Deloitte. | paloalto NETWORKS

SECURING OPERATIONAL TECHNOLOGY

Integrating technology and governance to mitigate cyber risks in industrial environments

TABLE OF CONTENTS

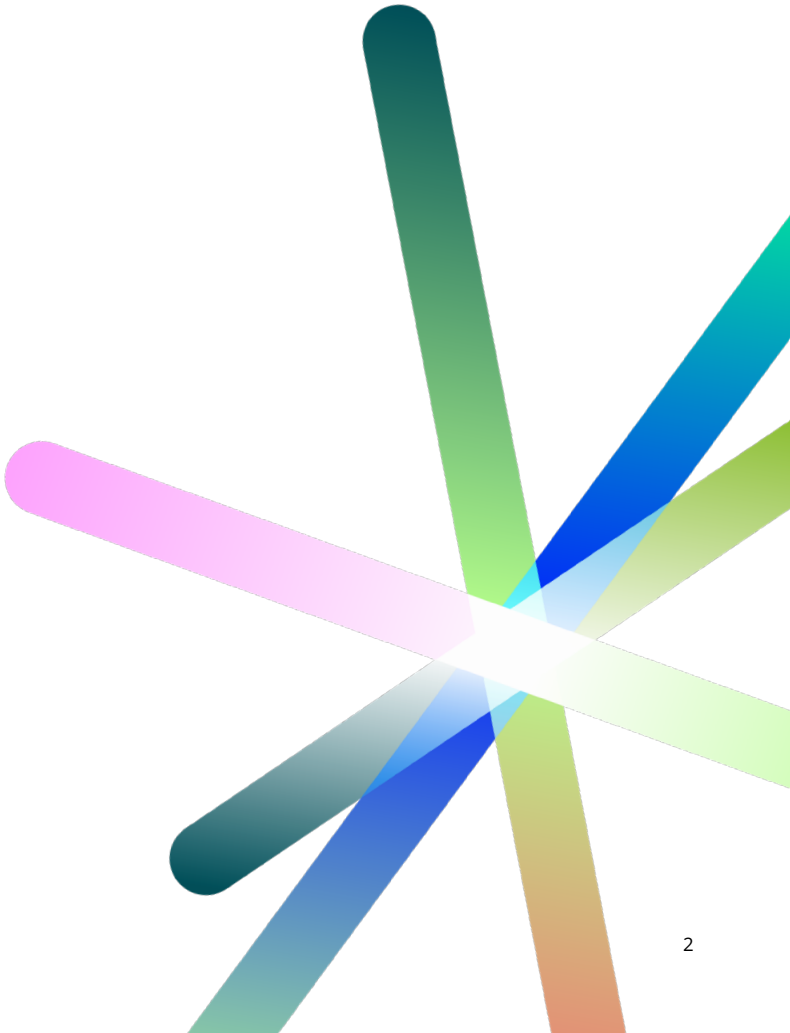


TABLE OF CONTENTS

INTRODUCTION

Manufacturers are prime targets for cyberattacks due to their high value, complexity, and outdated systems. Motivations include financial gain, competitive advantage, and strategic disruption. The integration of information technology (IT) and operational technology (OT) has created new vulnerabilities, requiring stronger security measures.[1]

Across the globe, a power grid narrowly avoided disaster when attackers exploited legacy OT equipment to gain remote access, highlighting the fragile boundary between uptime and catastrophe.[2]

Several high-profile cybersecurity breaches involving supervisory control and data acquisition (SCADA) systems have highlighted the growing risks to critical infrastructure. One notable incident involved a US-based energy provider that identified unusual activity within its SCADA network. Subsequent investigations revealed that threat actors exploited unsecured remote access protocols to gain unauthorized control over grid operations, exposing vulnerabilities in the system's defenses and emphasizing the urgent need for stronger OT security measures.[3]

These stories are not anomalies—they are part of a rising trend targeting OT environments, the backbone of industries such as manufacturing, energy, and health care.[4] **In the past two years alone, OT-targeted attacks have increased by 50%**, with ransomware groups shifting their focus from data theft to disrupting critical infrastructure.[5]

The problem? Unlike traditional IT environments, OT systems were designed for reliability and longevity—not security.[6] Industrial control systems (ICS), Internet of Things (IoT) devices, and legacy machines now coexist in sprawling, interconnected environments, expanding the attack surface exponentially.[7] While IT teams regularly apply patches to address vulnerabilities, OT environments often postpone updates to avoid downtime, which can create potential security gaps.[8]

Imagine the cost of losing control over smart manufacturing lines, medical devices, or energy grids. For many enterprises, the question isn't if an attack will happen, but when.[9]

This white paper unpacks hidden risks of OT environments and offers actionable solutions, blending insights from Deloitte's strategic advisory services and Palo Alto Networks' cutting-edge technology. Real-world case studies and practical frameworks can guide you in fortifying OT systems, protecting critical assets, and enabling operational resilience to reduce potential downtime.

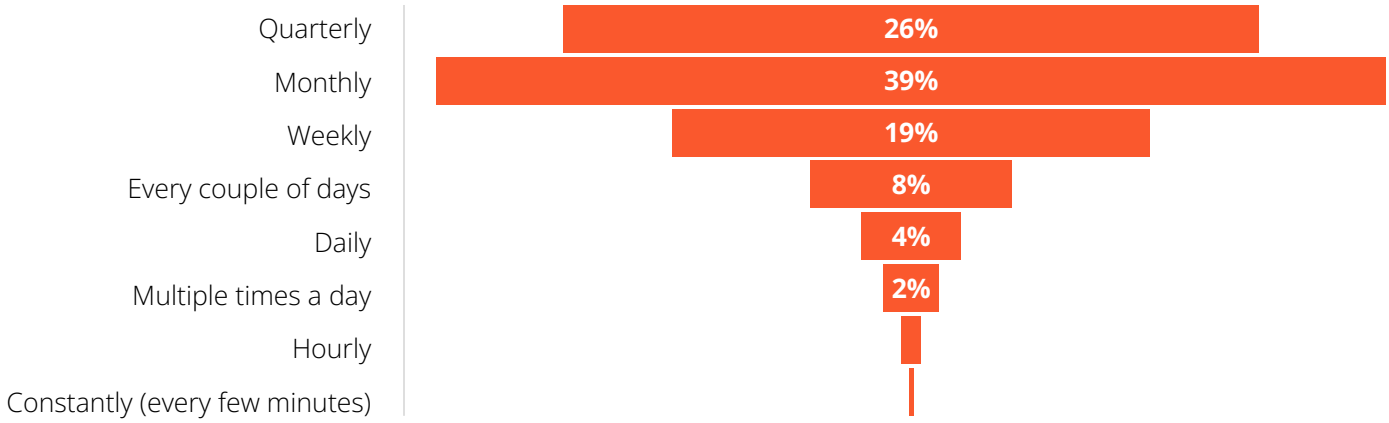
Will your enterprise take control before attackers do?

1.0

Common OT challenges

This white paper focuses on the OT environment by identifying specific security challenges faced by large enterprises. As OT environments converge with IT, vulnerabilities in traditionally isolated operational systems may be exposed. The National Institute of Standards and Technology (NIST) emphasizes that while security solutions exist for typical IT systems, special precautions are required when introducing these solutions to OT environments.[10]

HOW FREQUENTLY DO YOU TYPICALLY EXPERIENCE ATTACKS (OR INCIDENTS) IN YOUR OT ENVIRONMENT?



Source: Palo Alto Networks' **State of OT Security Report 2024**

Close to *70% of respondents* from a global survey of C-suite management and practitioners report at least monthly attacks within their organization's OT environment.

