Solution Brief: Shield 24x7 SOAR Capabilities

SOAR Solutions in 2023

SOAR (Security, Orchestration, Automation, and Response (SOAR) solutions burst onto the market in 2015 and helped teams leverage the massive telemetry they started collecting in the cloud age. The market quickly matured and SOAR solutions by the big SIEM vendors became big license options and some early point solutions appeared. Many SOAR implementations failed due to their complexity and the number of integrations required to make them work seamlessly across attack surfaces, infrastructure and silod teams.

The best SOAR solutions are either native to a modern platform or easily and affordably configured and coordinates and automates tasks in response to threat indicators, incidents or alerts. It enables organizations to not only react swiftly to cyberattacks, but also monitor, analyse, and prevent future threats, thus enhancing their overall security posture.

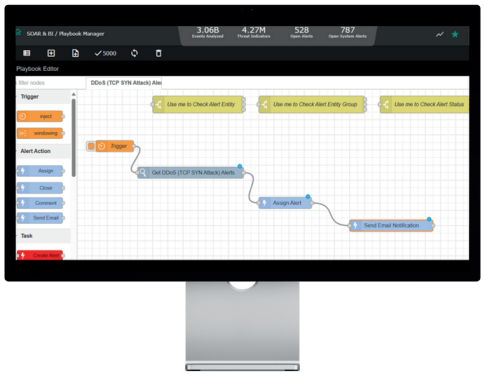
Shield 24x7's Platform Includes Native SOAR Capabilities Powered by AI

Shield 24x7 is a leading provider of AI/ML Powered SIEM and XDR solutions that feature AI-powered Security Operations and Response (SOAR) capabilities the enable your teams to automate and streamline your security operations program. With Shield 24x7, you can leverage smart and intelligent AI to detect, analyze, and respond to threats faster and more effectively. Whether you need to protect and detect threats in your on-premises, cloud, network, endpoint, or IoT devices, Shield 24x7's platform is able to ingest and automate a response.

- Shield 24x7's SOAR capabilities leverage automation and AI to detect and respond to cyber threats
- Artificial Intelligence and Automation: key technologies that enable faster and more accurate threat detection and mitigation
- Shield 24x7's SOAR capabilities can be configured to alert, and block quarantine, threats with an automated action or manual step. It features pre-built responses, a drag-and-drop playbook builder and complete visibility and audit logs into the actions it takes.

Key Benefits of Native SOAR Integration

A comprehensive security platform with native SOAR capabilities helps improve security operations by:



- Automating repetitive tasks and workflows that otherwise require manual intervention and coordination.
- Integrating various security tools and data sources to provide a unified view of the threat landscape and the incident response process.
- Enabling faster and more consistent detection, analysis, and remediation of security incidents across the organization.
- Enhancing collaboration and communication among security teams and stakeholders, as well as facilitating knowledge sharing and best practices.
- Measuring and improving the performance and effectiveness of security operations with metrics and reports.

Key SOAR Deliverables Teams Are Reporting

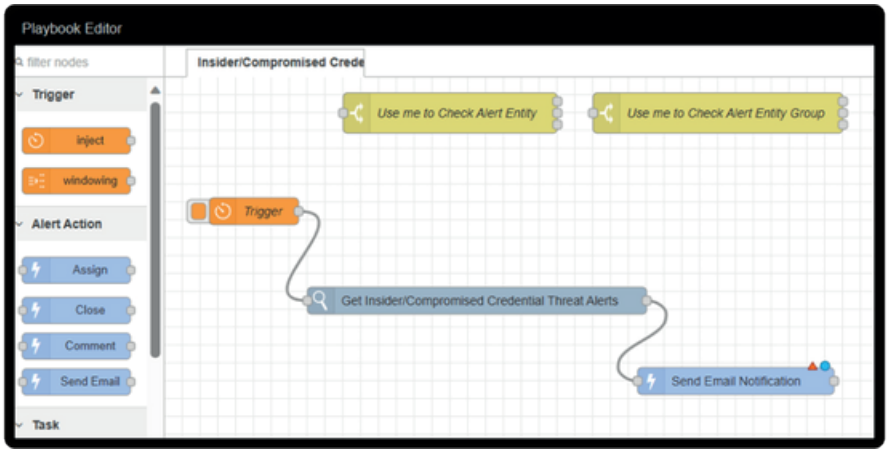
- Optimized case management processes by prioritizing urgent and complex issues
- Efficiencies with opening and closing incident tickets with templates and automated responses
- Ability to investigate and resolve incidents by following best practices and documented platbooks
- Teams are able to use the MITRE ATT&CK framework to correlate events and map their playbooks to attack types
- Find hidden attacks by linking related events
- Discover new connections among known events
- Achieve faster and more effective security response by automating alert qualification and remediation
- Reduction in MTTD and MTTR from months or weeks to minutes
- Improved es security posture and efficiency by streamlining workflows and processes

