

SOAR INTEGRATION

Automate Response Workflows with SOAR Integration

Containing every incident before it interrupts the business.

Many security teams already have the detection they need. The gap is what follows the alert: enrichment, approvals, containment, ticketing, and evidence still pass between tools and people by hand, so response speed depends on the shift, the analyst, and the size of the queue.

Security orchestration, automation, and response (SOAR) integration closes that gap. It connects detection, identity, endpoint, and IT operations tools through governed workflows that run the same way every time, and it gives analysts back the hours that routine triage consumes.

How SOAR Automates the Incident Response Lifecycle

● Detect, triage, and enrich

Alerts are notified from security information and event management (SIEM), endpoint detection and response (EDR), email security, identity, and cloud tools. Playbooks correlate related signals into one incident, merging duplicates and separating isolated alerts from developing threats. They then score each incident against asset criticality, threat reputation, and observed behaviour, and enrich it with user identity, endpoint telemetry, and threat intelligence before an analyst opens the case.

Alert

Correlate

Score

Enrich

Approve

Contain

Remediate

Recover

Record

● Contain, remediate, and recover

Once an incident is validated, playbooks coordinate action across security and IT tools: isolating a compromised endpoint, blocking a malicious IP address, or suspending an affected account. Remediation follows approved workflows, so corrective steps are complete and consistent. Recovery restores systems to a secure operating state through credential resets, integrity checks, and post-incident verification, and every step is recorded in an auditable trail.

WHAT CHANGES WITH SOAR INTEGRATION

Response runs the same way on every shift.

Correlated evidence reaches the analysts.

Every action is recorded and auditable as it happens.

Practices for Building SOAR Playbooks That Perform in Production

These practices keep automated workflows consistent and aligned with how the security operations centre (SOC) works.

- 01 Start with frequent, low-complexity incidents.** Phishing reports, malware alerts, and suspicious sign-ins occur often and follow predictable patterns, so they are quick to standardise and validate. A phishing playbook can extract URLs, check their reputation, and close low-risk reports without an analyst opening them.
- 02 Define triggers, decision points, and success criteria first.** Before deployment, state the event that starts each playbook, the severity and business-impact thresholds that route each case, and the outcome that counts as success.
- 03 Standardise enrichment across incident types.** Draw context from the same identity, endpoint, and threat intelligence sources every time. Each endpoint alert, for instance, arrives with user identity, device risk score, and recent sign-in activity, so analysts decide from the same evidence on every case.
- 04 Place approval gates before disruptive actions.** The playbook gathers the context and recommends a response; an analyst approves actions such as deactivating an account or isolating a system from the network. Response is fast, and accountability stays with team.
- 05 Connect security actions to IT remediation.** Integrate SOAR with detection tools, security controls, and IT service management platforms. When an incident is confirmed, the playbook opens a service ticket and starts endpoint remediation, with no manual handover between security and IT teams.
- 06 Measure what automation changes.** Track mean time to respond (MTTR), alert reduction rate, escalation rate, and playbook success rate. Reviewed regularly, these metrics show which playbooks need refinement and which processes need more automation.

SOAR Integration Inside One Connected Framework

As alert volumes increase and response timelines get shorter, SOC teams need faster and more controlled response processes. iStreet SIEM++ integrates with SOAR to support this. It uses AI to correlate alerts, assess risk, and prioritise incidents across existing security tools without changing current workflows. SOAR workflows can start with a prioritised incident instead of individual alerts. The same integration also helps connect detection, investigation, and response across iStreet's cyber security and resilience capabilities, enabling a more coordinated and governed SOC response.

Secure by design

Alerts are correlated, risk-scored, and summarised before response, with governance built into automated actions.

Operating at scale

The Resilience Operating Centre gives security and IT teams a unified view across AIOps and AI-native security operations.

Govern with assurance

Approval controls and recorded actions maintain a clear audit trail for governance and reporting.

Why iStreet Network

As Bharat's digital economy expands, enterprise security environments are becoming more complex, interconnected, and exposed to a growing volume of threats and alerts. iStreet SOAR helps security teams move beyond manual and fragmented response toward coordinated, automated, and governed security operations. The response journey progresses from correlating alerts and understanding incident context to prioritising risk, orchestrating actions, and automating repeatable workflows with human oversight where required.

iStreet Network Limited is an enterprise-grade AI-native platform ecosystem. At its core is Sanjeevani of AI™, iStreet's AI Center of Excellence and integrated framework, bringing together AI-native SecOps, observability, resilience, governance, risk, and compliance. Within this ecosystem, SOAR serves as the response orchestration layer, connecting detection, investigation, decision-making, and governed action across the security lifecycle.

Shift security response from manual processes to governed automation.

contact@istreetnetwork.com