Security Operations as a Service (SOCaaS)

At the center of zero trust is enterprise visibility, automation, orchestration, and governance enabled by a security operations center.

Whitepaper

September 2022

MANAGEMENT SUMMARY

Considering recent security breaches, the Executive Office of the President has mandated agencies to adopt a "Zero Trust" cybersecurity strategy. According to the Executive Order (EO), agencies should: create an inventory of devices, segment and encrypt networks, implement single sign-on authentication, treat all applications as Internet-connected, and improve data monitoring across cloud and computer networks.

An essential tenant to Zero Trust is the ability to monitor and verify enterprise activity. Security operations centers are necessary for an agency's Zero Trust strategy. Using a managed security provider to obtain SOC services can be a quick win for agencies.

This white paper will cover the following topics:

- What is zero Trust, and how should SOCaaS be part of your agency's roadmap?
- Why managed security service providers can deliver innovations at affordable rates?
- What capabilities are offered by SOCaaS?
- SOCaaS value to agencies?

Table of Contents

Introduction

"At the center of a Zero Trust strategy, agencies will need enterprise visibility of users, assets, applications, and workloads."

What is Security Operations as a Service? Security Operations Center (SOC) is essential for monitoring, managing, and responding to cyber-attacks. Many organizations struggle to implement their SOC. SOC challenges include identifying and retaining skilled resources, meeting the Federal Government's FEDRAMP standards, integrating systems and tools, and using the most cost-effective technologies. Some agencies understand that building and operating a 24 x 7 SOC is complex and costly and are considering fully managed, or hybrid managed SOCs.

SOCaaS Offers? Many agencies have made significant investments in their existing Security Operations Centers. Displacing your current investment is not necessary with our SOCaaS because we can provide complementary services. For example, your agency may provide the SOC functions during regular business hours while tasking off-hours to us. This is a great example of how your agency may leverage our SOCaaS while continuing to use your existing SOC investment. Our flexible service offerings allow your agency to outsource SOC management or task-specific SOC functions to us.

SOCaaS Capabilities? SOC capabilities will vary by provider. Our vision is a holistic approach that combines traditional monitoring, detecting, investigating, and reporting with vulnerability management and compliance. Our approach will ensure that the SOC systems and tools are configured to focus more closely on known vulnerabilities and that SOC leadership is knowledgeable about your agency's enterprise vulnerabilities and risks. The result is a more secure enterprise for your agency.

SOCaaS value to agencies? Disruptive Solutions offers agencies a team of experienced security operators, a suite of systems in a cloud infrastructure that is FEDRAMP High and IL4/IL5 certified, and proven SOC processes that set the stage for continuous improvement and exceeding our service level objectives. Our highly customizable services enable agencies to leverage managed, and hybrid managed offers while allowing us to introduce new systems and tools as your agency's requirements evolve.

ZERO TRUST AND SOCaaS

Zero Trust is a strategy that moves from the traditional perimeter defense to many perimeters, focusing on protecting data, where you never trust and always verify.

WHAT IS ZERO TRUST?

The traditional perimeter-centric defense has been ineffective at keeping hackers from gaining access to enterprises. Since users within the perimeter are authorized and trusted, there are limited protections and visibility within the perimeter. Zero Trust is a strategy that overcomes the limitations of perimeter defense. Zero Trust assumes the enterprise is untrusted; users have the least privilege; you can monitor and control workloads; all workloads are encrypted, and the enterprise is audited and monitored.

Department of Homeland Defense (DHS) Zero Trust Maturity Model defines five zero trust pillars.

Identity – Consists of a list of attributes and uniquely describes a user. Agencies should enforce access to data based on the users identity using least privilege.

Device – Consists of IT hardware and software assets. Agencies should have asset inventory, vulnerability management program, and understanding of enterprise risk.

Network – Consists of communications medium between devices. Agencies should implement segmentation, encryption, and network security controls.

Application workload – Consists of enterprise software applications and how they interface with users and other applications. Agencies should manage access and implement application security controls.

Data – Consists of information on devices, networks, and applications. Agencies should inventory, categorize, label, and encrypt data.

> "Monitoring and verification is at the center of a zero-trust strategy, and Disruptive Solutions' SOCaaS can be a quick win for agencies."

SOCaaS AND ZERO TRUST

According to the DHS maturity model, monitoring, orchestration, and automation are required for meeting the advanced and optimal maturity levels. SOCaaS offers advanced monitoring and Security Orchestration Automation and Response (SOAR). These capabilities should be part of your agency's Zero Trust strategy and are quickly adopted with Disruptive Solutions' help.