1.1
THE CLOCK IS TICKING: WHY SECURING OT ENVIRONMENTS IS IMPORTANT

Cyberthreats are no longer just external—they've already stepped inside. OT environments, the beating heart of ICS and smart manufacturing lines, are under siege.[11] **Many connections, each IoT device, and each unpatched system can expand the battlefield for attackers, leaving enterprises dangerously exposed.[12]**

The priorities in OT systems—uptime, safety, and efficiency—have traditionally outweighed security in many instances, but that trade-off is no longer sustainable.[13] **Ransomware groups now target critical infrastructure with surgical precision, threatening to shut down production lines, disrupt power grids, and cripple essential services.[14]** For large enterprises, the question isn't *if* an attack will happen, but *when*—and the cost could stretch into millions, not just in dollars, but in reputational damage and environmental disasters.[15]

1.2
THE HIDDEN RISK IN PROGRESS

OT systems have evolved from isolated, proprietary networks into highly integrated, open platforms that interface effectively with IT environments. This digital transformation has unlocked greater productivity, efficiency, and cost savings, but also it has torn down the walls that once shielded industrial environments from external threats.[16]

The result? **Cyber vulnerabilities that once plagued IT environments now lurk within OT networks, exposing fragile systems infrequently designed for the security-first world of today.[17]** Many industrial advancements are shadowed by new attack vectors that could lead to catastrophic downtime, production halts, and safety incidents.[18]

1.3
WHAT'S AT STAKE?

A compromised ICS doesn't just mean a temporary halt in production; it can trigger operational issues, risk to workers, pollution, and cascading financial losses.[19] **A single breach can cripple operations for days or even weeks, with ripple effects across supply chains.[20]**

1.4
ISOLATING SYSTEMS ISN'T THAT ANSWER

Closing the doors to innovation and reverting to siloed, stand-alone control systems may not be a viable solution. **Instead, enterprises can consider embracing the reality of modern OT environments—layered, interconnected, and complex—by embedding cybersecurity at the core of many systems.[21]** Just as machine safety engineering evaluates risks and implements protective layers, OT security should consider adopting the same rigor to defend against evolving threats.[22]

1.5

CYBERSECURITY IS AN OPERATIONAL IMPERATIVE, NOT JUST AN IT CONCERN

Manufacturers, power grid operators, chemical plants, transportation hubs, and pipeline owners **can be prime targets.**[23] Attackers see these industries as goldmines—with the potential to extract massive ransom payments or cause unprecedented disruption. **Regulators and insurers are raising the stakes**, recognizing the urgency of safeguarding OT systems to maintain both operational continuity and the well-being of the public.[24]

1.6

SECURITY IS NO LONGER OPTIONAL IN OT

This mantra rings truer than ever. The diverse technology, scale, and age of OT systems demand a customized, risk-informed approach to cybersecurity. There is no universal fix, but doing nothing is no longer an option.[25]

The longevity of critical infrastructure depends on swift, decisive action. **The time to secure OT environments is now—before attackers make the next move.**

2.0

Issues around people, process, technology, and corporate culture

OT environments are the blackbone of industries, yet they face relentless cybersecurity challenges driven by gaps in people, processes, technology, and culture.

Conflicting priorities between IT, cybersecurity, and operations teams can create a tug-of-war, leaving critical vulnerabilities unaddressed. Operational staff, hesitant to adopt new security protocols, may fear downtime more than breaches, while a glaring skills shortage leaves OT personnel ill-equipped to tackle modern cyberthreats.

Fragmented governance divides responsibility between IT and OT, which can result in reactive, **inconsistent policies** and sluggish incident response that fails to protect critical assets.

As IoT devices flood OT environments, legacy systems grow more exposed, expanding the attack surface with **unpatched, aging technology** that lacks basic security features.

Despite the rising tide of threats, many organizations continue to prioritize uptime and productivity over security, reinforcing a corporate culture **where resistance to change is common**—even when those changes are clearly in their best interest. Without executive buy-in and broad training, cybersecurity risks continue to escalate.

To safeguard critical infrastructure, enterprises should consider bridging the divide between operational efficiency and broad security—

because in OT, the cost of complacency could be far greater than the cost of action.

2.1

PEOPLE: ADDRESSING THE HUMAN ELEMENT IN OT SECURITY

OT environments are complex ecosystems involving multiple stakeholders, each with different objectives and responsibilities. This diversity can create misaligned priorities, hindering the development of cohesive security strategies.

2.1.1

DIVERSE STAKEHOLDERS AND MISALIGNED PRIORITIES

The intersection of **IT, cybersecurity teams, operations staff, and third-party vendors** introduces competing interests. IT teams prioritize **data integrity, availability, and confidentiality**, while OT personnel focus on **safety, uptime, and productivity**. Cybersecurity teams advocate for **risk mitigation and compliance**, often clashing with operational teams reluctant to implement changes that could disrupt workflows.

According to Deloitte's **2023 cybersecurity for OT report**, the lack of collaboration between IT and OT departments remains a **top barrier** to achieving effective OT security.[26] The report highlights that **40% of OT leaders** cite poor cross-departmental communication as a critical **vulnerability** in their infrastructure.[27]

2.1.2

RESISTANCE TO CHANGE AND CYBERSECURITY AWARENESS

Operational teams frequently resist cybersecurity initiatives due to concerns over **downtime, production delays, and potential system instability**. This resistance is further compounded by a documented skills gap in OT cybersecurity, with the report highlighting that a significant portion of OT professionals lack the necessary training and expertise to implement or support modern security measures.[28] **Sixty percent of OT personnel** view cybersecurity protocols as **disruptive** rather than beneficial, contributing to **delayed security implementations**.[29]

A Palo Alto Networks study found that **58% of OT operators** had **never participated in cybersecurity awareness programs**, leaving critical systems vulnerable to phishing and ransomware attacks.[30]

2.1.3

SKILLS SHORTAGES IN OT CYBERSECURITY

A significant gap exists in **OT-specific cybersecurity experience**, compounding the risks posed by emerging threats. While IT teams often receive regular cybersecurity training, **OT personnel are rarely equipped** to identify or respond to advanced threats.[31] Advanced threats refer to complex, targeted cyberattacks that are difficult to detect and often are designed to bypass traditional security measures. The SANS Institute's 2024 ICS/OT cybersecurity survey reveals that **only 34% of organizations prepare for cyber incidents using environments equipped with ICS/OT-specific tools.[32]** Additionally, **51% of respondents are protecting these systems without relevant certifications, raising concerns about their preparedness to recover from industrial cyber incidents.[33]**

2.2 PROCESS: BUILDING A UNIFIED GOVERNANCE FRAMEWORK

Fragmented governance and insufficient incident response plans can create operational silos that expose OT environments to **unmonitored risks**. Bridging the gap between IT and OT security processes is important to achieving broad protection.

2.2.1 FRAGMENTED GOVERNANCE AND POLICY MISALIGNMENT

Security responsibilities are often divided between IT and OT teams, which can lead to **inconsistent policies, misaligned strategies, and operational inefficiencies**. Disjointed governance can result in **incomplete risk assessments** and **vulnerable OT assets**.

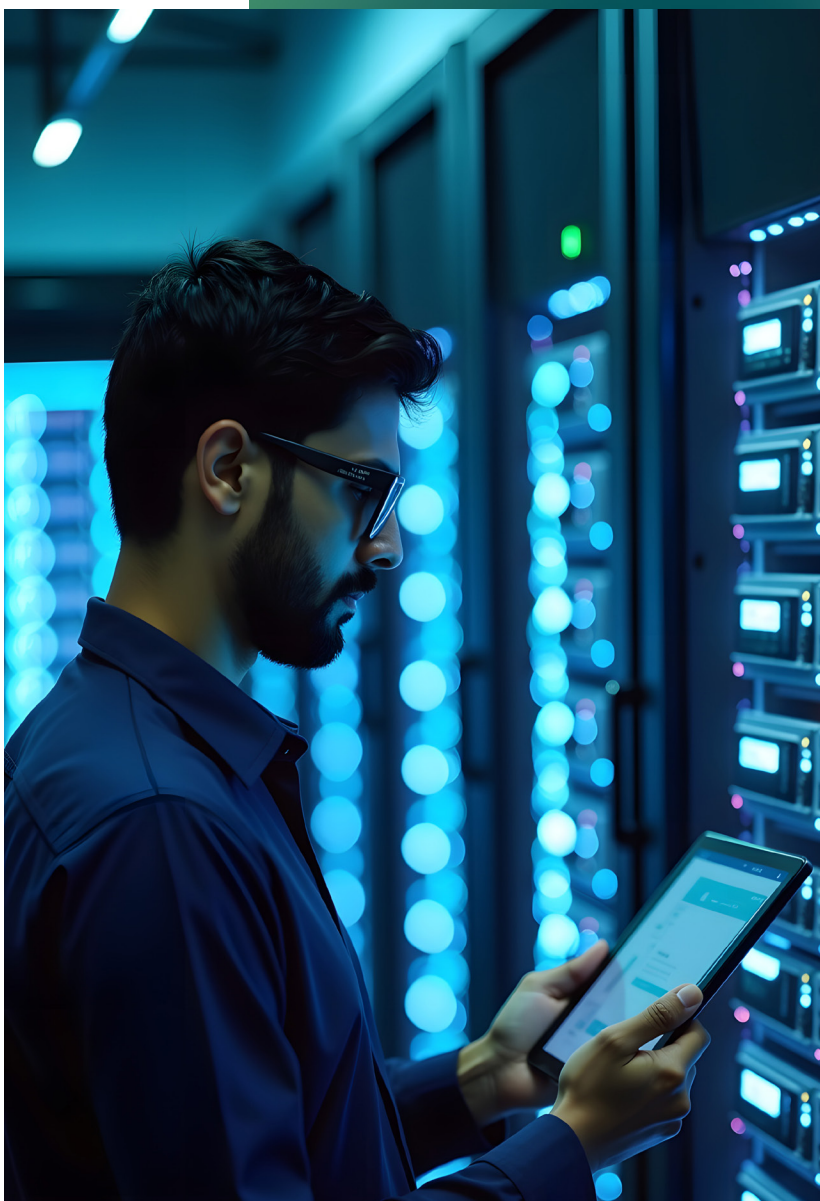
Deloitte's **OT Governance Framework** emphasizes the need for **integrated governance models** that unify security across IT and OT. Enterprises that implement centralized governance structures can see more **reduction in breach-related downtime**.[34]

