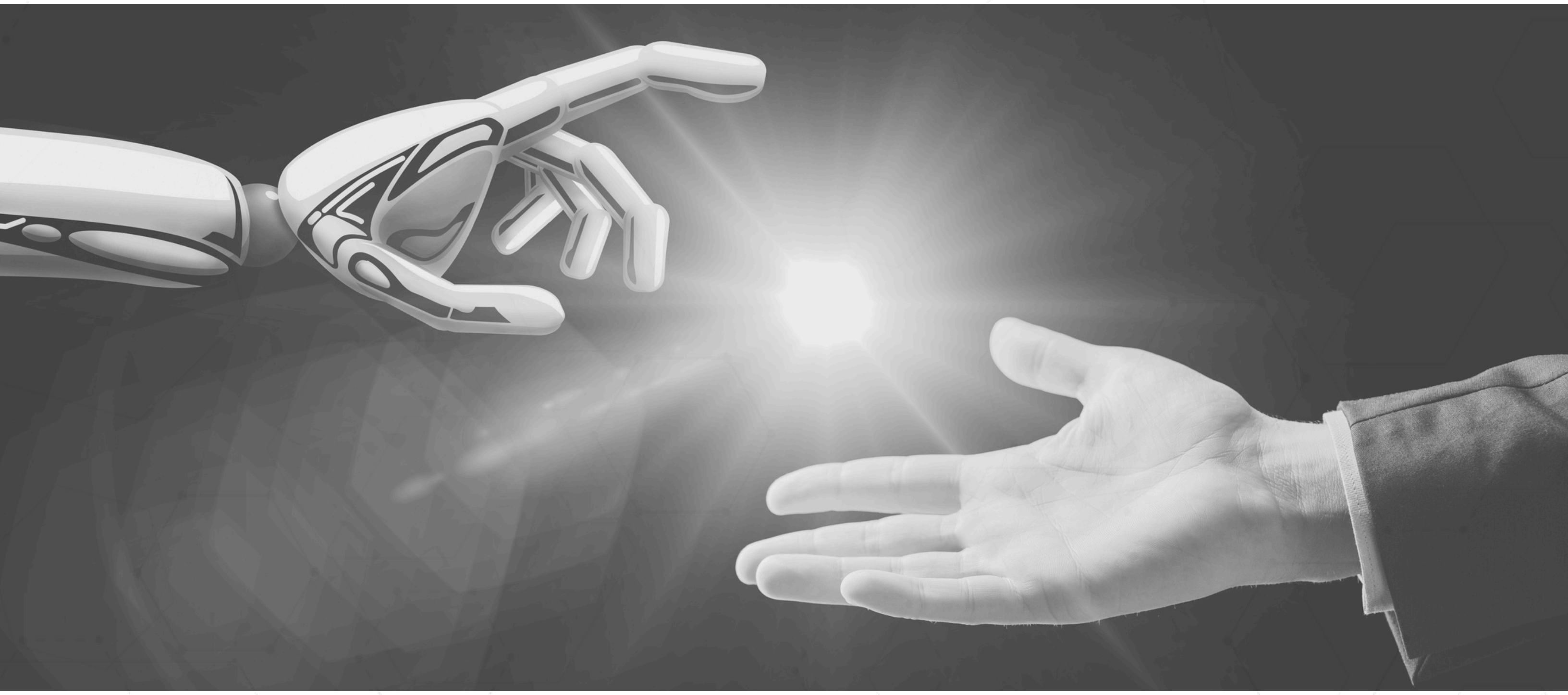
NEXT PERIMETER

SOAR Essentials: How Automation Transforms Cybersecurity for SMBs

A quick guide to enhancing SMB security with automation and SOAR best practices



888-286-4816

NextPerimeter.com

SIMPLIFIED, SCALABLE, AND EFFECTIVE THREAT RESPONSE WITH NEXT PERIMETER

Protect Faster. Respond Smarter. Secure Better.

Discover how Next Perimeter's SOAR solution empowers your business to detect, respond to, and neutralize cyber threats automatically—without the complexity or cost of traditional tools.

WHAT IS SOAR?

Security Orchestration, Automation, and Response (SOAR) is a cybersecurity solution that integrates and automates security processes to enhance threat detection and response. It combines orchestration, automation, and response capabilities to streamline security operations, reducing reliance on manual intervention and enabling rapid containment of threats.

Why SOAR Matters for SMBs

Cyber threats evolve rapidly, and SMBs often lack the resources to monitor and respond to them effectively. SOAR ensures:

- **Threats Are Stopped Early** – Prevents lateral movement and limits the scope of attacks before they escalate.
- **Security Is Simplified** – Automates repetitive tasks, freeing up valuable IT and security resources.
- **Your Business Stays Protected** – Minimizes downtime, financial losses, and reputational damage.

HOW SOAR WORKS

SOAR automates threat response by executing predefined playbooks triggered by specific events or anomalies. Instead of waiting for a human response, the system takes immediate action, preventing breaches before they cause harm.

Key Features

- **Pre-Built Playbooks**

  Ready-to-use workflows for common threats like business email compromise, malware infections, and unauthorized access attempts.