Shield 24x7 SOAR use cases to modernize you SOC/MSSP/MSP operations to highest level

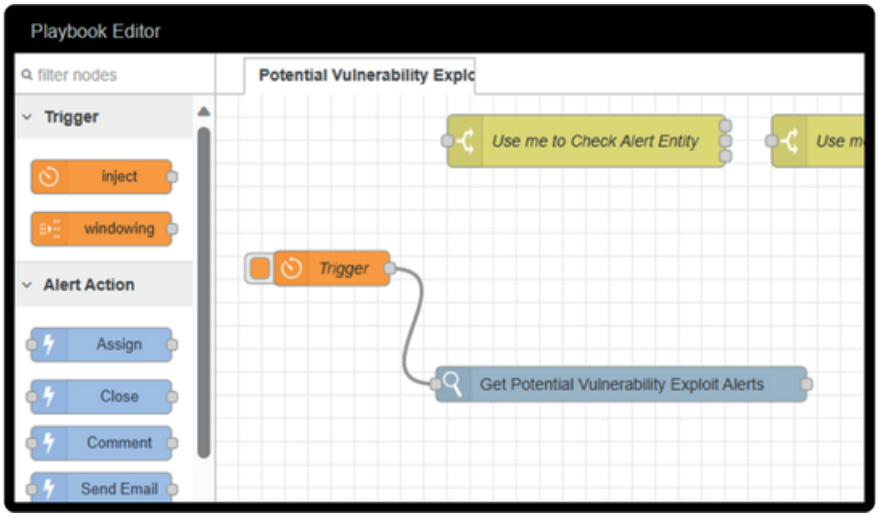
1.Threat Hunting
2.Case Management
3.Threat Intelligence coordination automation
4.Vulnerability Management
5.Automated Phishing Attacks Investigation Analysis & Response
6.Automated Remediation
7.Incident response
8.Security Orchestration and response
9.Forensic Investigation
10.Automated alert triage and enrichment
11.Endpoint malware mitigation
12.Automated phishing investigation and response
13.Handling alerts related to malicious network traffic.

Use Cases Continued

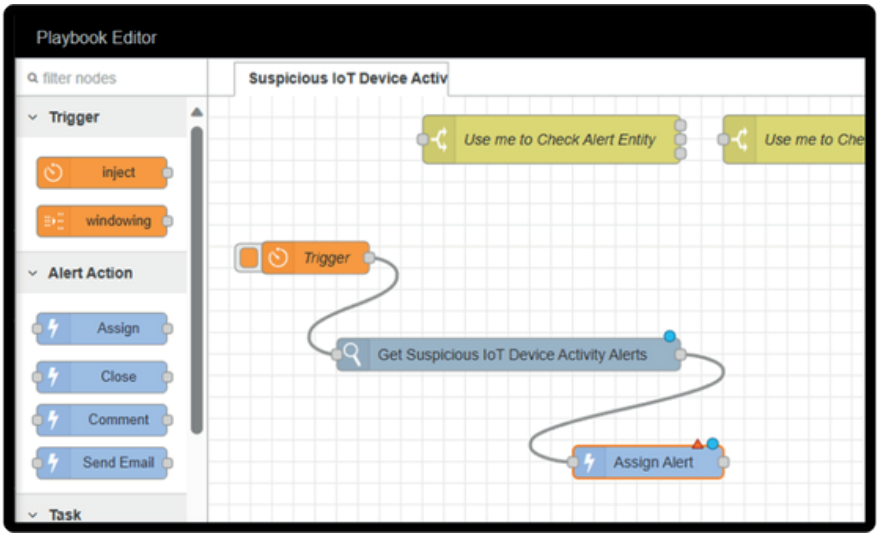
14.Protecting endpoints
15.Managing vulnerabilities
16.Stopping phishing attacks
17.Managing SSL certificates
18.Investigating failed user logins
19. Hunting compromised indicators
20. Analyzing malware
21. Trojan Horses
22. Drive-by Attacks
23. XSS Attacks
24. Eavesdropping Attacks
25. Birthday Attack
26. SQL Injection Attack
27. Man-in-the-middle (MITM) types of cyber-attack
28. Whale-phishing Attacks
29. Spear-phishing Attacks
30. Password Attack
31. URL Interpretation
32. DNS Spoofing
33. Session Hijacking
34. Botnet Detected
35. Compromised Credentials
36. Web Attacks & Exploits
37. Malware Attack
38. Potential Web Exploit
39. Suspicious Login
40. Potential Web Exploit
41. Suspicious Login
42. Potential Malware Infected Host
43. Brute Force Attack
44. UDA - blacklisted site access