2.2.2 INCIDENT RESPONSE GAPS IN OT

Traditional IT-centric incident response plans may **fail to account for OT constraints**, such as the need for **continuous uptime and operational stability**. A Palo Alto white paper highlights that **70% of OT environments** lack dedicated response protocols, resulting in **longer recovery times** during cyber incidents.[35]

2.2.3 ASSET VISIBILITY CHALLENGES

A **lack of full asset visibility** may prevent enterprises from applying consistent security measures across OT networks. This issue can be compounded by **IoT device proliferation** and **legacy OT systems**. **NIST** underscores that **broad asset visibility** is the foundation of **effective OT security**.[36]



2.3

TECHNOLOGY: SECURING LEGACY SYSTEM AND IOT EXPANSION

Legacy OT systems, while reliable, may **lack the security features** required to withstand modern cyberattacks. The integration of IoT devices further expands the attack surface, creating **new entry points** for malicious actors.[37]

2.3.1

LEGACY SYSTEMS: THE WEAK LINK IN OT SECURITY

Legacy OT systems, while reliable, often **operate on outdated software with unpatched vulnerabilities, making them prime targets for modern cyberattacks.** The integration of IoT devices further expands the attack surface, introducing new entry points for malicious actors.

According to the **2023 Unit 42 Ransomware and Extortion Report** by Palo Alto Networks, approximately **50% of ransomware attacks and breaches result from attack surface exposures, with legacy systems being particularly vulnerable.[38]**

2.3.2

IoT EXPANSION AND SECURITY GAPS

The rapid adoption of IoT devices has significantly accelerated digital transformation within OT environments. However, this swift integration has often led to inconsistent security protocols, leaving many devices vulnerable to cyberthreats.

A report by Armis highlights that **67% of IoT devices in enterprise environments are unpatched, and 84% of health care delivery organizations have IoT devices running on unsupported operating systems**, underscoring the widespread nature of these vulnerabilities.[39]

2.4

CULTURE: EMBEDDING UBERSECURITY INTO OT MINDSETS

A strong cybersecurity culture is the **cornerstone** of effective OT security. However, **cultural barriers** often prevent the effective adoption of security protocols in industrial environments.[40]

2.4.1

OPERATIONAL PRIORITIES OVER SECURITY

In OT environments, prioritizing uptime and productivity often leads to cybersecurity being viewed as a secondary concern and increasing vulnerability to cyberthreats. However, research indicates that organizations implementing broad security awareness training can reduce security-related risks by up to 70%.[41]

3.0

Mitigating OT security challenges: A strategic and engaging approach

Addressing OT security is no longer just a technical necessity; it's a business-critical initiative that can mean the difference between operational resilience and catastrophic disruption. As OT environments become increasingly interconnected with IT systems, vulnerabilities multiply, making broad strategies imperative. By integrating **people, processes, technology, and culture**, organizations can effectively fortify their OT environments.[42]

Here's how enterprises can take decisive, impactful action to safeguard their most critical assets:

3.1 PEOPLE: BRIDGING THE SKILLS GAP AND DRIVING COLLABORATION

Why it matters

OT environments thrive on collaboration between IT, operations, and security teams. However, the divide between these groups can create a blind spots, leading to vulnerabilities that attackers can exploit. Closing this gap is important to building a resilient and secure infrastructure.

Cross-functional alignment

Break down traditional silos by fostering **cross-departmental collaboration** between IT, cybersecurity, and operations teams. Create joint task forces that align **security goals with operational priorities**. Encourage shared accountability by integrating security-focused professionals into daily operations, making cybersecurity a seamless part of the workflow rather than a barrier. This approach helps reduce potential disruptions and supports consistent productivity. Regular roundtable discussions and security inspections can foster a **culture of shared responsibility.**

Upskilling and training

A well-trained workforce is the first line of defense against cyberthreats. Implement **targeted, hands-on training programs** to equip OT personnel with practical cybersecurity skills. Focus on **real-world scenarios** like ransomware incidents, phishing attacks, and ICS vulnerabilities. Consider alliances with **cybersecurity firms** or certifications from organizations like SANS Institute or ISA/IEC 62443 to enhance skill sets. Continuous training not only **closes the skills gap** but also **empowers staff** to proactively identify and mitigate risks.

Incentivize security adoption

Create a **positive feedback loop** by tying security performance to productivity metrics. Offer **recognition programs** for teams that actively participate in security initiatives or effectively prevent breaches—highlighting how cybersecurity measures **protect uptime**, and **productivity** can reduce resistance to change, fostering **proactive participation** in OT security efforts.

3.2
PROCESS: GOVERNANCE, VISIBILITY, AND RAPID RESPONSE

Why it matters

A lack of structured governance and visibility may leave OT systems vulnerable to undetected threats. Governance should consider extending beyond IT to encompass OT environments, confirming that both IT and OT are aligned under a unified security strategy.

Unified governance framework

Establish **a centralized governance model** that bridges the gap between IT and OT to enable effective oversight across both domains. Appoint **OT security leaders** who are responsible for specific security areas and collaborate with cyber leadership to address issues, supporting the alignment of security measures with broader business objectives. Leverage frameworks like **NIST Cybersecurity Framework (CSF)** or **ISA/IEC 62443** to create policies tailored to OT-specific risks, fostering **consistent security practices.**

Asset visibility and monitoring

You can't secure what you can't see. Deploy **network monitoring tools** to gain full visibility into OT assets, IoT devices, and industrial networks. Conduct **broad asset inventories** and integrate **security information and event management (SIEM)** systems that continuously scan for anomalies. Regular **penetration tests** and **red team exercises** can uncover hidden vulnerabilities.

Tailored incident response plans

Generic IT incident response plans may fail to address the different constraints of OT environments. Design **customized OT incident response protocols that prioritize reducing operational downtime.** Conduct **regular tabletop exercises and live simulations** to test response effectiveness. Involve OT personnel in planning to guard that protocols reflect **real-world operational limitations** to help establish faster and more coordinated responses to breaches.

3.3
TECHNOLOGY: MODERNIZING LEGACY SYSTEMS AND SECURING OT

Why it matters	Outdated systems and the rapid adoption of OT can create a **growing attack surface**. Many OT environments operate on **legacy equipment**, which may lack modern security features, making them prime targets for cyberattacks.

Patch and upgrade legacy systems

Develop **phased upgrade plans** for legacy systems, focusing on **high-risk assets first**. Where patching is unfeasible, deploy **compensating controls** such as firewalls, micro-segmentation, and **zero trust architectures** to contain vulnerabilities. Implement **regular update schedules** to prevent systems from falling behind and becoming easy targets.

OT security by design

Secure OT from the ground up by embedding **security requirements** into procurement processes. Choose vendors that offer **built-in security features** such as **firmware protection, encrypted communication, and secure boot processes** among others. Use **network segmentation** to isolate OT devices, preventing them from serving as entry points to critical OT systems. Deploy **behavior analytics** to detect anomalies that may indicate compromised OT devices.

Broad security platforms

Integrate IT and OT defenses through a **unified security operations center (SOC)**. Leverage platforms like **Palo Alto Networks' Cortex XSIAM** to provide **real-time monitoring, centralized threat intelligence, and automated incident response** across the entire infrastructure. This unified approach cancels operational silos and determines **broad threat detection.**

3.4

CULTURE: DRIVING A SECURITY-FIRST MINDSET

Why it matters	Even the most advanced technology won't protect an enterprise if the corporate culture doesn't prioritize cybersecurity. OT environments often emphasize uptime over security, potentially creating **cultural barriers** that may leave systems vulnerable.

Executive buy-in and oversight

Security initiatives are more likely to succeed when supported by leadership. Educate executives on the **financial and operational risks of OT breaches**, providing real-world examples of **industrywide cyberattacks** to highlight the potential impact. Embed cybersecurity into **risk management strategies** and position it as a **business enabler**, not a cost center. See that cybersecurity leaders have **direct access to the board** to elevate OT concerns.

