

Our Autonomous SOC|SOAR platform is designed to monitor your cloud, network, and endpoints, so you can sleep at night.

We custom fit our SOC|SOAR to you so you not only get the best technology, but the right technology for your company. Adaptive, evolutionary and alert, we learn the normal behaviors of your on-premise network, cloud services, SaaS applications, and endpoints, so we can detect anomalous behaviors that can lead to a cyber-attack. When considering a SOC|SOAR partner, it's important to understand what each company offers and how they differ.

DIFFERENTIATORS OF THE ZEPHON 24/7 SOC:



SOAR



Integrated Threat Intel



Cyber Risk Scoring



Vulnerability Scanning



Multi-Tenant



Dashboards & Reporting



XDR Automated Response



CSPM

STRENGTHS AND ADVANTAGES:

Customization

We don't just watch for 'normal' industry threats. Our machine learning adapts to the behaviors of your specific cloud, network and users to create a one-of-a-kind security operations center.

Relentless Monitoring

Our algorithms look for malicious threats, malware, ransomware, and software vulnerabilities. Our 24 x 7 x 365 promise to you includes human-based responses, asset discovery, vulnerability assessment, intrusion detection, behavior monitoring, log management, and cloud-based SIEM.

Customer Service

We'll break down the info when you're in a crisis, and in between, you'll get consistent update meetings, one-on-one support, and quick access to real people when you need them.

EASY INTEGRATIONS:

- 2-week deployment time using a single agent across all endpoints
- Integrates with core threat vectors: Devices, Network, Cloud, Apps



Comparison Table

	 SOC XDR SOAR Platform	EDR / XDR	SIEM	MDR
Monitor Your Entire Digital Infrastructure Detect risks across your network, cloud platforms, endpoints, and applications.	✓	X	✓	X
Machine Learning & User Behavior Analytics Real-time alerts driven by anomalous patterns in your data.	✓	✓	✓	✓
SIEM Access and Visibility See all security log data in one centralized location with on-demand access to all retained logs.	✓	X	✓	X
Instant Access to Security Experts Communicate around the clock with a US-based SOC team.	✓	X	X	✓
Issue Triage and Guided Remediation Critical events, actionable, and response are delivered in ~ 8 minutes.	✓	X	X	✓
SOAR Holistic threat management system through security orchestration and automated response.	✓	X	X	X
Threat Hunting Daily hunting for suspicious activity across all of your environments.	✓	✓	X	✓
Vulnerability Scanning Complete visibility of your networks and endpoints and their vulnerabilities.	✓	X	X	X
Customized Reporting and Dashboards Automated and customizable KPI reporting and dashboards.	✓	X	X	X
Joint Install and Onboarding Support White-glove setup and integration to monitor and enhance existing security layers.	✓	X	X	✓
Internal and External Cyber Risk Score Calculated by evaluating your entire landscape of your internal and external digital infrastructure.	✓	X	X	X
Compliance and Governance Track adherence to public and private sector security mandates (PCI, HIPAA, GDPR, NIST, NYDFS, etc.).	✓	X	X	X



ZEPHON

Powered by AGILEBLUE

Our **Pro Subscription Plan** provides essential cybersecurity features through our innovative **Autonomous SOC|SOAR platform**, to meet your organization's needs.

	Pro Subscription Plan
24/7 Security Operations Center/XDR Includes: Detection, Alert Triage, and Escalations	✓
24/7 Analyst and Engineering Support	✓
Threat Hunting	✓
Dashboard and Reporting	✓
Machine Learning & User Behavior Analytics	✓
Alignment with NIST and MITRE Attack Chain	✓
Integrated Threat Intelligence	✓
Advanced Threat Intelligence with Tracking	✓
Managed Cloud-Based SIEM	✓
Joint Install and Onboarding Support	✓
Internal Risk Scoring and Recommendations	✓
SecurityScorecard License	✓
SOAR:	✓
-Orchestration	✓
-3rd Party Applications for Response	✓
-Auto-Response Actions	✓
-Automated Playbooks	✓
XDR with Managed EDR (Isolation, Prevention)	✓
Vulnerability Scanning, Discovery, and Priorities	✓
Log Retention	1 Year
vCISO Monthly Consulting Time	Inquire
-Compliance and Governance Reporting/Review	Inquire
-Incident Response Plans (Top 10)	✓
-SecurityScorecard Consulting	✓
Incident Response Retainer	Inquire