the challenges faced by the two teams in establishing an effective dialogue that fosters successful cooperation. The relationship between OT and IT in cybersecurity efforts often exhibits a significant degree of separation or friction. This suggests that interactions between the two areas are infrequent, and when they do occur, there is often a lack of alignment. Such misalignment can lead to challenges in decision-making processes.

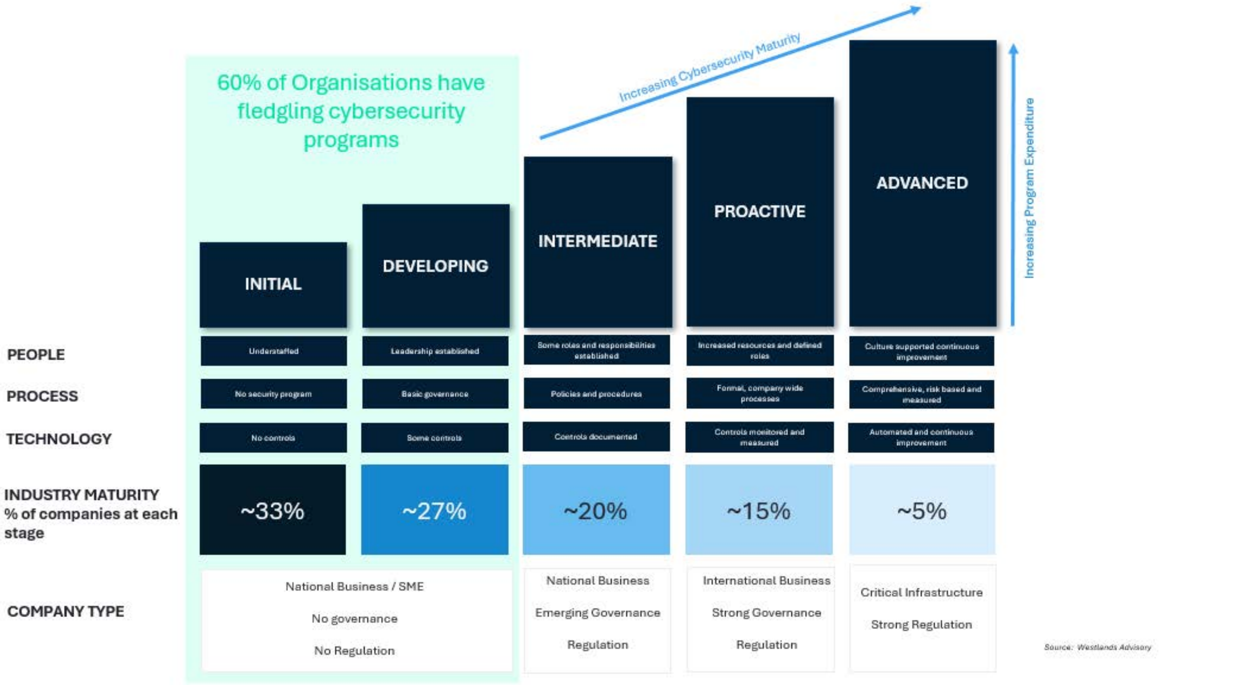
SO WHERE DOES THIS LEAVE THE INDUSTRY?

When assessed across a gradual maturity scale, most organizations currently fall in the “Initial” or “Developing” categories indicating a lack of advanced protective measures and comprehensive security strategies[2]. They struggle with:

- Understaffing, often only having leadership in place
- Achieving more than a basic understanding of governance requirements
- Documenting, monitoring and measuring controls

Many organizations remain reactive, hindered by disconnected systems and limited workforce expertise. This reactivity leads to increased risks and costs as organizations often fail to identify compliance violations and operational failures until they occur. Disconnected systems can create inefficiencies in data flow, reduce visibility and reporting capabilities hindering collaboration across departments – IT and OT. Addressing these gaps is critical for organizations to achieve continuous compliance and robust risk management.

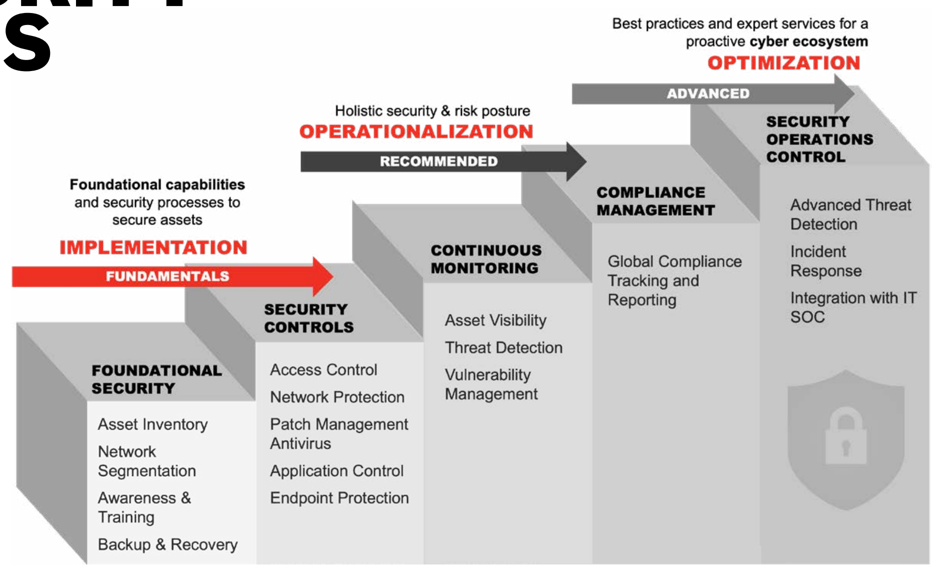
Despite significant change cybersecurity maturity remains low, albeit moving in the right direction.


