SOCaaS Means Rapid Response

SOCaaS
SOC AS A SERVICE

You've invested in security tools, but does your team have time to review a whole stack of alert types for telemetry? Attackers can be long gone before you even have the full scope of an attack. Effective remediation requires total, rapid visibility. SOCaaS from CISO Global ingests telemetry data from your disparate systems and toolsets. Adding automation and machine learning processes for rapid evaluation, correlation, and initial triage for security events. So, our security analysts get a jump on attackers when making decisions about remediation. SOCaaS not only speeds up analysis and recovery, but supports precision by replacing manual log reviews with automated processes, resulting in accurate, validated, correlated security information.

Certified Analysts, Never a Call Center

Many providers will route you to a call center for remediation support, due to an industry wide shortage of cybersecurity talent. In contrast, CISO maintains a strong team with a deep bench of certified experts in our U.S.-based SOC around-the-clock.

Custom Playbooks and Alerting

Using customized playbooks and alerts, CISO will also design a system of response and communication to fit your team's operating needs. We recognize that each environment is unique and you need security protocols aligned to your processes. We work as a true extension of your team.
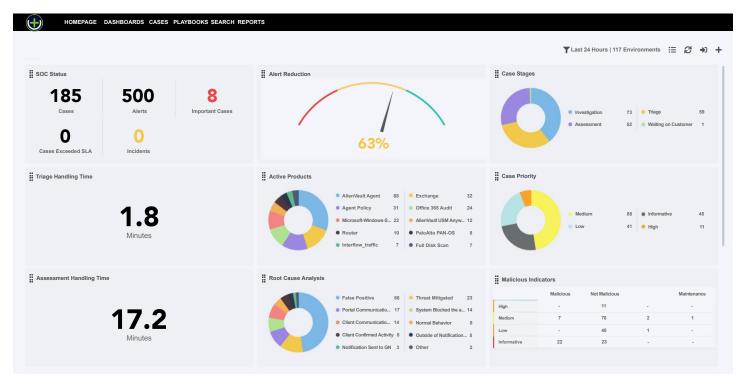

Managed & Co-managed

Leverage our 24x7x365 SOC full-time – or just for nights, weekends, and holidays so your team can rest without risking off-hour attacks.

CISO GLOBAL

480-389-3444 | **ciso.inc**

All your security tools, working **together**,
with total visibility in a single **dashboard**.

HOMEPAGE   DASHBOARDS   CASES   PLAYBOOKS   SEARCH   REPORTS

Last 24 Hours | 117 Environments

SOC Status

185	500	8
Cases	Alerts	Important Cases
0	0	
Cases Exceeded SLA	Incidents	

Alert Reduction

63%

Case Stages

Investigation	73	Triage	59
Assessment	52	Waiting on Customer	1

Triage Handling Time

1.8
Minutes

Active Products

AlienVault Agent	68	Exchange	32
Agent Policy	31	Office 365 Audit	24
Microsoft-Windows-S...	22	AlienVault USM Anyw...	12
Router	10	PaloAlto PAN-OS	8
Interflow_traffic	7	Full Disk Scan	7

Case Priority

Medium	88	Informative	45
Low	41	High	11

Assessment Handling Time

17.2
Minutes

Root Cause Analysis

False Positive	86	Threat Mitigated	23
Portal Communicatio...	17	System Blocked the a...	14
Client Communicatio...	14	Normal Behavior	8
Client Confirmed Activity	8	Outside of Notification...	5
Notification Sent to GN	3	Other	2

Malicious Indicators

	Malicious	Not Malicious		Maintenance
High	-	11	-	-
Medium	7	78	2	1
Low	-	40	1	-
Informative	22	23	-	-

Powered by US-based Expert Analysts & SOAR (Security Orchestration, Automation, and Response) Processes

Common Problems Solved by SOCaaS

· Dwell Time. Reducing your Time to Remediate (TTR) is essential to keep attackers from doing costly damage in systems. SOCaaS speeds up response times with automation, machine learning, and highly trained Certified Security Analysts.

· Too Many Tools Hinder Visibility. Making your tools work more efficiently is key to maximize your ROI on existing technology. SOCaaS pulls your tools together for orchestration, all on a single alerting dashboard.

· Nights, Weekends, Holidays. Criminals don't respect your 9-5, M-F work week. If you already have an internal security team, we can monitor and stop attacks while they're away. You'll rest better with your network in good hands.

AICPA SOC
SOC 2® Type II Audited

SOC 2 Type II Certified Provider

With 20 integration types, spanning well over 100 technology vendors, our SOCaaS reduces time lost investigating alerts one-by- one.

You can keep the platforms you have in place and still leverage the power of our Security Operations Center. Our deep bench of highly trained, certified Security Analysts and enterprise tool stacks will take your current technologies to the next level.

CISO
GLOBAL

480-389-3444 | **ciso.inc**

About Us

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, IEEE®-certified biometric professionals, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.

STRATEGY & RISK

- Gap Analysis
- Audit/Assessment
- Third Party Risk Management
- FedRAMP
- StateRAMP
- CMMC
- Advisory
- Virtual CISO
- Managed Compliance
- Managed GRC

CYBER DEFENSE OPERATIONS

- Extended Detection & Response
- Managed Detection & Response
- SIEM as a Service
- Threat Hunting
- Cyber Threat Intelligence
- Digital Forensics
- Vulnerability Management Program
- Attack Surface Reduction
- Cyber Incident Response

SECURITY ARCHITECTURE & ENGINEERING SOLUTIONS

- Secured Managed Services
- Advanced Firewall Management
- Identity & Access Management
- Cloud Security
- Data Protection
- Remediation

READINESS & RESILIENCY

- Penetration Testing
- Tabletop Exercises with Incident Response Retainer
- Training Programs

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations ™
SOC 2® Type II Audited

CISO
GLOBAL

480-389-3444 | **ciso.inc**