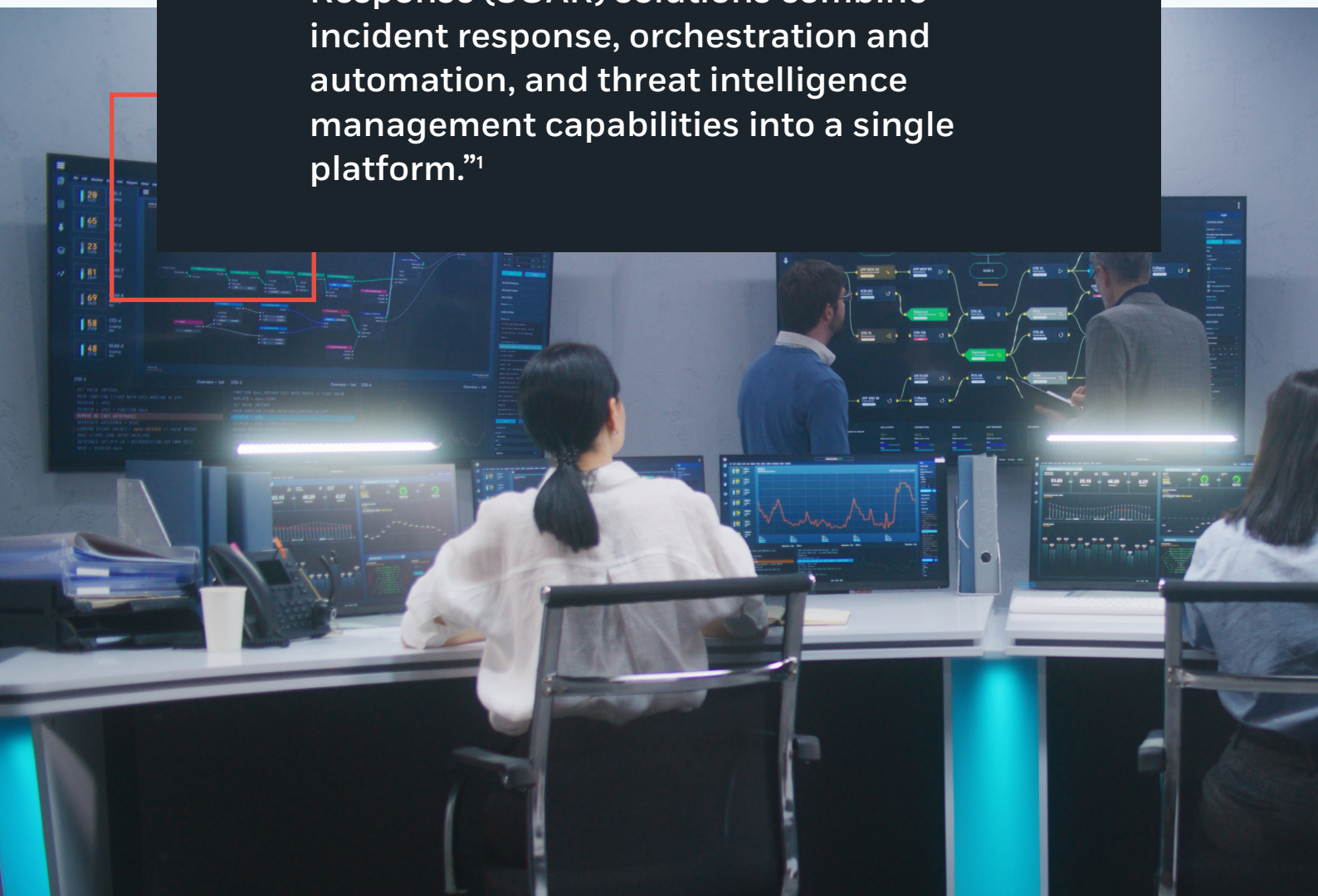
CyberProof®
A UST Company

Better Security, Together.

The Top 5 Benefits of SOAR Implementation

What is SOAR?