60% of Organisations have fledgling cybersecurity programs
Increasing Cybersecurity Maturity
Increasing Program Expenditure

	INITIAL	DEVELOPING	INTERMEDIATE	PROACTIVE	ADVANCED
PEOPLE	Understaffed	Leadership established	Some roles and responsibilities established	Increased resources and defined roles	Culture supported continuous improvement
PROCESS	No security program	Basic governance	Policies and procedures	Formal, company wide processes	Comprehensive, risk based and measured
TECHNOLOGY	No controls	Some controls	Controls documented	Controls monitored and measured	Automated and continuous improvement
INDUSTRY MATURITY % of companies at each stage	~33%	~27%	~20%	~15%	~5%
COMPANY TYPE	National Business / SME No governance No Regulation		National Business Emerging Governance Regulation	International Business Strong Governance Regulation	Critical Infrastructure Strong Regulation

Source: Westlands Advisory

THE JOURNEY TO A MATURE OT CYBERSECURITY OPERATIONS

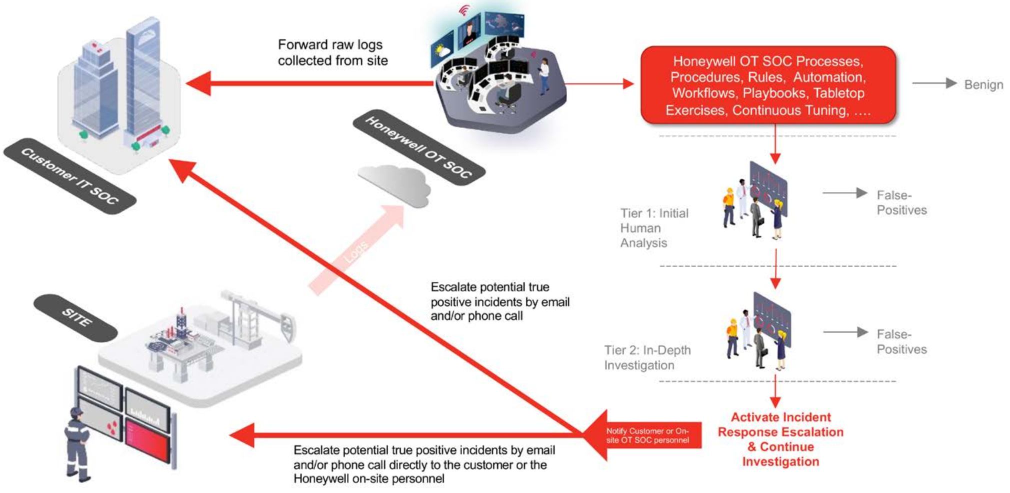


The increasing sophistication of attacks on OT environments requires a proactive and comprehensive approach to cybersecurity. Both cybercriminals and nation-state actors are employing sophisticated methods to exploit vulnerabilities in OT systems making it imperative to implement advanced detection and mitigation strategies. As the threat landscape evolves, organizations must develop robust threat intelligence programs, enhance detection systems and adopt network segmentation practices to safeguard their OT environments and be compliant with increasing global regulations. The development and implementation of a unified compliance framework that can scale from site to the enterprise, as well as automating compliance processes and fostering cross-functional collaboration are crucial steps towards navigating regulatory complexities and enhancing overall cybersecurity resilience.

Enterprise OT cybersecurity and compliance is best viewed as a maturity journey where organizations progressively enhance their security posture to defend against emerging threats while building out compliance capabilities to continuously comply with evolving global regulations. This journey starts with a comprehensive and foundational understanding of its current state, which will outline a structured pathway to enhance cybersecurity maturity through foundational security measures. This is followed by the implementation of robust security controls, continuous monitoring, risk-based compliance management and the automation of security operations.

It is also a sound practice to start the journey with the destination in mind: a highly automated **OT Security Operations Center (SOC)**. Thinking in the context of an OT SOC from day 1, helps enable the capability to mature with respect to people, process and tools that are required to meet cybersecurity objectives at each stage of the journey without investing in non-strategic areas. This approach also provides flexibility in adopting various SOC models to meet immediate needs, including the likes of the OT SOC in a box from Honeywell, which provides a quick, all-in-one solution (person, process and technology) for immediate deployment. A regional- or site-level OT SOC model allows for localized monitoring and response, catering to specific geographical and industry risks, while an Enterprise OT SOC provides comprehensive oversight of OT environments under a unified compliance framework that can scale from site to the enterprise while enabling global regulatory compliance.

HONEYWELL OT SOC CAN COMPLEMENT AN IT SOC


Forward raw logs collected from site
Customer IT SOC
Honeywell OT SOC
Honeywell OT SOC Processes, Procedures, Rules, Automation, Workflows, Playbooks, Tabletop Exercises, Continuous Tuning, ….
Benign
Tier 1: Initial Human Analysis
False-Positives
Logs
Escalate potential true positive incidents by email and/or phone call
Tier 2: In-Depth Investigation
False-Positives
SITE
Notify Customer or On-site OT SOC personnel
Activate Incident Response Escalation & Continue Investigation
Escalate potential true positive incidents by email and/or phone call directly to the customer or the Honeywell on-site personnel

IMPLEMENTING THE FOUNDATION

STAGE 1: FOUNDATIONAL SECURITY

At the foundational stage, organizations need to focus on basic protective measures to mitigate immediate risks. This includes asset discovery and inventory tools to gain visibility into OT assets, network segmentation to isolate OT systems from IT environments, and the establishment of robust L3.5 DMZs to control communication between IT and OT networks. Basic incident response protocols should be established and OT personnel trained to recognize common cyber risks.