Continuous awareness campaigns

Promote **ongoing awareness campaigns** that highlight the **real-world consequences** of inadequate OT security. Use **case studies** of incidents to capture attention and drive engagement. Incorporate **gamified learning experiences** and phishing simulations to make cybersecurity training engaging and memorable.

Align security with operational goals

Frame cybersecurity as **essential to operational resilience**, emphasizing that downtime caused by cyberattacks may pose a greater threat than proactive security measures. Involve OT leaders in decision-making to confirm that security aligns with **productivity and uptime requirements**. Position security teams as **partners in success**, and not barriers to efficiency.

3.5

ARTIFICIAL INTELLIGENCE (AI) IN THE USE OF THE OT

The use of AI in the context of large language models (LLMs) can enhance the detection and accuracy of anomalies and potential threats within the OT domain. As aforementioned, new definitions and signatures for emerging vendors and devices are relevant in the way of categorizing and itemizing detections in internal systems. The use of AI can also enhance and expedite these methodologies. This can allow internal security systems to define and process new devices and potential risk found on corporate networks.

There are several areas where AI and machine learning (ML) are making a positive impact in an organization's overall security posture.

Threat response

Organizations contend with a rapidly expanding OT footprint that extends beyond conventionally known OT signatures. With the proliferation of IoT and OT devices, there may be an increased necessity to rapidly onboard new signatures and definitions that may fall outside of conventional parameters.

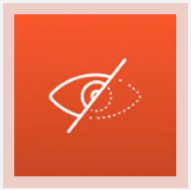
User Entity Behavior and Analytics (UEBA)

The use of UEBA within ML data sets can improve detection within security tools. Determining how a regular user interacts with an environment can inform and enhance the fidelity and accuracy of data sets. Additionally, UEBA characteristics can determine baseline functionality and augment the definitions of data sets on patterns and techniques that may likely be considered outside the bounds of regular use.

Skills gap

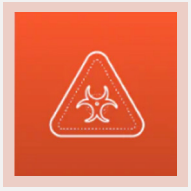
One of the more glaring issues with OT security is the skill set gap in practitioners' ability to detect and respond against security threats.[43] The use of ML and LLMs can bridge the gap between conventional detect-and-respond capabilities and the nuisances of OT-related attack definitions.

Modern OT security challenges

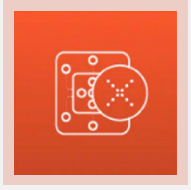


It's not possible to secure what can't be seen

Unseen vulnerabilities create exponential risk



Threats are outpacing the capacity for prevention



It is difficult to operate excessively complex systems

Source: Palo Alto Networks' **State of OT Security Report 2024**

Protecting against threats in modern OT systems is multifold. Leveraging the points above is important to having an effective security strategy. Modern advancements in AI and ML can help enhance an organization's ability to detect, respond, and counter modern-day sophisticated attacks within OT environments.

3.6

WHY ACT NOW?

Cyber adversaries are targeting OT systems with increasing precision. The convergence of IT and OT has opened the door for **sophisticated ransomware attacks and supply chain vulnerabilities**.[44] Enterprises that fail to act may risk not only financial losses but also **long-term reputational damage.**

By embedding cybersecurity at the heart of OT environments, organizations protect **operations, profits, and people**. In today's digital landscape, **proactive defense is important to future resilience.**

OT security

has moved beyond the technical realm. It stands at the heart of business resilience and continuity. OT security has evolved into a core driver of business resilience and operational continuity. As OT environments increasingly converge with IT systems, they inherit the vulnerabilities of interconnected digital networks. This interdependency, while driving efficiency and innovation, can expose critical infrastructure to cyberattacks capable of halting production and inflicting millions in financial losses.

The message is clear: Securing OT is a necessity. Organizations should consider adopting a proactive, strategic approach that integrates **people, processes, technology, and culture** to build strong defenses against evolving threats.

4.0

Palo Alto Networks: A broad approach to OT security

Palo Alto Networks stands at the forefront of OT security, providing **holistic solutions** designed to **anticipate, detect, and neutralize cyberthreats** targeting industrial systems.[45] Their integrated approach checks that OT environments are not only secure but also agile and resilient in the face of evolving risks.

Palo Alto Networks offers an extensive suite of OT security solutions that extend beyond traditional defenses. Its platform integrates **AI-driven threat detection, zero trust architectures, unified security management, and automated response** to address vulnerabilities across the full spectrum of OT environments. By focusing on the interplay between **people, processes, technology, and culture**, Palo Alto Networks can enable organizations to build a strong and **adaptive security framework.**

4.1

PEOPLE: ENHANCING COLLABORATION AND EXPERIENCE

Solutions

Palo Alto Networks fosters collaboration between IT and OT teams through unified platforms and zero trust principles that are aimed at simplifying security operations across industrial environments. It provides AI-powered tools, like **Guided Virtual Patching,** and offers educational initiatives for OT-specific security workflows.

Integrated security platform

Palo Alto Networks can bridge IT and OT teams by providing a **unified platform** that offers shared visibility and control. This can reduce conflicts, align security objectives, and enable effective **coordination between departments.**

Broad training programs

Through extensive training and certification initiatives, Palo Alto Networks can **upskill OT personnel** to handle modern cyberthreats.

OT security training

Industrial OT Security Hands-on Workshop

This on-demand workshop provides practical experience in safeguarding OT assets and networks. Specific learning outcomes include gaining precise asset visibility, conducting OT asset vulnerability and risk assessments, and implementing broad protection for OT perimeters and assets.

Cybersecurity Academy

Through a global network of K–12 schools, colleges, and universities, Palo Alto Networks offers world-class cybersecurity education. The Cybersecurity Academy provides a turnkey curriculum developed by experienced cybersecurity and threat intelligence professionals, introducing students to the rapidly growing field of cybersecurity.

4.1.1

WHY IT MATTERS

Security gaps frequently emerge due to a disconnect between IT, cybersecurity, and operational teams. Limited collaboration and inadequate cybersecurity experience within OT environments can create exploitable blind spots for adversaries. **Effective IT and OT convergence demands teamwork to mitigate security risks.** Without alignment, vulnerabilities can persist potentially leading to operational inefficiencies and increased risk.

4.1.2

MAIN OUTCOME

By promoting collaboration and enhancing team skills, organizations can decrease internal friction, which can enable security measures to support rather than disrupt operational efficiency. Greater alignment between IT and OT teams can break down security silos, which can foster a unified approach to protecting industrial systems.

4.2
PROCESS: STREAMLINING GOVERNANCE AND INCIDENT RESPONSE

4.2.1
SOLUTIONS

Unified governance frameworks

Palo Alto Networks facilitates the creation of **governance models** that align OT and IT departments under a **single security strategy.** This promotes consistent policies and can enhance visibility across the enterprise.

Tailored incident response plans

The platform provides tools to design **custom OT incident response protocols** that can decrease downtime during cyber events. These plans strive to provide rapid and coordinated response, and **reflect the different constraints of OT environments.**

4.2.2
WHY IT MATTERS

Without standardized processes and governance, OT environments **can become fragmented and inconsistent**, increasing the likelihood of unaddressed vulnerabilities. The absence of tailored incident response strategies can **heighten the risk of extended disruptions during cyberattacks**. To decrease downtime and maintain regulatory compliance, OT environments require efficient and adaptable governance, and an incident response process workflow.

4.2.3
MAIN OUTCOME

Organizations can enhance operational resilience by streamlining security practices and reducing response times. **Accelerated recovery can reduce financial losses and support business continuity**. Improved compliance management and rapid incident response can support ongoing operations to meet both security and regulatory requirements.

4.3
TECHNOLOGY: MODERNIZING AND SECURING INFRASTRUCTURE

4.3.1
SOLUTIONS

The introduction of ruggedized next-generation firewalls (NGFWs), Precision AI™, and zero trust architectures can secure legacy systems, remote operations, and distributed industrial setups. AI/ML-powered tools can enable advanced threat detection, asset visibility, and vulnerability management.

Ruggedized firewalls for harsh environments

The **PA-400R** Series, a ruggedized NGFW, provides **ML-driven threat protection** for industrial environments, even under extreme conditions such as high temperatures, humidity, dust, vibrations, and corrosive elements.

5G security solutions

Palo Alto Networks secures industrial 5G networks by offering **visibility, segmentation, and protection** for cellular-connected OT devices so that new technologies can be **safely integrated** into OT ecosystems.