45. Insider/Compromised Credential Threat

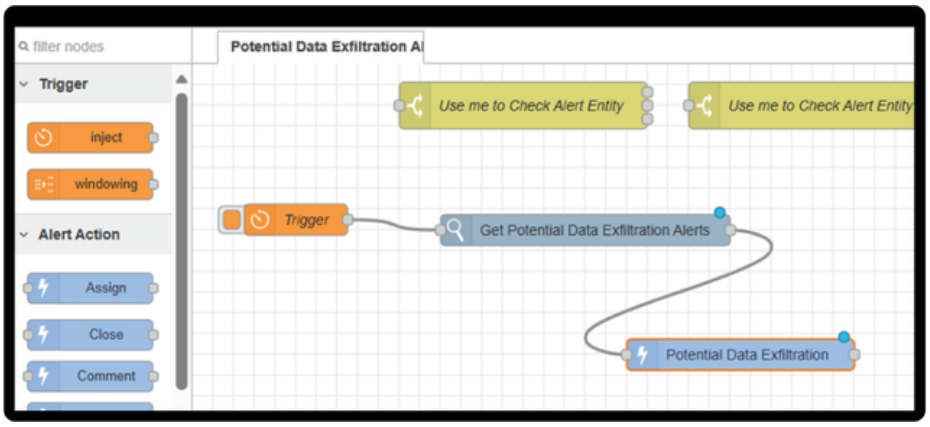


46. Potential Vulnerability Exploit

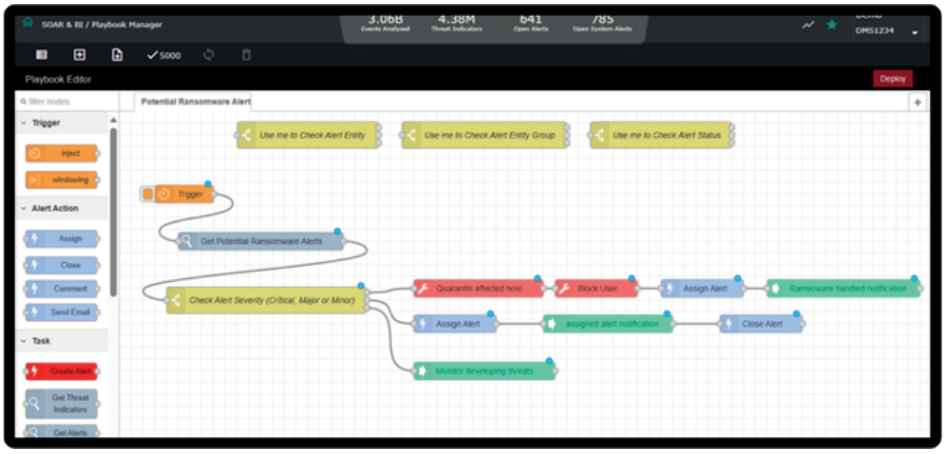


47. Suspicious IoT Device Activity

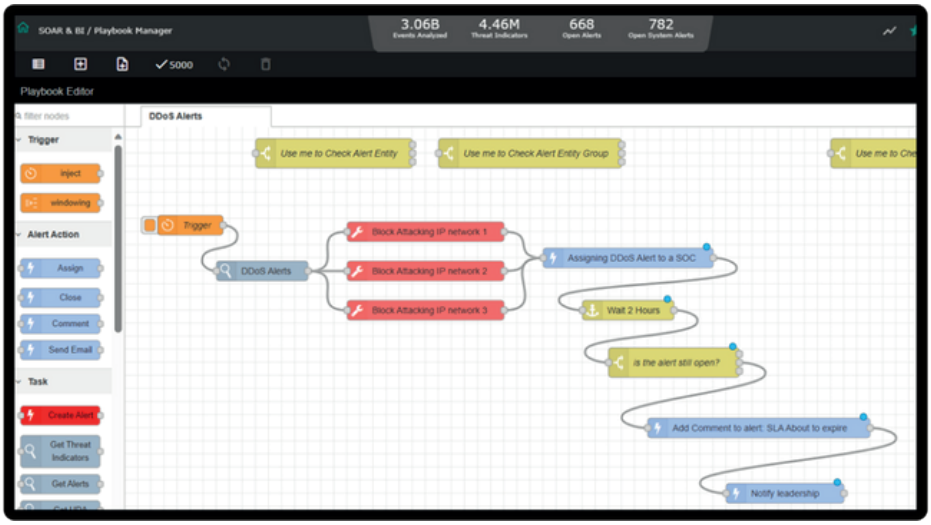
Use Cases Continued



48. Potential Data Exfiltration



49. Ransomware Attack



50. ICMP DoS and DDoS Attack

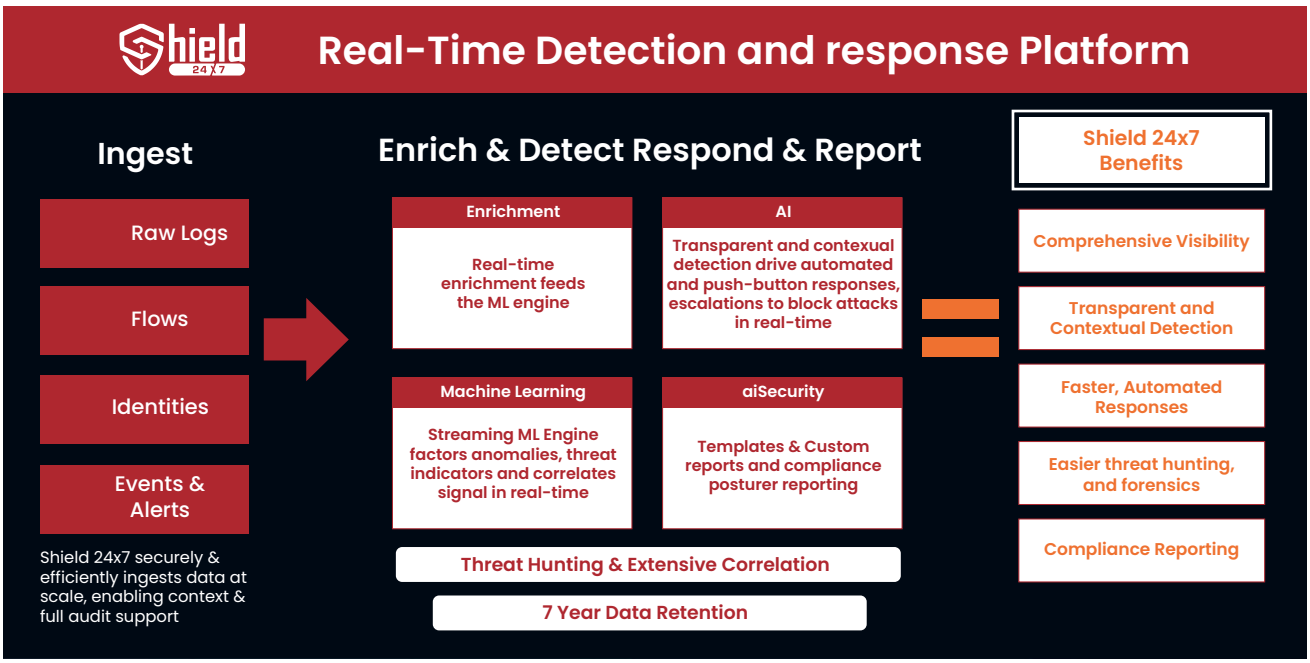
Shield 24x7 Consolidates Your Security Stack

"Modernizing Cybersecurity for the Digital-Era" Consolidating Security Stacks and Reducing Risks with the AI/ML-Powered Cybersecurity Platform by Shield 24x7

One of the most fundamental choices a successful SOC or managed services provider makes is the stack they use to run their security program. And the most fundamental component of any stack has always been the SIEM. SOC teams and MSSPs fully understand this, and for years many MSPs have avoided a SIEM as legacy SIEMs built a reputation as giant logs databases that required expert security analysts and incident responders to manually query and and automate responses from.

Legacy SIEM and their new incarnation as "Next-Gen SIEM" - continue to add weight and cost to a team without truly adapting to today's zero-day threat world and expanding attack surfaces. Most SIEM platforms still offer SIEM as an optional license. Many never fully realized the power of AI/ML to automatically detect and respond to threats in real-time.

And today, as more SOC teams and managed service providers search for newer ways to tackle the core challenges of reducing mean time to detect and mean time to respond, the only modern choice is an integrated SIEM with SOAR capabilities



Shield 24x7 Platform Benefits Summary

Shield 24x7 Enables Response Automation With Your Existing Solutions

Sample Integrations Include:

Visit https://www.Shield 24x7.com/intigrityshield-connectors/
to see complete list

About Shield 24x7

Shield 24x7 reduces cyber threat risks and security stack complexity while significantly improving the ability to detect and block threats and breaches at scale. Shield 24x7's Open Threat Management (OTM) platform enhances and automates security with our AI and ML-powered aiSIEM and aiXDR solutions. The platform provides comprehensive coverage by collecting telemetry from logs, identity management systems, networks, endpoints, clouds, and applications. This data is enriched and analyzed in real-time using threat intelligence, AI and ML models based on behavioral analysis, and correlation engines to generate reliable and transparent detections and alerts. Shield 24x7 supports over 8,000 clients by delivering high-margin, efficient security services with automated cyber threat remediation and continuous compliance.

Learn more about Shield 24x7 SOAR

Schedule a Demo