STAGE 2: SECURITY CONTROLS

In this stage, organizations should implement stronger security policies, conduct regular security assessments, and provide continuous training in security awareness for employees. Regular patching and updates are essential to mitigate known vulnerabilities and comprehensive incident response plans can enable swift and effective reactions to security breaches. These practices help form a resilient framework that can significantly enhance an organization's ability to defend against cyber threats in OT domains.

OPERATIONALIZATION

STAGE 3: CONTINUOUS MONITORING

As the threat landscape evolves, organizations must shift from reactive to proactive security measures. Continuous monitoring is essential for detecting potential cyber threats in real time, especially as IoT devices increase the number of entry points into OT systems. Advanced analytics, including machine learning and behavior analysis, are deployed to detect potential anomalies and suspicious activities. Security operations centers (SOCs) specializing in OT environments can provide centralized oversight, enabling rapid detection, investigation and response to cyber incidents.organization's ability to defend against cyber threats in OT domains.

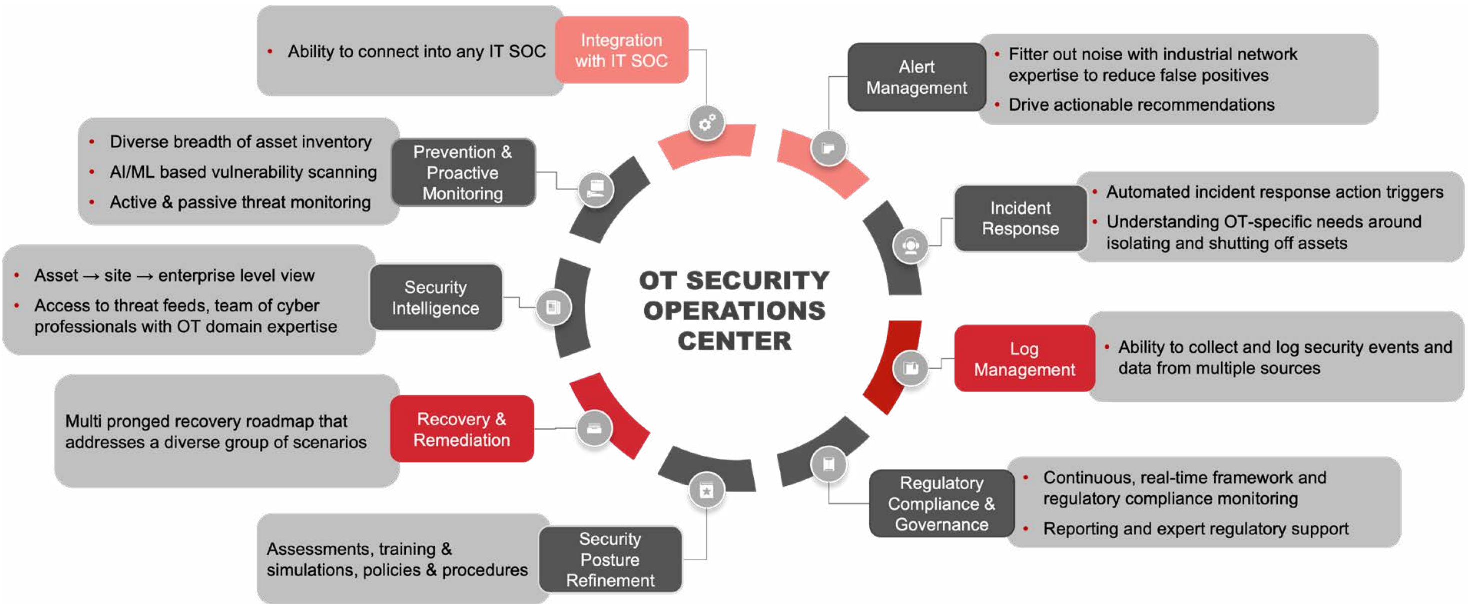
STAGE 4: RISK-BASED MONITORING, ASSESSMENT AND COMPLIANCE MANAGEMENT

Organizations integrate compliance management into daily security operations, maintaining regulatory adherence without diverting focus from operational priorities. Risk-based compliance management automates regulatory alignment and risk management across OT environments. AI-driven analytics can continuously monitor assets, processes and policies to support real-time compliance with industry-specific regulations. This strategy shifts compliance from a static activity to a dynamic, business-aligned endeavor that enhances overall cybersecurity resilience.

OPTIMIZATION

STAGE 5: AUTOMATED SECURITY OPERATIONS

In the final stage, organizations should fully integrate advanced technologies to automate and streamline cybersecurity operations. The establishment of Operational Technology Security Operations Centers (OT SOCs) can provide real-time monitoring, detection and response to cyber incidents. Integrated IT/OT SOCs provide centralized oversight, enabling organizations to rapidly detect, investigate and respond to cyber incidents. Real-time visibility and rapid response capabilities can help minimize the impact of security breaches and operational disruptions.