Competition drives innovation and lowers costs

"The nature of managed service drives lower costs by sharing investment and resources between many customers."

BUY VERSUS BUILD SOC SERVICES?

Agencies are considering SOC services through a Managed Security Service Provider (MSSP) over building or continuing to operate their SOC. The reasons are that it is increasingly becoming more challenging to recruit and hire new cybersecurity talent, the increasing complexity of technology, and the cost of dedicated systems and tools. The following are benefits of using an MSSP for SOC services:

INNOVATION

MSSPs routinely evaluate their competition and emerging technologies to identify innovations for adoption to maintain competitiveness and market differentiation. Competition forces the MSSP to make important cost trade-offs delivering a balance of price and innovation. The result is agencies will receive service features the market demands at affordable prices.

ACCESS TO TECHNICAL TALENT

An MSSP offers access to high-level expertise that may take years to build, processes that have undergone years of refinement, and an integrated suite of systems and tools. Agencies receive these benefits while paying for what they use.

FOCUS ON OUTCOMES

Often organizations focus on vendor products rather than outcomes.   Time has shown that technologies, products, and vendors rapidly change. What was once an industry leader either gets replicated or replaced over time. Managed services enable agencies to focus on objectives, user experience, and key performance indicators rather than software applications and tools.

LOWER COSTS

Agencies will benefit by an MSSP's routine capital investment in new technologies. Since an MSSP shares systems and people, agencies can receive SOC services only paying for a fraction of the capital investment and resource expenses.

SOCaaS CAPABILITIES

We offer two SOCaaS options that can either provide a comprehensive suite of capabilities and tools or flexible services that can become an extension of an agency's current security operations.

FLEXIBLE SERVICE OPTIONS

For organizations that choose to build their SOC, many struggles to recruit and hire new cybersecurity talent, adapt to the increasing complexity of technology, and afford the cost of dedicated systems and tools. After acknowledging the magnitude of this effort, some public sector organizations are exploring options such as outsourcing or transitioning to a hybrid SOC model. A hybrid model use case may be that the agency SOC will support business hours while we support after hours. This use case will task us with hard-to-staff night shifts saving time and money for your agency. Many agencies are opting for a hybrid model because of this flexibility.

Managed
- All-inclusive SOC services
- 24x7 fully staffed by us
- SOC systems and tools
- Access to dashboards and tools

Hybrid
- A-la-carte SOC service
- Staffed by the agency and our staff
- Division of roles and responsibilities
- Custom interface agreements
- Shared systems and tools

SOCaaS CAPABILITIES

SOCs are essential for monitoring, managing, and responding to cyber-attacks and can help enterprises of all types and sizes mitigate the impact of these events. We provide a suite of security operations services via a managed service 24x7, anywhere in the world. Table 4-1 describes our SOCaaS capabilities.

Table 4-1 SOCaaS capability summary. Agencies will receive a comprehensive suite of services to mitigate risk and respond to security incidents.

Feature	Description	Activities
24 x 7 Monitoring	Monitoring, detection, investigation, and coordination of suspicious events.	• Aggregation, categorization, and normalization of logs • Creation, tuning, and management of alerts • Data gathering, correlation, and analysis of events • Filter false positive events • Categorizing severity and priority
Incident Response	Incident management consists of planning, event analysis, validation, and response to security incidents in an enterprise.	• Open and assign security cases • Case coordination and management • Analyze, identify, research, and gather event information • Categorize and analyze the source of all incidents • Perform incident forensics • Assess technical and business impact

Feature	Description	Activities
		• Contain, eradicate, and recover from incidents. • Document and preserve evidence. • Provide appropriate follow-up reporting and lessons learned, and recommendations
Threat Hunting	Responsible for searching for adversaries with intent, capability, and opportunity to exploit. Threat hunters look for adversaries and deploy countermeasures.	• Enterprise evaluation • Assess high-risk information and potential targets • Gather information using analytic tools • Identify suspicious activity
Vulnerability Management	Vulnerability management is identifying, classifying, and remediating vulnerabilities.	• Establish a continuous vulnerability scanning strategy • Conduct routine vulnerability scans • Categorize vulnerabilities by risk factor • Analyze results and provide risk-based mitigation recommendations • Scoped reporting for stakeholders
Compliance	Routine certification and accreditation of systems with security laws, standards, and policies.	• Incorporate organization policy into tailored scanning benchmarks • Documentation • Audit • Penetration testing
Service level objectives	Service level objectives are performance indicators that measure agency experience.	• 99.9% systems availability • 5 min mean time to respond • 15 min mean time to triage event • 30 min mean time to notify the agency • 95% proactive versus reactive agency notification

Monitoring. Each device and application will generate informational-level logs. Logs from monitored agency assets are collected, stored, and analyzed to create enterprise events. Our security operation tools correlate enterprise events into a subset of notable events. These notable events are prioritized based upon criticality, by which our Tier 2 analysts investigate according to clearly defined event criteria to provide reports and remediation recommendations to your agency. Active monitoring of these logs will ensure that the agency's network and security devices are in good operational health and will alert the SOC team to any potential security threat.