> Security Orchestration, Automation and Response (SOAR) solutions combine incident response, orchestration and automation, and threat intelligence management capabilities into a single platform."[1]



Cybersecurity has never been as challenging as it is today, and security leaders are juggling more concerns than ever before. Four million professionals are needed to close the global cybersecurity skills gap , and with increasing costs and shrinking budgets — 73% of security experts have missed, ignored, or failed to act on a critical alert. Many organizations are relying on dozens of security point products, and with a lack of integration between these products, and threat actors increasingly leveraging AI to launch sophisticated attacks, visibility and control is often impossible.

Driven by these challenges and more, the need for SOAR has risen to the top of the organizational agenda. Breaking it down, SOAR is made up of three key elements:

Orchestration

Connecting the dots between disparate tools and siloed or distributed data, and collating and operationalizing threat intelligence.

Automation

Establishing customizable workflows, playbooks and processes, and automating triggers to augment human analysts and add consistency to operations.

Response

Improving response time through automated detection, investigation and response, as well as storing incident management data to support incident response.

[1] Gartner, SOAR Solutions
[2] WeForum, Cybersecurity Skills Shortage 2024
[3] Security Magazine, June 2024

Top 5 Business Benefits of SOAR

1 Enhanced Orchestration and Integration

On average, organizations use 80 security tools to manage their environment. [4]

By integrating with a wide array of security tools and systems, organizations can ensure that all of their components work well with one another — working together harmoniously to reduce the complexity of monitoring and response, adding visibility, and limiting alert fatigue and data deluge.

2 Increased Efficiency through Automation

SOC teams spend 32% of the day on incidents that pose no threat. [5]

An intelligent SOAR solution can reduce the time spent on investigations down from hours to seconds, automating repetitive and manual tasks which steal time and focus. Analysts can focus on more strategic activities such as threat hunting and proactive defense, dramatically improving Mean-time-to-Detect and Mean-time-to-Respond.

3 Improved Incident Response Times

Organizations that leverage AI and automation see a data breach lifecycle that is 108 days shorter than those who do not. [6]

A cornerstone of SOAR is automated playbooks and workflows, which support faster triage, investigation, and resolution of a wide range of security incidents. By responding to threats with automation, both speed and accuracy can be prioritized, which means time to remediation is greatly reduced.

4 Ultimate Scalability and Flexibility

The number of organizations that maintain minimum viable cyber resilience is down 30% in 2024 [7]

SOAR solutions are designed from the ground up to scale alongside an organization as use cases grow over time. This includes horizontally (the number of server instances) and vertically (the amount of hardware resources). This supports increasingly complex security environments as well as an increase in data volume and data load.

5 Optimized Reporting and Collaboration

58% of CISOs struggle to communicate to senior leadership in a way that they will understand [8]

Detailed performance metrics and reporting capabilities quantify the benefits of SOAR aligned with customizable business objectives including reduced analyst hours, cost savings or improved Mean-time-to-Respond. To enhance collaboration and shared responsibility, SOAR supports shared resources, playbooks and best practices.

---

[4] Microsoft, 2023 | [5] Morning Consult Report 2023, Security Intelligence | [6] IBM, Cost of a Data Breach 2023 | [7] WEF, Global Cybersecurity Outlook, 2024 | [8] FTI CISO Redefined Study, 2024

CyberProof®
A UST Company

Better Security,
Together.

About CyberProof

Fortify your enterprise with cloud security transformation. CyberProof, a UST company, helps enterprises migrate to cloud-native security operations with advanced Managed Detection & Response services that allow you to protect, detect, and respond to new and existing cyber threats faster and more effectively. Our team of nation-state trained experts together with our AI virtual assistant SeeMo challenge the status quo in the cybersecurity industry with a risk-based approach that helps mitigate the potential threat to your business. Our mission is to empower your organization to anticipate, adapt, and swiftly counter cyber threats – with our global security operations centers, in-depth expertise, and a portfolio of services including Tailored Threat Intelligence, Advanced Threat Hunting, Use Case Management, and more. See: www.cyberproof.com