PDI TECHNOLOGIES

SOCaaS Accelerates Your Journey to Predictive Security Operations

security.pditechnologies.com

Table of Contents

PDI TECHNOLOGIES

Introduction

The Journey from Reactive to Predictive Security Operations

The time for reactive security has passed. It can't effectively address sophisticated cyberthreats, evolving threat vectors, and complex technology requirements. Threat actors constantly fine-tune their tactics, techniques, and procedures (TTPs), outpacing reactive security programs and increasing risk.

Over-reliance on frameworks leans into reactivity. Checking 50 or 100 boxes leads some decision makers to believe their organizations are protected. But frameworks aren't lightweight, adaptable, risk-aware, or business-enabled, unlike predictive security operations. Frameworks are essential, but forward-looking decision makers see the urgency in anticipating, preventing, and neutralizing cyber risks before they impact the business.

New thinking prioritizes the move from reactive to predictive cybersecurity. The journey requires the right technology foundation, unified security operations, and an integrated security ecosystem that leverages artificial intelligence (AI). This eBook explores security operations center as a service (SOCaaS) and the role it plays in the future of cybersecurity.

PDI TECHNOLOGIES

Chapter 1
From Standalone Tools to Integrated Ecosystem

Remember the early days? Everything felt fragmented. Tools operated in isolation. Managed detection and response (MDR) identified threats, and endpoint detection and response (EDR) monitored endpoints. Data silos flourished because the tools weren't integrated. Practitioners perfected their techniques for swiveling screen to screen and populating spreadsheets. Teams scrambled to connect the dots and decide what actions to take.

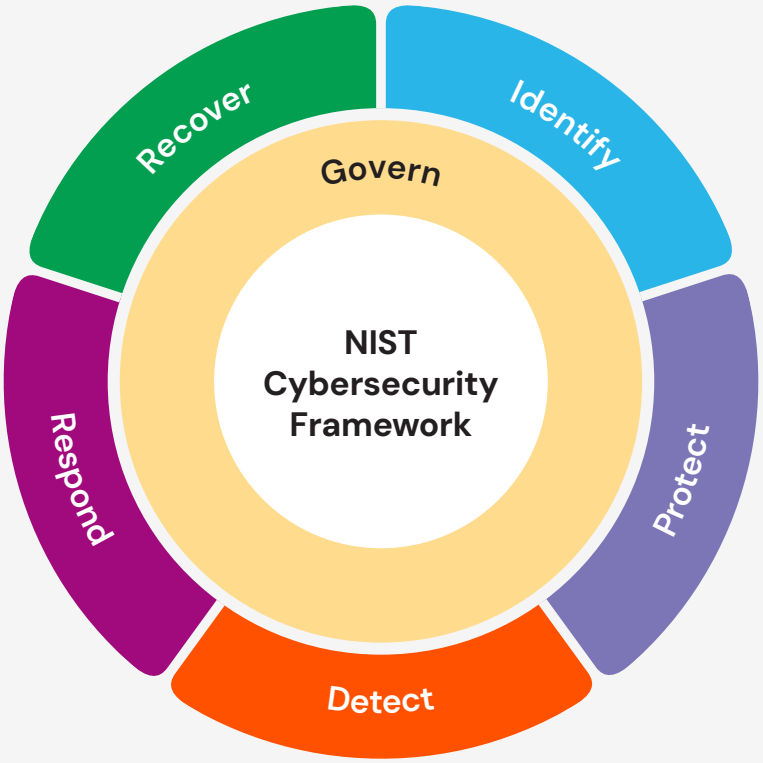
MDR and EDR went on, along with vulnerability management service (VMS) and managed gateway service (MGS), to form the technology foundation that enables modern SOCs. Many organizations tried to call this concept a "fusion center." However, the real evolution of standalone tools into an integrated security ecosystem is the backstory of the synchronized detection and response engine known as SOCaaS.

With businesses increasingly emphasizing proactive cybersecurity measures, the demand for AI-driven SOC is expected to rise, further contributing to the SOC as a Service market growth.[1]

PDI TECHNOLOGIES

The broad ecosystem includes the frameworks that provide necessary security standards and guidance. SOCaaS aligns with the NIST Cybersecurity Framework, ISO 27001/27002, SOC Type 2, PCI DSS, and others. In fact, the automation and orchestration built into SOCaaS make it easier and less time-consuming to maintain compliance.

SOCaaS aligns with the top industry frameworks, including the NIST Cybersecurity Framework.



Chapter 2
Integration Turns Data into Intelligence

SOCaaS integrates and centers MDR, EDR, VMS, and other services in ways that enhance the quality of security work, reduce the risk of technology depreciation, and align with cybersecurity insurance requirements. Think of SOCaaS as a single source of truth that helps to close cybersecurity OODA loops.

Integration turns data into the intelligence that supports predictive security operations. Every tool spews out data that feeds threat hunting, forensic investigations, verification of control failures, and other activities. When the tools talk to each other and/or to the SOC, humans and AI engines collaborate to produce intelligence that ideally considers your industry, organizational type and size, current controls, and risk tolerance. So armed, you can more quickly prioritize what to do—quarantine, evict, apply compensating controls, counterattack, or take another action.