- **Real-Time Response**

  Instantly isolates compromised devices, revokes access, and notifies administrators before an attack can spread.

- **Customizable Automation**

  Tailor workflows to fit your organization's unique security requirements.

- **Simulation Mode**

  Test playbooks in a controlled environment to ensure they function as intended.

- **Exclusion Lists**

  Prevent disruption by designating critical systems and users exempt from automated actions.

SOAR IN ACTION

Scenario 1: Anomalous Sign-In Detected

A user logs into Microsoft 365 from an untrusted location. Without SOAR, even with instant detection from a SIEM or a fully staffed SOC with a four-minute mean time to acknowledge (MTA), an attacker could still steal data or deploy malware. Security teams may detect the breach quickly, but the time it takes to respond manually still allows for damage to occur.

With SOAR, the system immediately revokes access, blocks the attacker's IP, and escalates security controls. Additional security layers, such as enforcing multi-factor authentication (MFA) or requiring additional identity verification, can be activated automatically. The result? The threat is contained within seconds, preventing data theft and unauthorized access while allowing legitimate users to verify their identity securely.

Scenario 2: Malware Infection

A device is flagged for suspicious activity. Without SOAR, security teams may take minutes or even hours to respond, allowing malware to spread, exfiltrate sensitive data, or establish persistence within the network.

With SOAR, the compromised endpoint is instantly isolated, malicious processes are terminated, and further infection is prevented—all without human intervention. Additionally, security logs are analyzed in real time, and similar threats across the organization can be identified and mitigated proactively, ensuring complete containment of the attack.

SOAR IN ACTION

Scenario 3: Phishing Attack Mitigation

An employee receives an email containing a malicious link disguised as an invoice. Without SOAR, the phishing email might go unnoticed until the employee reports it, or worse, clicks on the link, leading to credential theft or malware execution.

With SOAR, the system automatically scans email content, detects known phishing patterns, and isolates suspicious messages before they reach the recipient's inbox. If an employee clicks a malicious link, SOAR can instantly block network access to the phishing domain, notify security teams, and trigger security awareness training for the affected user. This proactive response prevents account compromise, reduces the risk of further exposure, and strengthens an organization's overall phishing defenses.

BENEFITS OF SOAR FOR SMBS

Faster Incident Response

Eliminates the delays associated with manual intervention by automating time-sensitive actions, reducing response times from hours to seconds.

Enhanced Efficiency

Automates repetitive security tasks, allowing IT teams to focus on higher-priority initiatives rather than chasing false positives.

Reduced Risk of Breaches

By responding in real time, SOAR prevents lateral movement and minimizes the impact of attacks before they can escalate.

Simplified Security

Integrates seamlessly with Next Perimeter's SIEM, MXDR, and SASE solutions, reducing the complexity of managing multiple security tools and vendors.

Cost-Effective Enterprise Protection

Brings enterprise-grade security automation to SMBs at a fraction of the cost, making advanced cybersecurity accessible to businesses of all sizes.

WHY CHOOSE NEXT PERIMETER'S SOAR?

Seamless Integration

Next Perimeter's SOAR solution works flawlessly with SIEM, MXDR, and SASE, creating a unified security ecosystem where threats are detected, analyzed, and mitigated automatically.

Pre-Tuned for SMBs

Unlike traditional SOAR solutions that require months to implement, Next Perimeter's platform is pre-configured for SMB environments, enabling quick onboarding and immediate value.

Customizable and Scalable

Whether you need out-of-the-box automation or tailored workflows, Next Perimeter's SOAR adapts to your business needs and scales as your security requirements grow.

Hands-Off Security Management

For SMBs without dedicated security teams, Next Perimeter's SOC handles everything—from configuration to continuous monitoring and response—so you can focus on running your business.

READY TO AUTOMATE YOUR SECURITY?

Next Perimeter's SOAR provides **enterprise-grade security automation without enterprise complexity**. Protect your business with real-time threat detection, automated response, and simplified security operations.

What You'll Get:

- **Instant Threat Containment** – Automated responses that stop attacks before they spread.
- **Seamless Security Integration** – Works with SIEM, MXDR, and SASE for a unified defense.
- **Dedicated SOC Support** – 24/7 monitoring and expert response to threats.

Why Next Perimeter's SOAR?

Simplicity

Easy deployment and pre-tuned for SMBs.

Comprehensive Coverage

Protects your endpoints, networks, identities, and cloud apps.

Expert Support

Managed by our SOC team with 24/7 monitoring and response.

LEARN MORE ABOUT SIEM

▶ Visit NextPerimeter.com to explore how SOAR can provide 24/7 threat detection, real-time response, and proactive security for your business.

NEXT PERIMETER

We're Here to Help

Phone

888-286-4816

Email

sales@nextperimeter.com

Website

NextPerimeter.com

About Us

Next Perimeter simplifies IT and security for growing businesses by eliminating complexity, boosting productivity, and ensuring seamless, secure experiences.

We streamline onboarding to get new hires up and running on day one, replace outdated systems with cloud-first, zero-trust solutions, and deliver unified IT and security services that protect your business while enabling smarter work.