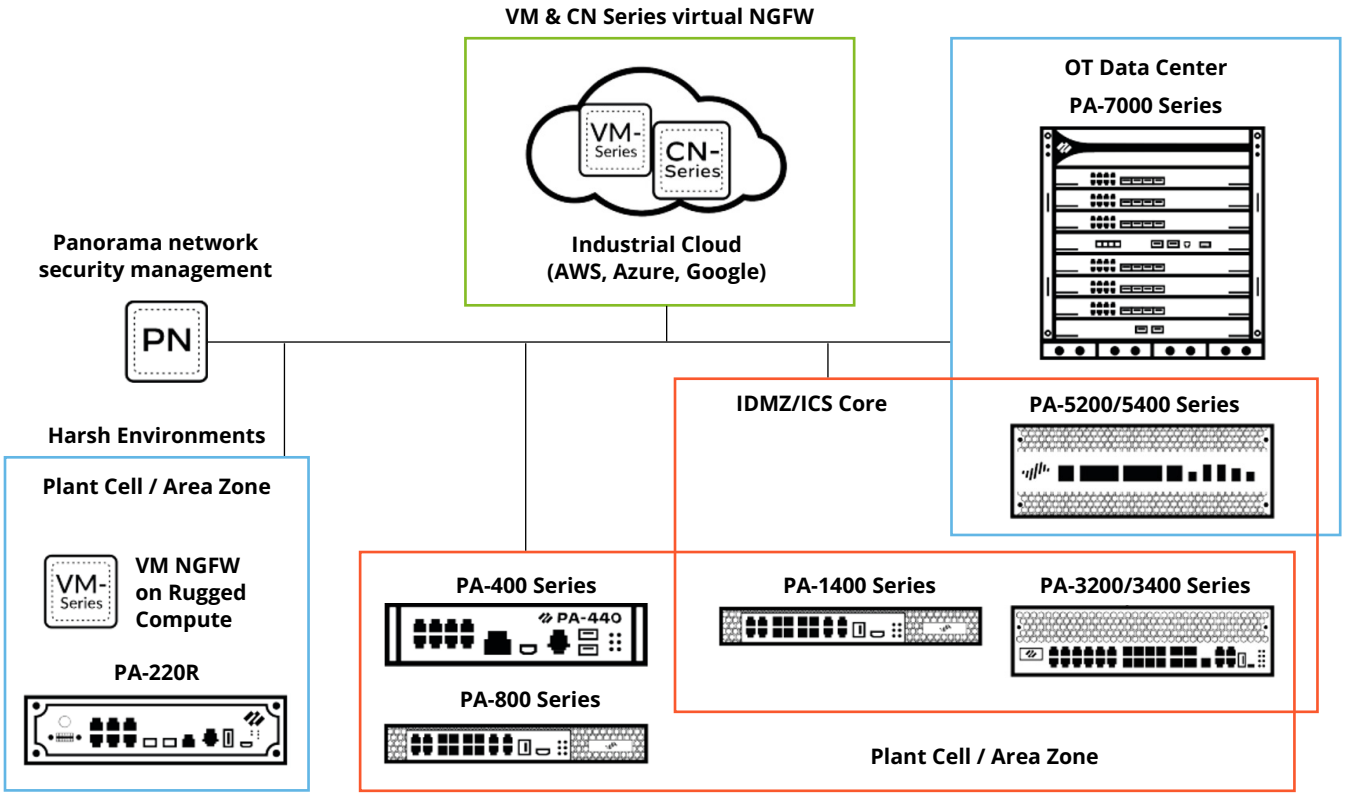
4.3.2
WHY IT MATTERS

Legacy OT systems and the rapid growth of IoT can introduce critical vulnerabilities in industrial environments. To address escalating cyber threats, modernizing infrastructure and integrating advanced security technologies should be treated as strategic imperatives. As industrial systems become more interconnected, **updating OT infrastructure can provide broad protection** against evolving risks and enhance overall resilience.

4.3.3
MAIN OUTCOME

Organizations can gain future-proof security and enable the adoption of emerging technologies while **safeguarding critical systems from potential risks**. This can result in resilient OT systems with reduced vulnerabilities, extended protection in harsh environments, and effective security management across both IT and OT infrastructures.

The Palo Networks NGFW product line, combined with zero trust features and Precision AI™, can secure the enterprise across the areas of the enterprise, including OT and the cloud.



Source: Palo Alto Networks, **Asset Visibility and Security for Industrial Control Systems, 2023**

4.4
CULTURE: FOSTERING A SECURITY-FIRST MINDSET

4.4.1
SOLUTIONS

Palo Alto Networks and Deloitte advocate for a **zero trust framework and OT-specific security training** to cultivate a culture where security is an intrinsic part of many operations.

Executive engagement

Palo Alto Networks provides **resources and insights** to help leadership understand the strategic importance of OT security, and cybersecurity investments are aligned with **business objectives.**

Continuous awareness campaigns

Regular awareness programs can emphasize real-world case studies showcasing the potential consequences of **cyberattacks on OT systems.** This can promote proactive engagement at many organizational levels.

4.3.2
WHY IT MATTERS

OT environments frequently emphasize uptime and efficiency at the expense of cybersecurity by creating a corporate culture that overlooks potential risks. Transitioning to a **security-first mindset** is important for safeguarding long-term operational integrity. **By fostering proactive security awareness**, organizations can empower employees to prioritize risk mitigation and reduce errors and vulnerabilities in critical industrial operations.

4.3.3
MAIN OUTCOME

Cybersecurity should be embedded within the organization's culture and making risk mitigation a collective responsibility across departments and roles. This widespread adoption of a **security-first mindset can enhance resilience and strengthen preparedness against OT-related threats.**

5.0

Deloitte OT security service: A business-critical imperative

Deloitte's OT security services go beyond patchwork solutions offering **broad and scalable programs** that can safeguard critical assets and provide operational resilience. Through **program design, technical assessments, governance frameworks, and managed services** Deloitte can help empower organizations to manage cyber risks across their OT environments effectively.

Deloitte offers a broad spectrum of OT security services designed to help organizations **mitigate vulnerabilities, enhance system reliability, and align to regulatory compliance.** These services are tailored to focus on the different challenges faced by industries reliant on OT infrastructure such as manufacturing, energy, health care, and transportation.

5.1
OT SECURITY PROGRAM DESIGN, DEVELOPMENT, AND IMPLEMENTATION

5.1.1
SOLUTIONS

Deloitte collaborates with organizations to design, develop, and implement OT security programs that align with operational goals while helping them address cyber risks. Services include:

Crafting security framworks

Tailored to OT environments

Integrating security

Into operational workflows

Embedding cyber risk management

Into the OT asset life cycle

5.1.2
WHY IT MATTERS

Embedding security into daily operations can **reduce the likelihood of disruptions** and strengthen critical infrastructure resilience.

5.1.3
INTENDED OUTCOMES

Operational continuity

Cyber risks are reduced; OT systems maintain productivity.