OT SECURITY OPERATIONS CENTER
Integration with IT SOC
• Ability to connect into any IT SOC
Alert Management
• Fitter out noise with industrial network expertise to reduce false positives
• Drive actionable recommendations
Prevention & Proactive Monitoring
• Diverse breadth of asset inventory
• AI/ML based vulnerability scanning
• Active & passive threat monitoring
Incident Response
• Automated incident response action triggers
• Understanding OT-specific needs around isolating and shutting off assets
Security Intelligence
• Asset → site → enterprise level view
• Access to threat feeds, team of cyber professionals with OT domain expertise
Log Management
• Ability to collect and log security events and data from multiple sources
Recovery & Remediation
Multi pronged recovery roadmap that addresses a diverse group of scenarios
Regulatory Compliance & Governance
• Continuous, real-time framework and regulatory compliance monitoring
• Reporting and expert regulatory support
Security Posture Refinement
Assessments, training & simulations, policies & procedures

NAVIGATING THE COMPLEXITIES IN OPERATIONALIZING THE SOC

ENTERPRISE ASSET VISIBILITY AND DATA LEVERAGE

Challenges with OT data often arise due to proprietary protocols and data formats, complicating integration for analysis. Harmonizing this data and correlating it with information received from the IT network is crucial for security analysts to gain a comprehensive view of OT network activity, improve the signal-to-noise ratio and reduce the time it takes to respond. For instance, solutions like Honeywell CDA and FTE, Emerson DeltaV or ABB TotalFlow have proprietary protocols that require specific knowledge for proper deep packet inspection, without which analysis becomes guesswork, thus increasing false positives and straining the SOC.

For an OT SOC to be effective, it is important to harmonize OT and IT data at the Security Information and Event Management (SIEM) level using several methods:

- **Data normalization:** Transforming data into a consistent format. An OT asset alerting a deviation from operational policy needs to be normalized into the same type of data that an analyst is accustomed to seeing from IT assets.
- **Data correlation:** Linking related information from various OT and IT systems. Correlation between events occurring on the OT side of the network needs to be related to the upstream IT network to provide a comprehensive view.
- **Data aggregation**: Combining data from multiple sources for easier analysis in a SIEM with proprietary correlation and detection logic, as well as security orchestration, automation and response (SOAR) automation tailored to the OT playbook response and a hand off with the IT SOC.
- **Data enrichment:** Adding context through external sources like asset inventories and threat intelligence feeds, especially those proprietary to a specific vendor, is key to enabling a proper and timely response. Metadata made available through an extensive threat feed enhances this process by improving data searchability, quality and governance to help reduce investigation and response time.

Using OT security solutions like Honeywell's Cyber Insights can simplify data collection, integration and analysis with tailored filtering, detection and alerting logic. This is possible because of a mature protocol detection library, alerting logic and a combination of advanced active and passive asset monitoring coverage and capabilities. Holistically, these tactics result in better risk visibility for the CISO, potentially leading to fewer breaches and faster recovery times.

COMBATING ADVANCED THREATS – AI IS A FRIEND

To combat advanced threats, organizations must implement sophisticated detection and response strategies that leverage the combination of harmonized first-party OT data, advanced threat intelligence and AI embedded tools that can significantly enhance efficiency and effectiveness of OT cybersecurity operations. Key areas of opportunity include:

- Real-Time Threat Intelligence: Using threat intelligence tools to stay ahead of emerging threats and adapt security measures
- AI-Driven Defense: Leveraging AI-driven predictive capabilities to simulate potential system failures and prepare for a range of cyber and operational disruptions
- AI-Driven Monitoring/Analytics: Using AI to analyze vast amounts of data, identify patterns and detect anomalies to help improve threat detection and response
- Automated Threat Response: Implementing AI to automate threat response actions to help reduce the burden on SOC teams and allowing them to focus on high-priority threats
- Predictive Capabilities: Leveraging AI to predict potential threats and system failures thus enabling proactive measures to mitigate risks

AREAS FOR AI LEVERAGE

MONITORING	ASSESSMENT	REMEDIATION	COMPLIANCE
• Anomaly detection • Behavior detection • Real-time threat detection • Predictive threat intelligence • Early threat detection	• Risk models • Reduce false positives • Alert correlation • Vulnerability assessment • Threat hunting	• Automated incident response • Guided play books • SOC augmentation • Improved response times • Detailed forensics of threat vectors for faster remediation	• Automate compliance tracking with industry frameworks: NIST CSF, IEC 62443 • Generate real-time compliance reports to simplify audits

RISK-BASED APPROACH TO OT CYBERSECURITY

A risk-based approach to cybersecurity involves identifying, assessing and prioritizing potential cyber threats based on their likelihood of occurrence and potential impact. This allows organizations to allocate resources more effectively by focusing on the areas with the highest risk rather than implementing blanket security measures across all systems. This requires extensive leverage of data and includes:

- **Comprehensive Coverage:** Identifying threat actor profiles and behavior detection is possible by understanding potential attack vectors from various cybersecurity site solutions, process alarms, threat intelligence feeds, indicators of compromise, Tactics, Techniques, and Procedures (TTPs), and enhancing the enterprise-level view of cyber risk. Understanding high volume of threats, vulnerabilities and monitored assets with contextualized process data leveraging algorithms and embedded process knowledge is essential for an accurate risk assessment.
- **Risk-Based Assessment and Prioritization:** Employing a holistic approach to assess vulnerabilities and threats and informing a strategic response to potential risks. This combines the likelihood of a threat occurring with the potential impact on the organization to determine the overall risk level and ranking identified risks based on their severity to allow for focused mitigation strategies.
- **Operational Impact Considerations:** Identifying true positives to significantly reduce preventable cyber incidents can be achieved by harmonizing assets, correlating alerts across solutions, and learning continuously by capturing human actions on remediations. This can help facilitate rapid response to cyber threats and reduce false positives. OT playbooks can serve two primary purposes: provide real-time guidance for recommended remediation actions or offer information that supports further research and investigation by forensic analysts or OT security analysts.