Incident response and forensics. Events are assessed in real-time to identify malicious activity utilizing both commercial and customized cybersecurity visualization and analytics tools. The 24x7 incident response team is responsible for identifying, evaluating, and remediating security incidents. The Incident Response team will escalate the security incident for executive visibility or engage other engineering based on the severity of the incident. The forensics team provides the capabilities to perform system log analysis, network activity analysis, and system forensics. Processes are in place to work with operations teams to freeze forensic images, extract those images, and perform forensic analysis.

Threat hunting. Threat hunting is essential because sophisticated attackers occasionally get past automated security systems and tools. As good as the tools' ability to identify attacks through advanced correlation and artificial intelligence, agencies will still need threat hunters. Threat hunters will gather valuable clues using the information collected by our sensor and SIEM tools. Our hunters will begin with a hypothesis based on perceived agency risks or intelligence. The threat hunter will conduct a structured, unstructured, or situationally driven campaign. Routine threat hunts are essential in identifying unknown exploits and reducing attacker dwell time within an enterprise.

Vulnerability management. Vulnerability management is the ongoing, regular process of identifying, assessing, reporting, managing, and remediating device vulnerabilities within your agency's enterprise. It is a critical function for protecting your assets from compromise. Our security operations center uses it to closely monitor assets with a high risk of compromise because they may have a critical or high vulnerability. As part of our SOCaaS, we will routinely scan your enterprise, identify vulnerabilities, and

develop a plan of action to remediate or mitigate them. We will work with your agency's IT staff to make them aware of the vulnerabilities and report on the progress of addressing the vulnerability.

Compliance. All IT enterprises should adhere to a set of policies and standards. Federal agencies are required to adhere to the Federal Information Management Act (FISMA) law. This law requires Federal agencies to meet mandatory processes and systems controls to ensure confidentiality, integrity, and availability of IT information. NIST 800-53 describes these processes and controls for low, moderate, and high-impact systems. Our SOC services adhere to FISMA high-impact controls, and we may assist agencies by supporting security audits, possessing the appropriate systems documentation, and conducting penetration tests.

SOC PLATFORMS

Our SOC platforms can help detect and react to new zero-day attacks and threats. Whether it is network traffic, user activity, or application use, any variation from a regular operation could indicate that a threat is imminent and that the agency's data or infrastructure is at risk. Our SOC systems will detect and predict cybersecurity incidents by ingesting and correlating terabytes of data generated from audit logs, syslogs, active directory, Domain Name Services (DNS), Dynamic Host Control Protocol (DHCP) servers, and other enterprise systems. The systems will automate and orchestrate to reduce overhead and allow analysts to focus on important activities. This security platform provides API integration with other dedicated SIEM products a customer may have made investments

Although systems and tools may change over time, we will use industry-leading tools as part of our managed security service, as illustrated in **table 4-2**.

Table 4-2 Example SOCaaS platforms. Security platforms are essential to ensure that threats are accurately identified and that analyst investigation time is short.

Function	Description	Platforms and Tools
Security Event Information Management (SEIM)	We will collect, store, analysis, and enterprise log information to identify events.	• Tenable Log Correlation Engine (LCE) • Elastic Search, Logstash, and Kibana • Splunk • MS Sentinel
Vulnerability management	We will provide scanning, tracking, and plans of actions and milestones (POAM) for vulnerability remediations.	• Tenable.sc • Nessus
Incident Management	We will review, classify, and investigate security incidents.	• Jira • Service Now • MS Service manager
Forensics	We will collect, analyze, track, and report digital evidence during a cyber investigation.	• PassMark • OSForensics
Case Management	We will track, workflow, and manage security incidents and responses.	• Jira • Service Now • MS Service manager
PenTesting	We will conduct Pen Testing to identify areas of weakness in the enterprise identifying vulnerabilities and potential exploits.	• PentestBox, • IBM AppScan • SAINT Security Suite
Security Intelligence	Tools will be tuned to identify events using the latest in threat intelligence, lowering the rate of false positives.	• Open Threat Exchange (OTX) • MITRE ATT&CK

Our SOCaaS has standardized on Tenable products but has experience using many tools to suit our client's IT environments. Each tool in table 4-2 enables SOC analysts to investigate events and collaborate with other team members. Each agency will receive a dashboard that reports volumes, alerts, threats, and trends.