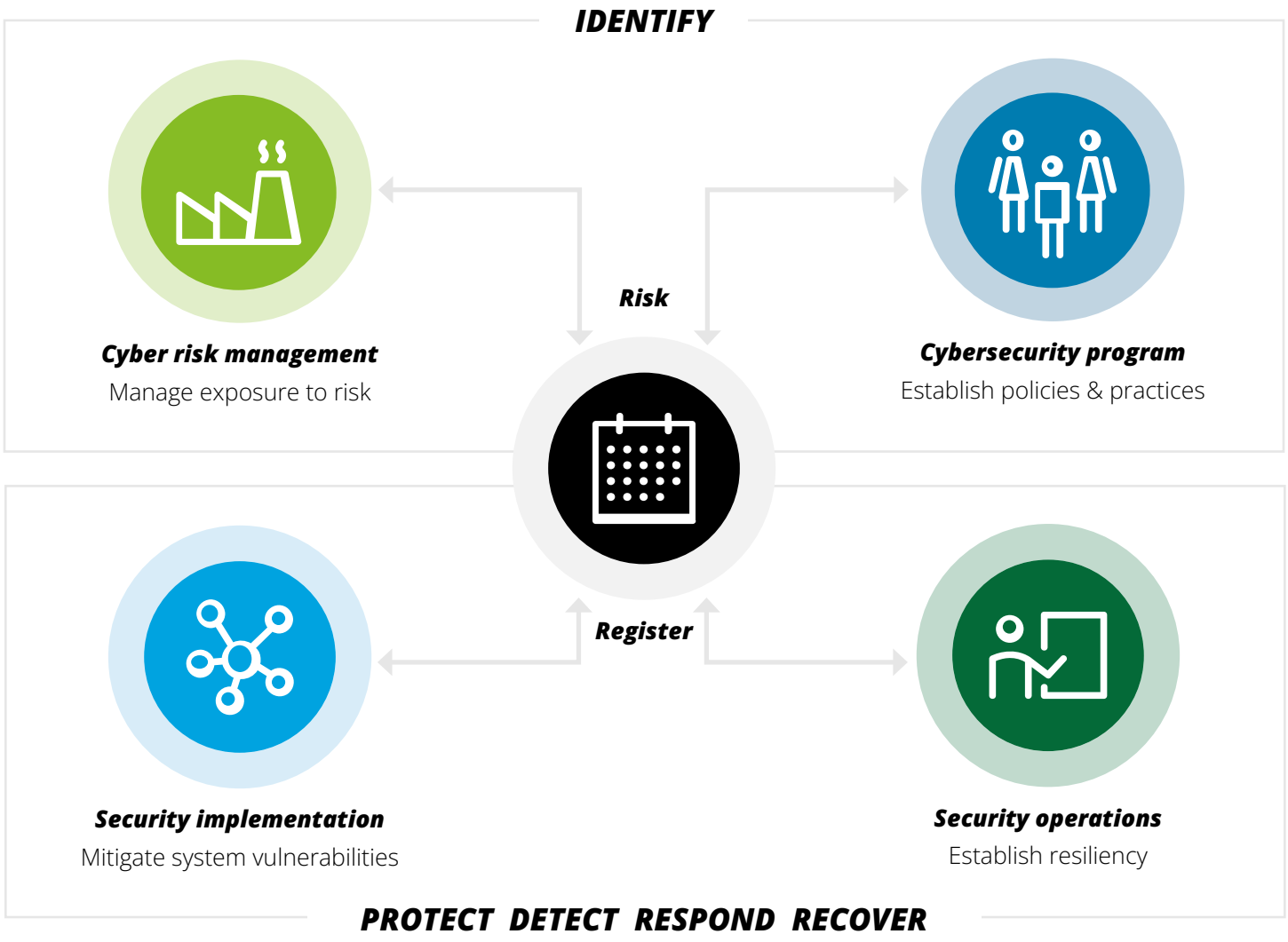
Risk-driven infrastructure

Security becomes an integral part of asset management and reducing vulnerabilities across the OT environment.

Adaptability

Programs are designed to scale and evolve with emerging threats and safeguarding long-term operational integrity.

Deloitte offers a suite of end-to-end services that can help organizations address OT cyber risks of today while also preparing for the future.



5.2
OT SECURITY ASSESSMENTS

5.2.1
SOLUTIONS

Deloitte conducts in-depth assessments to evaluate the strength and maturity of existing OT security frameworks. These assessments can take two distinct approaches:

Standards-based gap analysis

Aligning with industry frameworks (e.g., NIST CSF, IEC 62443).

Cyber Process Hazard Analysis (PHA)

A consequence-based assessment to identify vulnerabilities and evaluate potential impacts on operations, production, and regulatory compliance.

5.2.2
WHY IT MATTERS

These assessments can reveal **hidden weaknesses** and potential entry points for cyberattacks, empowering organizations to take proactive steps toward remediation.

5.2.3
MAIN OUTCOMES

Strategic remediation

Vulnerabilities are prioritized and allow security teams to address the most pressing threats first.

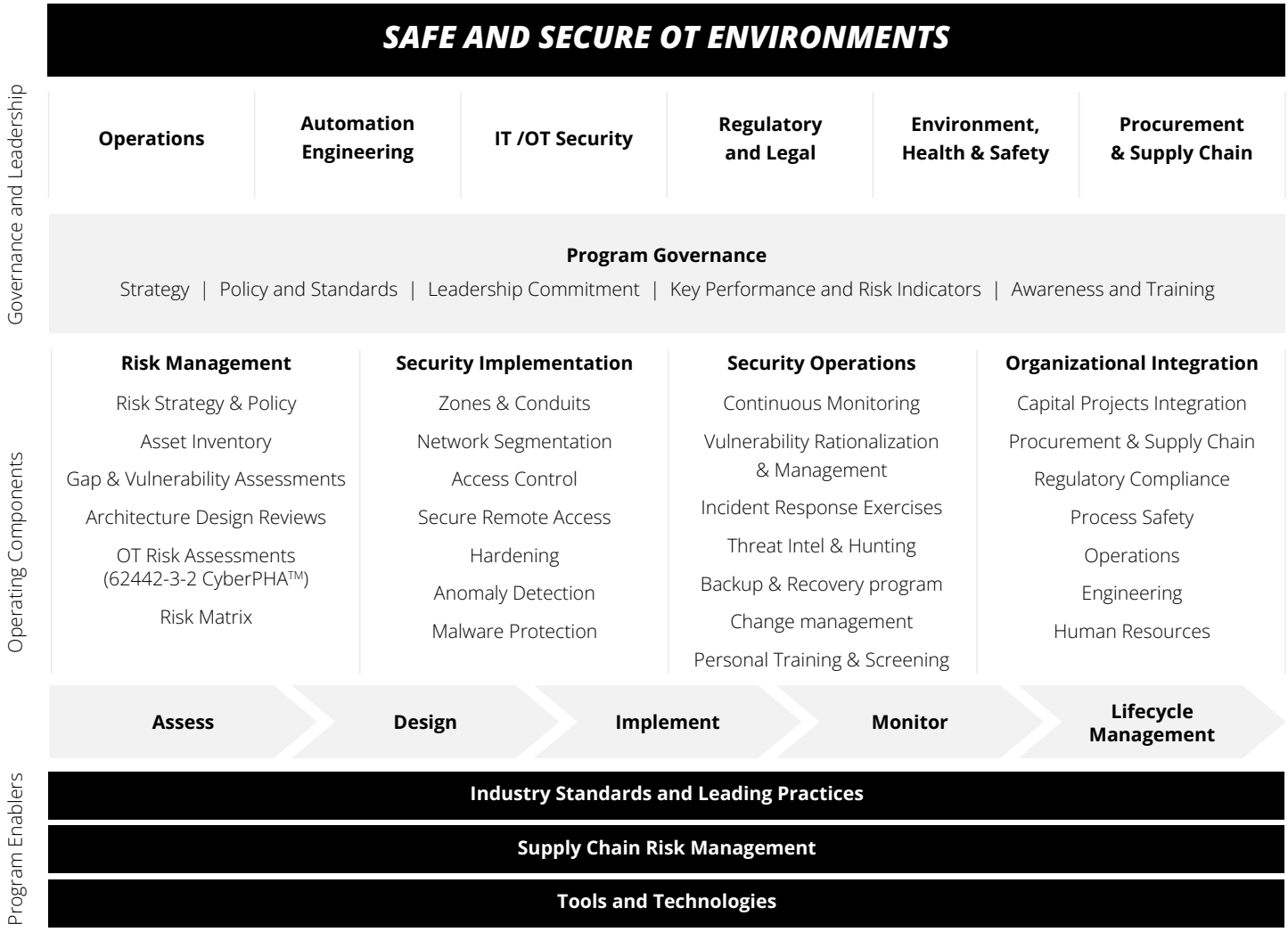
Compliance adherence

Organizations can achieve alignment with regulatory frameworks and reduce the risk of noncompliance penalties.

Operational safety

Vulnerability assessments can improve both cybersecurity and the physical protection of OT environments by identifying risks to critical control systems.

Deloitte's OT Security and Privacy Program provides a broad framework that incorporates the OT security life cycle.



5.3
VULNERABILITY RATIONALIZATION

5.3.1
SOLUTIONS

Through OT vulnerability rationalization studies, Deloitte leverages Cyber PHA and alarm rationalization methodologies to prioritize vulnerabilities based on operational impact and risk severity. This can result in:

- **A risk-based approach** to vulnerabilities—guided by likelihood, impact, and business context—to determine when to **treat, tolerate, terminate, or transfer** risks.
- **Streamlined resource allocation** to focus on high-impact vulnerabilities first.

5.3.2
WHY IT MATTERS

Vulnerability rationalization can enhance efficiency by focusing resources on the highest risk areas, reducing downtime, and increasing protection.

5.3.3
MAIN OUTCOMES

Required resource use

Teams focus on high-impact areas, prioritizing that the most significant high-risk vulnerabilities are remediated efficiently and with optimal resource allocation.

Operational continuity

By addressing high-risk vulnerabilities, potential disruptions can be reduced, allowing systems to operate efficiently.

Reduced attack surface

Continuous rationalization progressively strengthens defenses, limiting opportunities for exploitation.