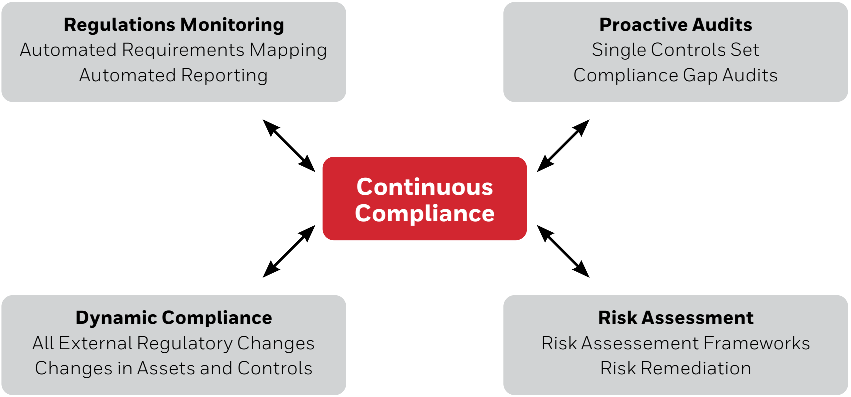
Understand, Detect, and prevent cybersecurity threats (Example: Industroyer Kill Chain Attack)

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

CONTINUOUS COMPLIANCE

Organizations must view compliance not as one-time tasks but as an ongoing, dynamic process. Continuous compliance can revolutionize this concept by automating regulatory alignment and risk management across operational technology environments. Key practices include:

- **Regulations Monitoring:** Automate regulatory mapping by leveraging AI techniques and aligning them with organizational controls and processes.
- **Proactive Audits:** Conduct proactive audits to identify and address compliance gaps for timely closure. Confirm ongoing adherence to regulatory requirements and comprehensive traceability.
- **Dynamic Compliance Processes:** Maintain regulatory adherence but also enhance security by addressing emerging threats and vulnerabilities promptly. Remain agile and resilient in the face of rapidly changing compliance landscapes.


Regulations Monitoring
Automated Requirements Mapping
Automated Reporting

Proactive Audits
Single Controls Set
Compliance Gap Audits

Continuous Compliance

Dynamic Compliance
All External Regulatory Changes
Changes in Assets and Controls

Risk Assessment
Risk Assessement Frameworks
Risk Remediation

A robust solution for continuous compliance requires a centralized regulatory repository, automation and advanced compliance monitoring. The repository organizes regulations (e.g., NIST CSF, ISA/IEC 62443, CIS) and maps them to technical controls that are certified and audited. Advanced analytics, including ML-based anomaly detection, predict and address compliance risks, while real-time dashboards and audit trails can streamline reporting. Designed specifically for OT environments, domain-specific controls, such as secure configurations for PLCs and SCADA systems, are essential components of and effective compliance solution. A crucial factor in maintaining continuous compliance is the ability to prioritize risk remediation efforts. Centralized and dynamic risk assessments based on established frameworks such as ISA/IEC 62443 and NIST Risk Management is a key input to this prioritization of compliance efforts.

SITE VS. ENTERPRISE

An important consideration when devising a OT cybersecurity strategy is to clearly define site- and enterprise-level capabilities and interactions. This is necessary due to the differences in their scope and priorities.

As regulations and cybersecurity requirements become more complex, centralizing OT cybersecurity operations to foster seamless collaboration – between site-level and enterprise-level and between OT and IT – will be crucial. Leveraging technologies like cloud computing and AI will significantly enhance enterprise-level aggregation and visibility. It's important to make sure the underlying technical and data architectures are robust enough to not only streamline operations but also prevent challenges down the line can help create a future-ready foundation for optimizing the interaction and flow between various levels of the organization.