Actionable intelligence elevates security programs:

- Predict threats before they materialize.
- Become threat-hunting experts.
- Demonstrate the value of security investments through visibility and metrics.

Modern MDR

Technologies are evolving faster than ever, raising questions about CapEx versus OpEx. The history of MDR demonstrates a steady progression.

"The inability to write code and integrate security tools internally is the reason many companies fail at being proactive in detection and response."
—J.R. Cunningham, Chief Security Officer, PDI Technologies

The Risk Equation

Security information and event management (SIEM) logs → Log management → Monitoring → Detection → Response → Intelligence

Chapter 3
Predictive Defense Anticipates and Neutralizes Threats

The integration and orchestration within SOCaaS enable predictive defense. Certain SOCaaS capabilities help to shut down cyberthreats before they cause harm:

24/7 expert monitoring and analysis

SOCaaS forms the backbone of an intelligent security ecosystem that goes far beyond monitoring. It raises the bar with a product-agnostic approach and experts capable of closing in on error-free services.

Integrated threat intelligence

Integration, which brings automation and repeatability to threat hunting, enables breadcrumb trails. A well-integrated SOCaaS enables precise threat hunting across technology platforms; in multi-tenant, cloud, and on-premises environments; and within industries in which particular threat actors specialize.

Unified security operations

A unified, comprehensive view simplifies security management. With less complexity, practitioners can collaborate more easily and act sooner.

Coordinated response capabilities.

Coordination leads to timely, efficient detection, analysis, prioritization, and response. Coordinated capabilities may include incident management, real-time sharing of threat intelligence, automated responses, and reviews to identify lessons learned.

SOCaaS is more than a security program upgrade. It's a fundamental change in how you think about and deploy cybersecurity defense. An AI-powered ecosystem comes with eyes and ears that never sleep.

PDI TECHNOLOGIES

Chapter 4
Old Versus New Cybersecurity Thinking

Certain cybersecurity challenges persist—lack of visibility, resource constraints, operational inefficiencies, and emerging threats. They likely will intensify. How will your security program cope?

Old thinking anchors you in reactionary mode. You keep doing what you're doing. Perhaps this means throwing more tools at the problem. Or taking the path of least resistance, which might be the status quo or trusting in "wait and see." Or feeling overwhelmed every day. Old thinking increases vulnerabilities and risk because the threat actors, technologies and processes continue to change.

New thinking centers on AI-driven intelligence derived from normalized data located in one place. Centralized data allows automation and orchestration to streamline every aspect of SecOps. New thinkers ponder questions such as:

- How do we adapt traditional technology buying cycles and depreciation schedules to the current pace of cybersecurity?
- How can we connect our tools intelligently?
- What is the ideal way to transform data into foresight and alerts into action?
- How do we reduce the noise when an attack is real?
- What changes to our security program will demonstrate that it's a strategic asset and not a cost center?

Tips to Advance New Thinking

- Share knowledge about software development that supports integration.
- Talk about strategies for modernizing your tech stack.
- Evaluate and buy only tools that have built-in APIs.
- Discuss the wildly different motions required in cloud and on-premises environments.

Cybersecurity Trends to Watch

- Use of AI, machine learning (ML), and generative AI (GenAI) to close the cyberskills gap and to augment detection, response, and prediction
- Security of IoT devices
- Evolution of TTPs
- Increase in cyberattacks, particularly ransomware and phishing
- Greater adoption of cybersecurity insurance—the policies typically require 24/7 SOC coverage
- Reliance on metrics to help prove the value of cybersecurity investments
- The geopolitical landscape (global conflict, trade)
- Big-tech and societal trends

PDI TECHNOLOGIES

Chapter 5
On the Road to Predictive Security

Security programs pass through maturity stages: technology-centric, compliance-driven, threat-aware, and risk-based. Ideally, programs mature to the point where security discussions are primarily about the business and risk, not technology. Risk-based security operations are grounded by AI-driven predictive intelligence, which speeds up inferences, connections, and decisions.

Maturing your security program won't happen overnight, but adding risk assessment to any stage will expedite your journey. Generally, risk-based discussions span topics such as:

- Who you are as a business
- How you generate revenue
- What's at risk, whether assets, reputation, revenue, etc.
- Who are the bad actors and how they operate
- What controls are in place to stop a threat
- What controls need to be put into place to stop a threat and/or reduce risk

Decisions about individual threat situations call for specificity and precision. A risk equation facilitates risk calculation without straying into technical minutiae. The equation identifies the assets to be protected along with the threat, the vulnerability, and the countermeasure(s). For example, X threat at X time is using X technique for X purpose, and recommendations include X controls and/or process changes.

Security Program Maturity Stages

- **Technical/ infrastructure-centric.** Problems are solved mainly with technology.
- **Compliance-driven.** Regulations drive security decisions.
- **Threat-aware.** Gaps in security controls and/or industry-standard frameworks trigger actions.
- **Risk-based.** Predictive intelligence drives priorities that are aligned with business needs and risk tolerance.