5.4
OT SECURITY DESIGN AND IMPLEMENTATION

5.4.1
SOLUTIONS

Deloitte provides end-to-end design and implementation services for:

OT network design and segmentation

Aligning with industry frameworks (e.g., NIST CSF, IEC 62443).

System integration

Enabling new security technologies to integrate effectively into existing OT systems.

System hardening

Strengthening OT infrastructure by reducing vulnerabilities and improving system resilience. System hardening refers to the practice of securing a system by reducing its vulnerabilities, applying security patches, configuring settings to minimize risks, and improving its overall resilience to potential threats or failures.

5.4.2
WHY IT MATTERS

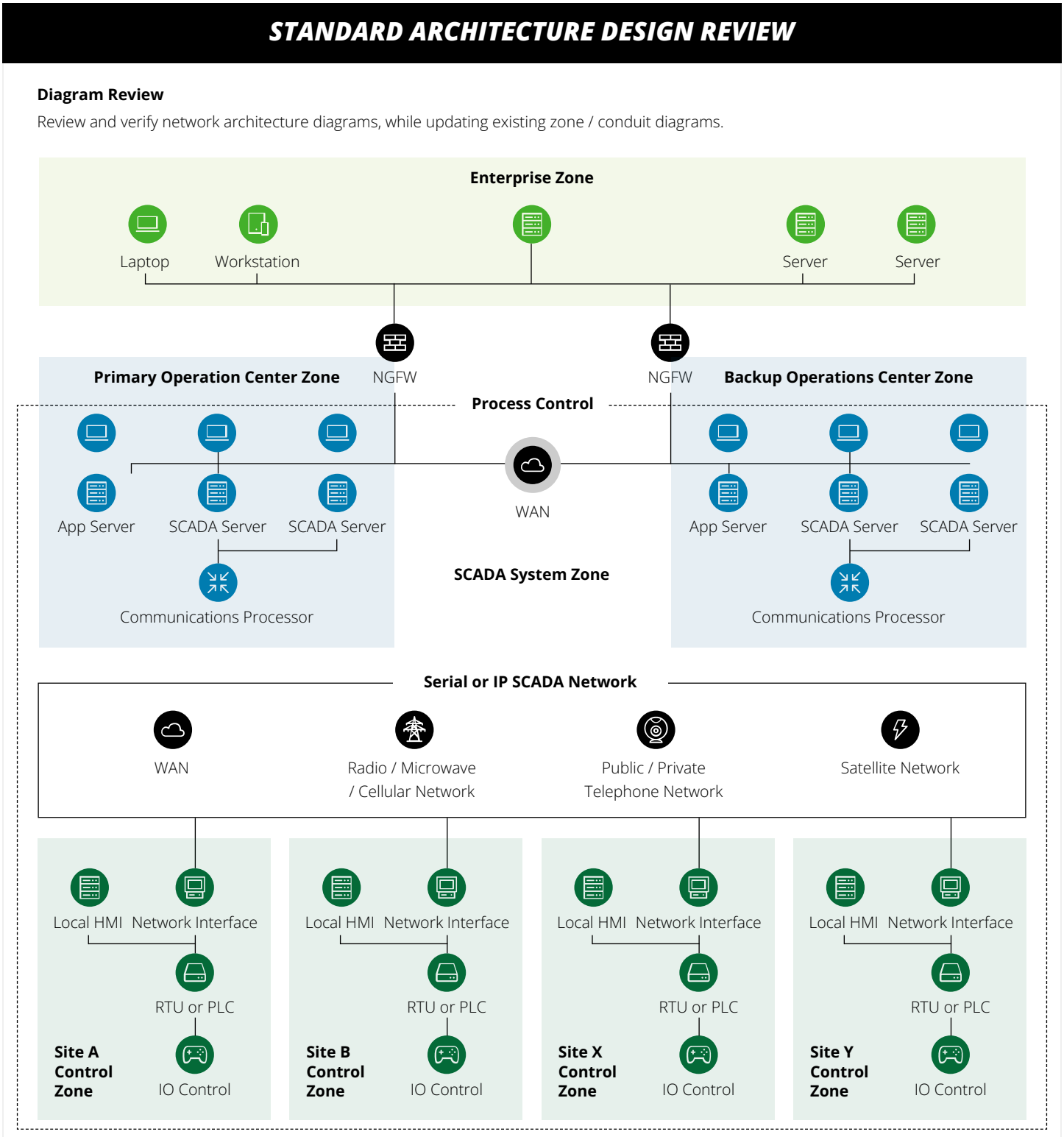
The solutions mentioned above support the implementation of secure-by-design environments where security is built in from the start of the development and deployment process. By embedding security throughout the life cycle, organizations can reduce the attack surface, improve system resilience, and proactively address vulnerabilities before they are exploited. This approach is essential for securing OT environments, as it supports long-term operational stability and protection.

For example, maintaining continuous operations securely may involve routine patching, firmware updates, and implementing role-based access controls. Additionally, to prevent misconfigurations, applying hardened system settings and pre-testing OT components in isolated environments are also core secure-by-design practices.

5.4.3

MAIN OUTCOME

Deloitte's methodology goes beyond a standard diagram review by analyzing and correlating multiple sources of information, leveraging OT tools, and contextualizing the results.



5.5
REGULATORY AND CERTIFICATION READINESS

5.5.1
SOLUTIONS

Deloitte prepares organizations for industry certifications and regulatory reviews by conducting OT assessments that evaluate security posture against:

- ***ISA/IEC 62443***
- ***NIST CSF***
- **Industry-specific regulations** such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP).

5.5.2
WHY IT MATTERS

These assessments can reveal **hidden weaknesses** and potential entry points for cyberattacks, empowering organizations to take proactive steps toward remediation.

5.5.3
MAIN OUTCOMES

Regulatory confidence

Organizations are prepared for checks and reviews. This can reduce the likelihood of fines and penalties.

Competitive advantage

Certification signals to clients and third parties that the organization prioritizes security. This can enhance reputation and business prospects.

Operational alignment

Regulatory compliance frameworks can improve overall security posture. They also can enhance protection and operational efficiency.

5.6
SECURITY TOOL EVALUATION

5.6.1
SOLUTIONS

Deloitte assists organizations in:

- **Generating evaluation criteria** for OT security tools.
- **Vendor selection and technical evaluations** to identify suitable security technologies for companies to select.
- Providing **recommendations** on firewalls, intrusion detection systems (IDS), asset monitoring solutions, and more.

5.6.2
WHY IT MATTERS

Selecting the applicable tools can enable **continuous protection** and reduce the risk of tool misalignment with organizational needs.

5.6.3
MAIN OUTCOMES

Enhanced protection

When implemented properly, the applicable tools can provide broad coverage, effectively reducing vulnerabilities and blind spots. Proper configuration, continuous monitoring, and regular updates help these tools provide consistent protection.

Cost efficiency

Investments are directed toward solutions aimed to provide the high-quality return on security.

Scalability

Tools are selected with growth in mind and are designed to evolve with the organization.

5.7
OT DETECTION TOOL ARCHITECTURE, DEPLOYMENT, AND CONFIGURATION

5.7.1
SOLUTIONS

Deloitte architects and deploys OT detection tools to manage:

- Asset inventory and tracking
- Vulnerability and anomaly detection
- Incident management and reporting

5.7.2
WHY IT MATTERS

Early detection is **important to preventing cyberattacks** from escalating into full-blown operational disruptions.

5.7.3
MAIN OUTCOMES

Proactive defense

Anomalies can be detected before they esclate and can reduce the impact of breaches.

Operational transparency

Continuous monitoring can help organizations maintain full visibility into their OT environments.

Efficient response

Incident management workflows can reduce the time to contain and mitigate threats.

5.8
TRAINING AND UPSKILLING

5.8.1
SOLUTIONS

Deloitte provides OT-specific cybersecurity training, including:

ISA IC32 – Individual Cybersecurity for Control Systems

This course introduces the basics of the ISA/IEC 62443 standards and their application in industrial settings, covering terminology, concepts, and models essential for securing control systems.

Maritime FSO – Cybersecurity for Maritime Operations

This program provides specialized training designed for the maritime sector including shipping, ports, offshore platforms, and related infrastructure. The focus is on cybersecurity practices relevant to maritime operations.

Customized programs

This initiative develops and delivers OT-specific cybersecurity training. Courses range from general awareness to in-depth technical instruction tailored to meet the unique needs of various industry environments.

5.8.2
WHY IT MATTERS

A well-trained workforce can be the **first line of defense** against cyberattacks.

5.8.3
MAIN OUTCOMES

Reduced human error

Staff can detect and respond to threats effectively and reduce vulnerabilities caused by oversight.