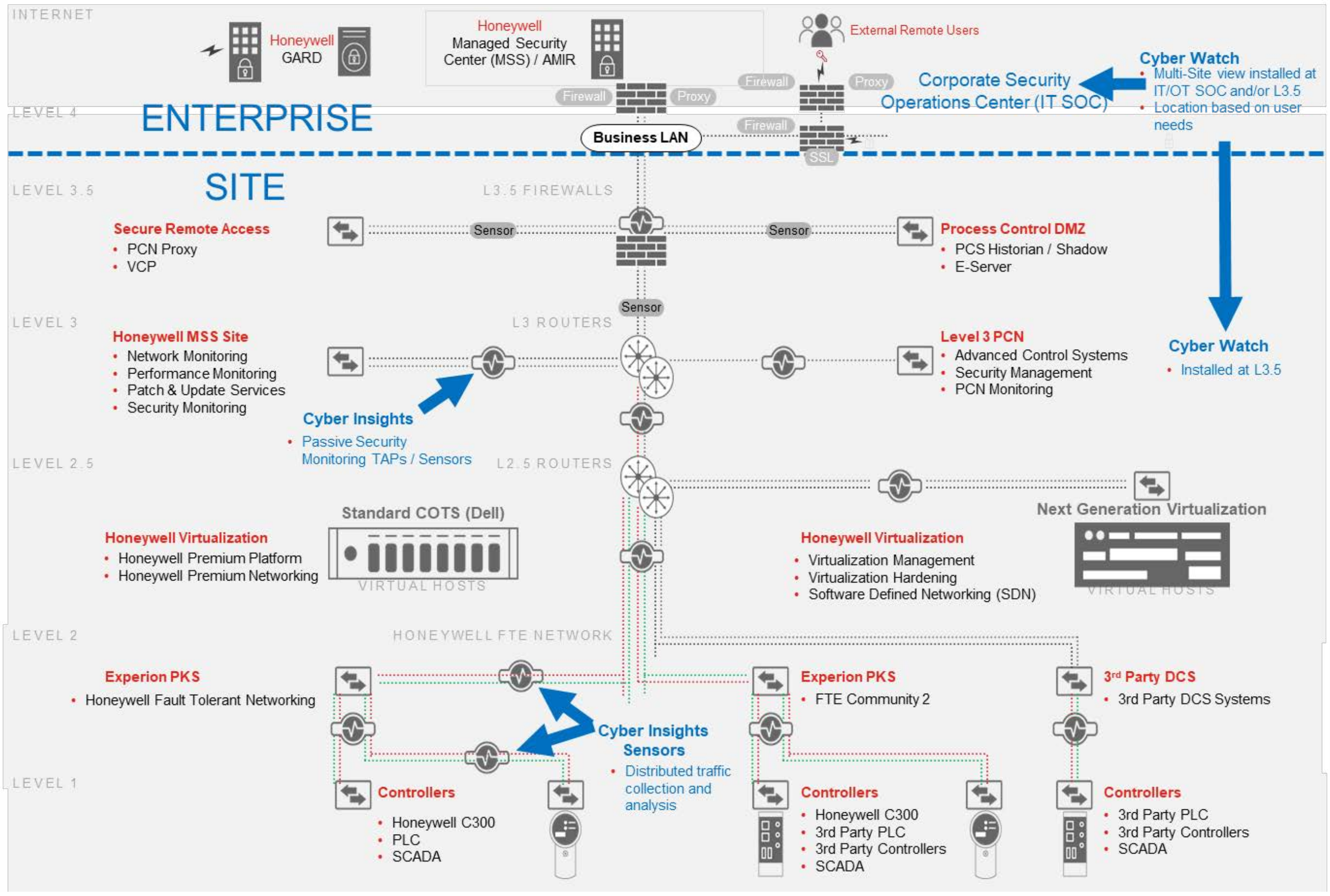
SITE-LEVEL FOCUS AREAS	ENTERPRISE-LEVEL FOCUS AREAS
Protecting local OT systems supporting the safety, reliability and availability of physical assets, people and processes	Deploying unified, risk-based controls and strategies for OT Cybersecurity in alignment and convergence with IT and across multiple sites and geographies to protect critical infrastructure
Managing network segmentation, access control and physical security to prevent disruption to operations	Managing visibility into all OT assets including centralized monitoring, cross-site risk assessments and mitigation
Addressing asset visibility, legacy systems and operational constraints with a focus on immediate risk mitigation (e.g. patching).	Maintaining regulatory compliance, business continuity and data security.

ENABLING IT-OT CONVERGENCE AND COLLABORATION

SOCs with real-time data analytics tools to continuously monitor OT networks can help facilitate immediate cyber threat detection and response to incidents thereby minimizing potential damage from cyber threats. OT SOCs can provide swift incident management even in the face of unique challenges such as legacy system concerns and the need for real-time operational responses. These specialized SOCs are designed to address the needs of OT environments while fostering collaboration between IT and OT security teams. Key steps to foster this collaboration include:

- **Integrated SOCs:** Establishing integrated SOCs that encompass both IT and OT environments for cohesive security management.
- **Cross-Training Teams:** Providing cross-training opportunities for IT and OT personnel to understand each other's domains with common vocabulary, normalized data models and harmonized assets.
- **Unified Security Policies:** Developing unified security policies that address the unique needs of both IT and OT environments to provide comprehensive protection.
- **Data and Architecture:** Organizations must harmonize OT and IT data through data normalization, correlation and enrichment within a structured data architecture to help provide a contextualized and comprehensive dashboard.
- **AI Leverage:** Starting with anomaly detection and predictive capabilities, organizations can showcase immediate benefits like improved efficiency and reduced downtime. Continuous operator involvement in training and validating these models fosters confidence while integrating AI tools as decision-support systems rather than automated decision-makers helps enable safety and control.

SOC ARCHITECTURE



OT SOC + IT SOC
24/7 OT security monitoring integrated into enterprise IT SOC with AI LLM playbooks

(L3-L5) Cyber Watch
Keep watch over the cybersecurity posture of multiple sites.

(L2-L3) Cyber Insights
Know your OT cybersecurity posture at a single site with industrial grade deep packet inspection and full visibility to assets, network traffic and events

(Optional L2) Cyber Insights Sensors
Distributed packet analysis, efficient use of network band-width and higher cybersecurity survivability during network outages