Calculate Risk Using a Risk Equation

A standardized approach to risk assessment helps to clarify risk tolerance and determine where to focus resources. The risk equation facilitates conversations about risk, investments, threats, vulnerabilities, assets, and countermeasures. It emphasizes the totality of risk, not individual controls or technical issues.

Risk =  ×  ÷ 

NACD Critical Questions

What are our critical assets? (What do we use the risk equation against?)

Threat

Who are the bad guys?

How would they compromise us?

Vulnerability

Where are we exposed?

What do our weaknesses look like to the treat actors?

Countermeasures

What defenses do we have in place to stop a threat or mitigate a vulnerability?

Are our defenses working?

Chapter 6
Moving Forward with AI

The AI boom is happening worldwide. Not embracing it is worse than standing still. Without AI, your security program slides backwards.

AI's top strengths are integrating technologies, connecting tools, and automating workflows. It is transforming activities such as threat detection, threat hunting, behavioral analytics, automated incident response, vulnerability management, and security orchestration. Old thinking may discount AI. New thinking views AI as a powerful, necessary human assistant.

With help from AI, practitioners work efficiently and precisely, whether it's sifting through big data, eliminating noise, identifying anomalies, analyzing historical trends, forecasting threats, or completing other tasks. AI enables the predictive intelligence that modernizes your security program:

- Transform threat detection from a series of alerts into an intelligent early warning system.
- Convert raw security data into a strategic advantage.
- Build a unified defense that evolves as fast as the threats it faces.

> One of the challenges in cybersecurity is the high volume of indicators, a lot of which can be false positives. AI-pushed structures use behavior analysis and system studying algorithms to clear out and prioritize signals, ensuring that only credible threats are flagged for human analysts. This notably reduces noise and permits protection groups to focus on genuine problems.[2]

Invite AI Discussion

- In which areas of our security program can AI assist practitioners to improve efficiency and reduce risk?
- What are the integration options for workflow/ticketing systems and a large language model?
- How do we develop training requirements and refine prompt engineering?
- Which mechanisms or processes prevent hallucination?
- How do we balance privacy and security using AI-driven systems?

Conclusion

The future starts tomorrow. Speed counts against the bad guys, and SOCaaS accelerates your access to predictive, unified security operations.

An intelligent, integrated ecosystem, SOCaaS is built on the technical foundation of services such as MDR, EDR, VSM, and MGS. SOCaaS solutions powered by AI are laser-focused on one goal: to turn the tables on threats before they materialize. Pre-emptive actions bolster protection and reduce risk.

Learn more about SOCaaS, risk management, and the risk equation by talking to one of our experts. Alternatively, to review an example of how to use the risk equation, check out the Managing Risk eBook.

The PDI Cybersecurity Platform

SOCaaS delivered by PDI is implemented within the PDI Cybersecurity Platform, which combines the latest technology, human expertise, and advanced AI. The platform includes:

- Technology-agnostic integration
- Customizable dashboards
- An AI assistant
- Industry-specific threat intelligence
- Unified visibility
- Data-driven insights and recommendations
- A mobile app for on-the-go management

PDI TECHNOLOGIES

SOCaaS Evaluation Checklist

SOCaaS is a cost-effective alternative to building and maintaining an in-house SOC, considering persistent industry challenges. SOCaaS offerings, however, vary in their levels of AI, ML, automation, and orchestration, all of which are critical to predictive security. Ask providers to explain current and future capabilities, starting with these components:

- Continuous protection against cyberthreats with 24/7 monitoring and response
- Up-or-down scalability to address changing organizational needs
- Mechanisms to help organizations meet compliance standards efficiently
- An AI large language model that is built specifically for security purposes
- Highly accurate detection methods that reduce noise related to false positives
- Enriched decision support intelligence with a tool that accelerates data gathering and reconciliation from different devices and answers questions about compliance with a particular policy or standard

References

[1] Fortune Business Insights, SOC as a Service Market Size, Share and COVID-19 Impact Analysis..., December 16, 2024. https://www.fortunebusinessinsights.com/soc-as-a-service-market-108879

[2] Business Research Insights, SOC as a Service Market Size, Share, Growth and Industry Analysis..., December 16, 2024. https://www.businessresearchinsights.com/market-reports/soc-as-a-service-market-117570

About PDI Security and Network Solutions

With over 25 years of expertise, PDI Security and Network Solutions (formerly known as Nuspire) is redefining cybersecurity and network management through intelligent unification and unparalleled protection. The company delivers fully managed security and network services, including managed detection and response (MDR), endpoint detection and response (EDR), Firewall as a Service, 5G as a Service, and Wi-Fi as a Service. This technology-agnostic platform seamlessly integrates human expertise, advanced AI, and cutting-edge technologies, providing holistic visibility across security and network infrastructure. PDI's 24x7 SOCs and expert teams enable organizations to stay ahead of emerging threats while optimizing investments.

PDI TECHNOLOGIES

security.pditechnologies.com

LinkedIn @pdisecurityandnetworksolutions