Enhaned resilience

Teams are prepared to handle incidents with confidence and reduce operational disruptions.

Cultural shift

A focus on training can promote a security-first mindset across the organiation.

5.9
OPERATE/MANAGED SERVICES

5.9.1
SOLUTIONS

Deloitte offers outsourced managed services that cover:

- **Day-to-day OT security operations.**
- **Ongoing governance and oversight** of OT security programs.

5.9.2
WHY IT MATTERS

Managed services provide **continuous protection, 24/7 monitoring, and experienced oversight.**

5.9.3
MAIN OUTCOMES

Operational continuity

Organizations can maintain uptime even without in-house experience.

Rapid incident response

Continuous monitoring checks that breaches are detected and addressed in near real time.

Cost efficiency

Managed services can reduce the overhead associated with full-time in-house security teams.

CONCLUSION

A FUTURE-READY APPROACH TO OT SECURITY

Palo Alto Networks and **Deloitte** offer powerful and complementary approach to **OT security**. This colaboration can help protect industrial environments and strengthens their resilience.

PALO ALTO NETWORKS: CUTTING -EDGE OT SECURITY TECHNOLOGY

Palo Alto Networks provides **broad, AI-driven security solutions** that can proactively **detect, prevent, and neutralize threats** targeting OT systems. Their **zero trust architecture, automated response, and unified security management** extend across IT and OT environments. This approach enables and broadens protection against evolving cyber risks. By addressing vulnerabilities across **people, processes, technology, and corporate culture**, Palo Alto Networks provides an **adaptive and resilient security framework** that can effectively integrate with existing infrastructure and reduce operational disruption.

Real-time threat detection

AI and ML can drive proactive threat prevention.

Zero trust security

Micro-segmentation and least privilege access can reduce the attack surface.

Effective integration

Solutions can integrate with existing OT and iT environments without major infrastructure changes.

Industry recognition

Palo Alto Networks is consistently recognized as a leader in OT security by Forrester and other analysts.[47]

DELOITTE: STRATEGIC OT GOVERNANCE AND ADVISORY SERVICES

Deloitte's OT security services focus on **governance, risk management, and operational resilience**. By providing **end-to-end security program design, vulnerability assessments, compliance readiness, and managed services**, Deloitte can enable organizations to **align security with business objectives.** Our services help industries such as **manufacturing, energy, health care, and transportation** navigate complex OT environments and adhere to **regulatory compliance** with frameworks like **NIST CSF and IEC 62443.**

Broad assessments

In-depth evaluations can uncover hidden vulnerabilities and align OT environments with regulatory requirements.

Customized programs

Security services can be tailored to the different circumstances of industrial sectors.

Executive engagement and training

Upskilling and governance advisory services can engage and inform leadership.

Managed services

Ongoing monitoring, governance, and day-to-day OT security operations are just some of the managed services available.

Deloitte's OT assessment targets six specific initiatives that can act as drivers to a broad and scalable security program that can yield high-quality returns to an organization's OT risk profile.

01

Establish governance model and cross-functional team

02

Understand existing OT systems & risk

03

Enhance network segmentation

04

Apply Security Hardening

05

Continuous security monitoring and management

06

Enhanced response and recovery capabilities

ENDNOTES

1 Deloitte, "Global cyber executive briefing," March 11, 2020.

2 Erik Peterson, "Achieving visibility and control in OT systems: Remote maintenance, securing remote access, and the zero-trust approach," Cybersecurity & Infrastructure Security Agency (CISA), May 2023.

3 Pro-Tech Systems Group, "Unveiling vulnerabilities: Recent SCADA cybersecurity breaches and their implications," April 2, 2024.

4 Catherine Stupp, "Schneider Electric investigates cyberattack," *Wall Street Journal*, November 6, 2024.

5 Dean Parsons, *ICS is the business: Why securing ICS/OT environments is business-critical in 2024,* SANS Institute, August 28, 2024.

6 Callie Guenther, "Why OT environments are vulnerable—and what to do about it," *SC Media*, December 2, 2024.

7 John Leyden, "OT security becoming a mainstream concern," CSO, October 31, 2024.

8 Guenther, "Why OT environments are vulnerable—and what to do about it."

9 Gourav Nagar, "The evolution of ransomware: Tactics, techniques, and mitigation strategies," *International Journal of Scientific Research and Management (IJSRM)* 12, no. 06, (2024): pp. 1282–98.

10 Keith Stouffer et al., *Guide to operational technology (OT) security*, US Department of Commerce, National Institute of Standards and Technology (NIST), September 2023, p. 9.

11 Zsolt Olah, "Unveiling the dark side: Common attacks and vulnerabilities for industrial control systems," Aon, December 4, 2024.

12 Ibid.

13 Peterson, "Achieving visibility and control in OT systems: Remote maintenance, securing remote access, and the zero-trust approach."

14 Guenther, "Why OT environments are vulnerable—and what to do about it."

15 Nagar, "The evolution of ransomware: Tactics, techniques, and mitigation strategies."

16 Olah, "Unveiling the dark side: Common attacks and vulnerabilities for industrial control systems."

17 Anna Ribeiro, "Growing need to safeguard industrial systems with effective OT cybersecurity programs," *Industrial Cyber*, July 7, 2024.

18 Ibid.

19 Olah, "Unveiling the dark side."

20 Ibid.

21 Nagar, "The evolution of ransomware."

22 Ibid.

23 Parsons, *ICS is the business: Wy securing ICS/OT environments is business-critical in 2024.*

24 Tony Goulding, "Considerations for operational technology cybersecurity," Delinea, accessed May 2025.

25 Ibid.

26 Anna Burrell, "The imperative of IT-OT preparedness in a cyber-vulnerable world," Deloitte, April 27, 2023.

27 Ibid.

28 Michael M. Amiri and Michela Menting, *The state of OT security*, Palo Alto Networks, 2024.

29 Ibid.

30 Ibid.

31 Fortinet, *2024 cybersecurity skills gap*, 2024.

32 Anne Rebeiro, "SANS Institute 2024 survey reveals progress and gaps in ICS/OT cybersecurity for critical infrastructure," *Industrial Cyber*, October 8, 2024.

33 Ibid.

ENDNOTES

34 Rob Hayes, "Managing the successful convergence of IT and OT," Deloitte, 2020; Palo Alto Networks. *Incident Response for Industrial Control Systems*, 2023.

35 Amiri et al., *The state of OT security*.

36 Stouffer et al., *Guide to operational technology (OT) security*, p. 9.

37 Tom Chapman, "Overcoming OT security challenges and complexities," *Supply Chain Digital Magazine*, November 29, 2024.

38 Unit 42, *2023 Unit 42 ransomware and extortion report*, Palo Alto Networks, March 21, 2023.

39 Forrester, *State of enterprise IoT security in North America: Unmanaged and unsecured*, Armis, September 2019.

40 Dino Busalachi, "Bridging the gap between IT and OT to improve industrial cyber security," *Cyber Security: A Peer-Reviewed Journal* 7, no. 4 (2024): pp. 333–41.

41 Stu Sjouwerman, "Train employees and cut cyber risks up to 70 percent," *Security Awareness Training Blog*, Knowbe4, January 18, 2025.

42 Busalachi, "Bridging the gap between IT and OT to improve industrial cyber security,"

43 Fortinet, *2024 cybersecurity skills gap*

44 Parsons, *ICS is the business.*

45 Amiri et al., *The state of OT security*

56 Qiang Huang, "Forrester names Palo Alto Networks a leader in OT security," Palo Alto Networks, June 11, 2024.

THE POWER OF ALLIANCE

By combining Palo Alto Networks' **cutting-edge technology** with Deloitte's **strategic governance, implementation, and managed services**, organizations can gain **360-degree protection** for their OT environments, including:

Operational continuity and uptime

Reduced downtime from cyber incidents

Proactive threat defense

Rapid detection and mitigation of threats

Regulatory confidence

Understand alignment with industry standards and compliance requirements

Future-ready infrastructure

Adaptive solutions that grow alongside evolving threats and technology

For organizations seeking to **protect their OT environments**, the combined experience of Palo Alto Networks and Deloitte provides for **enhanced resilience, operational efficiency, and broad cybersecurity** in the face of rising industrial threats.

AUTHORS

Jane Chung, PhD
Managing Director
Deloitte & Touche LLP
jachung@deloitte.com

Wendy Frank
Principal
Deloitte & Touche LLP
wfrank@deloitte.com

Michael Ganal Maust
Manager
Deloitte & Touche LLP
mganalmaust@deloitte.com

Anthony Polzine
Global Solutions Architect
Palo Alto Networks
apolzine@paloaltonetworks.com