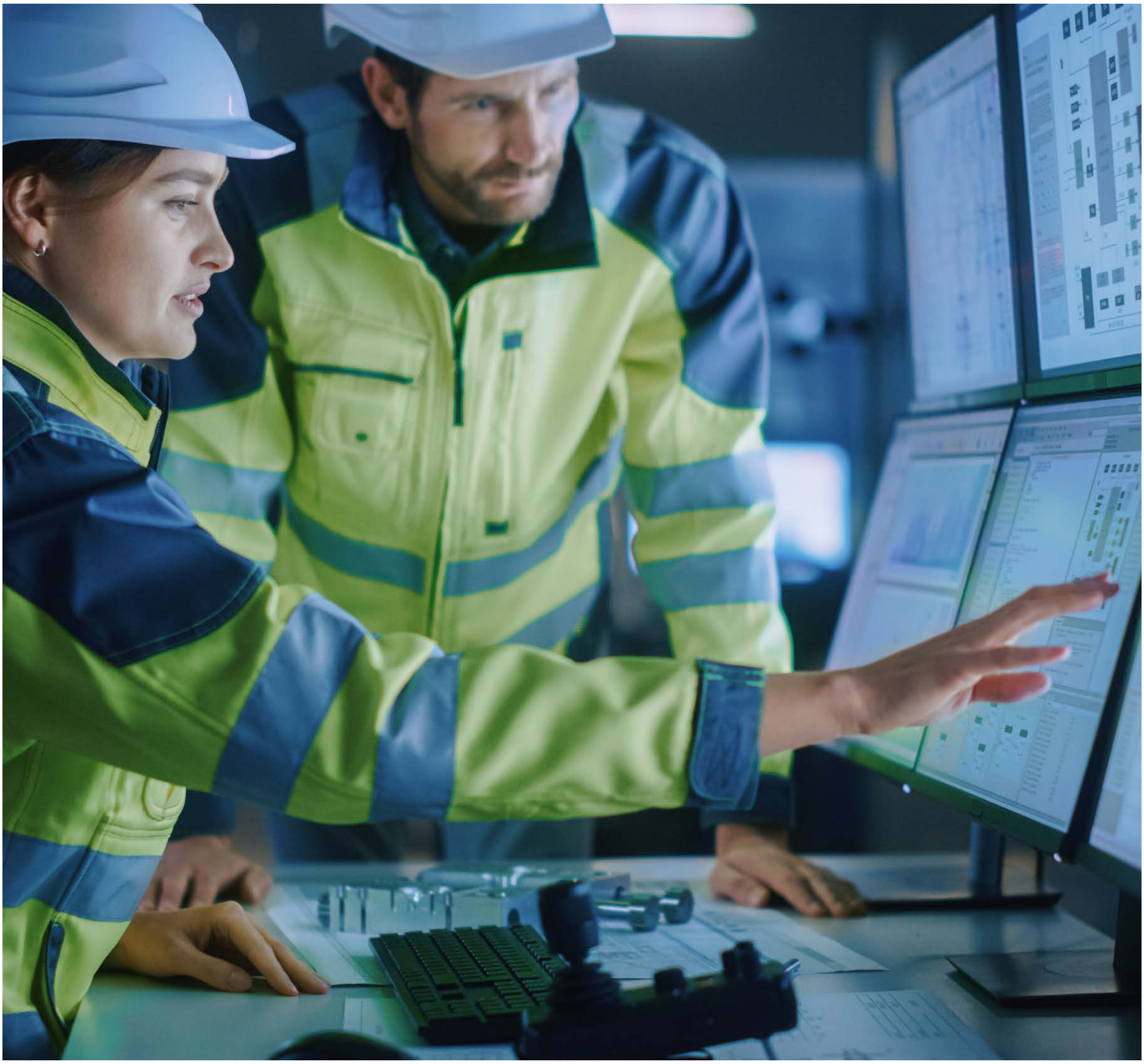
ADDRESSING THE TALENT AND CULTURE GAP

Creating an effective enterprise-level O) cybersecurity strategy is crucial for organizations to foster a culture of cybersecurity awareness among all employees. This strategy should encompass defense-in-depth principles that help address various cybersecurity challenges. Implementing multiple layers of security controls – such as network segmentation, asset monitoring, vulnerability and threat detection, incident response, assessments, and training – within OT systems is crucial for bolstering cybersecurity. This strategy incorporates design elements that provide a range of fail-safe mechanisms to help effectively establishing defense in depth for OT systems.

A well-rounded cybersecurity awareness program is an essential component of the overall cybersecurity stance as it encourages every individual – anging from executives to operational technicians – to recognize their responsibility in upholding security protocols.

To successfully bridge the skills gap, organizations can implement training and certification programs designed to enhance the expertise of their OT security teams in the form of self-paced, in-class, or instructor-led remote experiences. Additionally, building cyber-aware teams across various functional areas will contribute to a more secure environment.

Testing cybersecurity readiness is another fundamental practice. Conducting drills through tabletop exercises and red team assessments across operational technology (OT), information technology (IT), security operations centers (SOC), compliance, physical security, and cloud security can significantly improve an organization's cybersecurity resilience.