EFFICIENT AGENCY ONBOARDING

Onboarding begins with collecting the agency's asset inventory, and Internet Protocol (IP) addresses for the devices. We will implement the SOC services and start to ingest device logs. Our onboarding process documents team responsibilities, service metrics, incident response processes, and agency-specific playbooks. Our approach ensures success in effectively securing your enterprise.

FACILITY

We recognize that environmental and physical security is critical to any SOC. This capability is one of the most mature tenets of security. With this in mind, we will operate as an enterprise-grade service with physical and environmental redundancy to deliver a highly survivable five 9s service platform. The following are some of our SOC facility features:

Table 4-3 illustrates the SOC facility features that will deliver service reliability and unsurpassed physical security.

Table 4-3 Facility. The facility provides the ability for us to deliver highly available services.

Feature	Description
Space	7,500 square ft of space 2FA biometric authentication for access to the facility
Network connectivity	40GB or redundant network connectivity
Power	- Diverse and redundant power - Automatic fail-over
Uninterruptable Power Supply Power Failure	100% full DC backup power - The battery lasts 4 hrs without an on-site generator or 2 hrs with an on-site generator
Heating, Ventilation, and Air Conditioning (HVAC)	- Redundant HVAC - HVAC is equipped with alarms for high & low temperatures and mechanical failures (compressors, fans, refrigerant leaks, etc.).
Closed Circuit Television (CCTV) Video Surveillance	24 x a UL-certified monitoring facility monitors CCTV systems. - The monitoring center will dispatch the local law enforcement agency as appropriate.
Fire/Smoke Detection Sensors	- Site smoke detectors - Annually tested by technicians 24 x 7 monitoring by network and security operations center - Dispatch the local fire department or a technician for investigation

OUR VALUE TO AGENCIES

Disruptive Solutions has over 20 years of experience protecting agencies from cybersecurity threats. By leveraging our Tenable Assured Compliance Assessment System (ACAS), and our years of experience supporting some of the most challenging public sector missions, we deliver "best in class" cyber protections.

Disruptive Solutions' SOCaaS offers the following benefits:

- **Low cost.** We routinely make capital investments to keep infrastructure current while making longer-term investments to add new enhanced capabilities. SOCaaS customers have no capital costs, and the monthly costs can be as much as 32% lower for the same level of service because of our share SOC environment.

- **Flexible operations.** We recognize that many agencies already possess a degree of security monitoring. We offer two SOCaaS operational models that consist of managed and hybrid management.

- **Comprehensive SOC capabilities.** By including vulnerability and compliance security operations functions, we offer a complete set of SOC capabilities that extend beyond monitoring and responding to events.

- **Experience.** Extensive past performance performing continuous monitoring for DoD, DHS, and GSA since 2020**.** With notable customers and successes with DoD, Space Force, and 25 other federal agencies and components.

- **Public Sector Information Protection.** We understand the importance of meeting Federal security standards, US-based and cleared; personnel, and reliable facilities with over 20 years of securing FEDRAMP High impact and DOD IL 4/5 cloud infrastructures.

By the numbers

"Cybercrime costs will reach $10.5T annually by 2025"[1]

Unfilled cybersecurity jobs grew by 350%, in 2021 to 3.5M.[2]

"In most cases it takes companies 6 months to discover a data breach"[1]

"It costs $250-$750K and 18 months to FEDRAMP cloud services.[3]

[1]   Morgan, Steve. (2020) 'Cybercrime To Cost The World $10.5 Trillion Annually By 2025', Cybersecurity Ventures. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)

[2]   Farber, Malcomb (2021), 'Cybersecurity Jobs Report: 3.5 Million Openings Through 2025', Cybersecurity Ventures. Cybersecurity Jobs Report: 3.5 Million Openings Through 2025 (einpresswire.com)

[3]   'How much does it cost to get FedRAMP compliant and obtain an ATO?', Stackarmor, How much does it cost to get FedRAMP compliant and obtain an ATO? (stackarmor.com)

Contacts

Address
Chris@distuptivesol.com

Mobile
703-203-7500

Media
www.disruptivesol.com