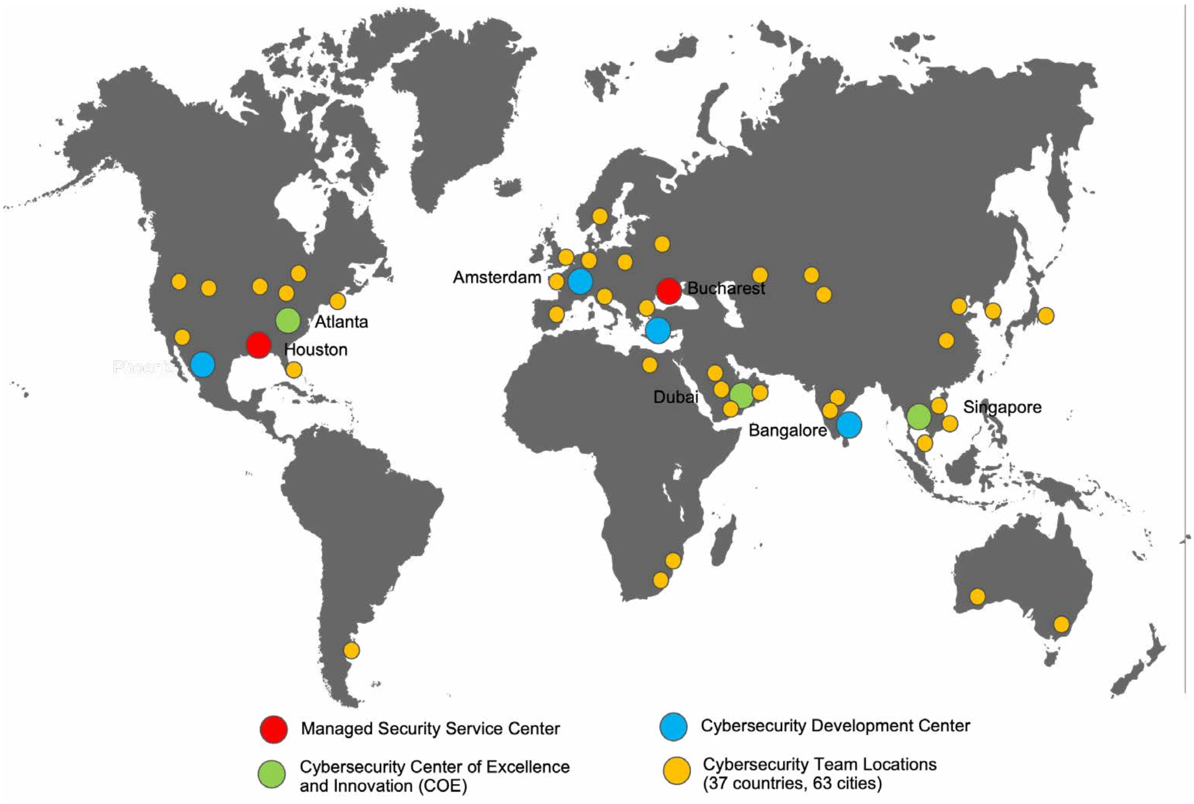
CONCLUSION: NAVIGATING THE FUTURE OF OT CYBERSECURITY

Cyber threats are ever-changing in sophistication, and unfortunately, also increasing at a rapid pace. Organizations must adopt a holistic, proactive strategy to better protect their OT assets and ultimately their operations. This means understanding potential risks at a site and enterprise level, creating a plan on how they will respond and deploying a SOC that monitors OT and IT threats.

By leveraging AI in SOC operations, organizations can enhance efficiency and reduce false positives as well as enable a scalable, adaptive and resilient cybersecurity posture prepared for both current and future threats. Taking a comprehensive approach to the establishment of an OT Cyber SOC that spans sites and the enterprise can help enable a defense in the face of an ever-changing threat landscape to help safeguard critical infrastructure and maintain regulatory compliance. It is critical for CISOs and cybersecurity professionals to continue to educate their company's leadership and board on the growing interconnectivity between IT and OT assets and how proactive investments can be more effective than reactive responses in the long term.

Connect with us to learn how Honeywell OT cyber experts and a Honeywell OT SOC can facilitate your journey to OT cyber resilience and compliance.
Honywell is an established leader in OT cybersecurity having completed more than 7,000 projects across more than 130 countries. The team has specialized expertise in protecting critical infrastructure, holds more than 35 patents and comprises more 500 dedicated cybsersecurity professionals who provide support to more than 600 customer sites through Managed Security Services. The organization prides itself on delivering comprehensive, vendor-neutral solutions that cater to diverse cybersecurity needs, providing clients with the most effective protective measures.

Honeywell supports a comprehensive suite of OT cybersecurity solutions through its Global Centers of Excellence located in Atlanta, Singapore and Dubai, as well as cybersecurity Security Operations Centers (SOCs) in Romania, Houston and Atlanta. Honeywell integrates capabilities with third-party solutions to effectively resolve cyber threats, employing intelligent systems for predictive modeling and real-time compliance monitoring. Honeywell aligns closely with its customers through collaborations with industry coalitions, technology leaders such as ISASecure, ISA/IEC, and government bodies like CISA and NIST, enhancing its expertise and strategies in cybersecurity response.


Amsterdam
Bucharest
Atlanta
Houston
Dubai
Singapore
Bangalore
Managed Security Service Center
Cybersecurity Development Center
Cybersecurity Center of Excellence and Innovation (COE)
Cybersecurity Team Locations (37 countries, 63 cities)

NIS2 Directive

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

U.S. DEPARTMENT OF HOMELAND SECURITY
CISA
CYBER+INFRASTRUCTURE

ISA IEC ISO

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

IT Service Management ISO 20000 Certified

Information Security Management ISO 27001 Certified

METHODOLOGY

This report is based on extensive research from multiple cybersecurity analyst firms as well as data from global surveys conducted by third-party research companies. It also leverages the latest research from NIST and the U.S. Securities and Exchange Commission (SEC). Please see full reference list for noted data sources.

References:

- Ponemon Institute - Cost of a Data Breach Report, 2024
- Industrial Cybersecurity Outlook, Westlands Advisory, 2024
- Keith Stouffer et al., Guide to Operational Technology (OT) Security, NIST, September 2023.
- McKinsey & Company, the-risk-based-approach-to-cybersecurity, Jim Boehm, 2019
- 7 Erik Gerding, Cybersecurity Disclosure, US Securities and Exchange Commission, December 14, 2023
- Industrial Cybersecurity Industry Analysis, Westlands Advisory, October 2023
- Critical Infrastructure Security, ABil Research, October 2024
- The Biggest OT Security Incidents of 2024: Lessons for Critical Infrastructure, InfosecK2K, December 2024

[i] "Cost of a Data Breach", Ponemon Institute, 2024

For more information

www.honeywell.com

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

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell