Cyber Defence Profile

Offensive and Defensive

Sandex Consulting

- 2023 -

Sandex

CONNECTING THE DOTS

Security Operations Center as a Service (SOCaaS)

An elite team of experts ready to detect and respond

What is a SOC as a Service?

SOC as a Service is an offering from a cybersecurity company that typically acts as a customer's entire security operations center (SOC). Due to extenuating circumstances, like a talent shortage or the fact that a business may be in startup or mid-life mode without the resources to property secure its network, SOC as a Service (SOCaaS) can act as that organization's tactical console from which it can track security alerts, defend against cyber attacks, and improve overall security posture.

According to IDC, organizations can outsource a set of security functionality to a SOC team, including those such as SIEM, vulnerability management, endpoint security, and other detection and response tools. A customer organization could also sign up for the entire menu of services. Delivered as cloud service though, operations will occur offsite and hosted in the cloud. A few real-world outcomes that SOCaaS providers look to provide on behalf of a customer are:

- Remediating cyber threats on behalf of customers
- Enabling customers to determine what services are relevant to them
- Streamlining data ingestion and analysis from a customer's network
- Translate processes and outcomes into relatable language that can be leveraged and understood by almost any stakeholder

With this in mind, it's also important for a business or security organization to conduct a thorough analysis of their current security program, identifying its strengths and weaknesses and practice areas they may not previously have addressed. This will help narrow the focus of a SOCaaS vendor search to criteria unique to the customer.

SOC as a Service (SOCaaS) Benefits

Perhaps the biggest benefit of engaging a service provider to take on a particular area of security concern is that a customer no longer has to worry about that area. Since SOCaaS encompasses many areas, as mentioned above, let's take a look at some of the specific benefits:

Faster detection and remediation

If a team is slow to respond when an anomaly is detected, odds are there are priorities pulling personnel in multiple directions. A SOCaaS provider will dispatch analysts dedicated to responding to cyber threats and vulnerabilities and taking them down or remediating. For an in-house SOC, rapid context switching from situation to situation can be a real time suck, thus a team dedicated solely to detection, response, and remediation will be able to move much faster.

Access to specialized security expertise

SOC analysts must cover the gamut of specialties, and respond quickly on behalf of customers. SOCaaS vendors should be able to provide access to analysts who can address endpoint containment, threat hunting, malware analysis and containment, distributed alerting and escalation pathways, and much more. Understanding a SOC's people, technology, and pathways can aid in the search for a trusted vendor.

Enhanced maturity

The benefit of an accelerated evolution of a customer security program can't be understated. SOCs are faced with threats every day – or many of them. Having a budget to address immaturity in a security program is great, but if there is no strategic in-house talent acquisition plan, then it might be a more efficient solution to shift that focus to finding the right SOCaaS partner.

Lower cost than on-premise SOC

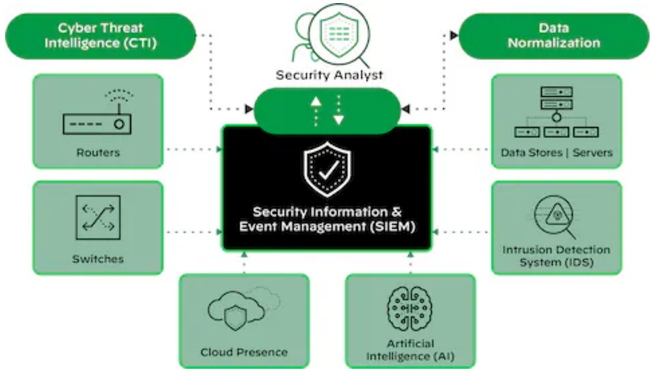
Speaking of talent acquisition, building a SOC from the ground up can come with many additional costs than engaging a managed services partner. There are the obvious start-up costs of sourcing the right technology and personnel and there's also the specter of churn once you have those people and operational processes in place. Around 71% of SOC analysts say they feel burned out on the job, especially if those analysts only total around seven in number and have the weight of the company's security world on their shoulders.

SOC as a Service Roles and Responsibilities

Even in the event a company or small security organization has decided to begin the search for a SOCaaS vendor, it's still critical to know the roles and responsibilities of the analysts and staff in that SOC. After all, they'll be the ones protecting your environment – and reputation.

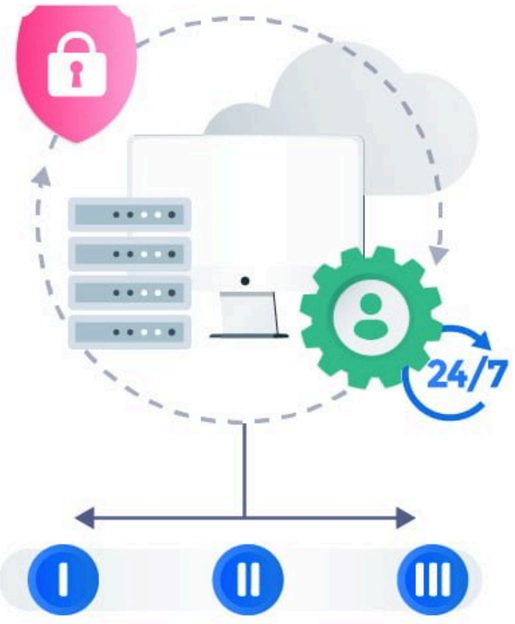
SOC Manager

This person/position oversees the SOC, and will be in charge of directly managing a security team of several people. The SOC manager role involves developing an overall security strategy for the company – creating a vision for hiring, building processes, and developing the technology stack. This person should be able to provide both technical guidance and managerial oversight.



Security Analyst Tier 1 - Triage

An analyst in the provider's SOC will field and alert and triage it. During that investigation, they'll determine where in the patch or remediation queue it should fall. Alerts can take up a significant amount of time for an in-house security organization, and with a team managing and automating the triage process, it can drastically reduce the daily burden on those in-house teams.



Security Analyst Tier 2 - Incident Responder

This type of analyst will typically field alerts from their Tier 1 counterpart. If an alert ends up in this person's queue, that means it has been determined to be real and should be prioritized for response. Deeper investigation into the alert, identifying systems affected, and crafting of a response and/or remediation plan are key responsibilities of this role.

Security Analyst Tier 3 - Threat Hunter

At this stage of the process, the hunt is on. If the incident has been determined to be of a more severe nature, a threat hunter will look at how an attacker or threat was able to get past initial security checks. A threat hunt enables security analysts to actively look at a customer's network, endpoints, and security technology to look for threats or attackers that may be lurking as-yet undetected.

Security Architect

An architect is typically responsible for building security architecture, engineering security systems, and implementing those systems. They should also be able to document the requirements, procedures, and protocols of the architecture and systems they create. Additionally, they'll weigh in on key regulatory and compliance requirements on behalf of their SOCaaS clients.

Challenges of SOC as a Service

A SOC is the control center for a company's cybersecurity operations, thus there are some complex operations taking place. Some aspects are automated, some are manual human operations. And a customer organization searching for the right partner is about to outsource some – or all of – those operations. Let's take a look at some challenges of SOCaaS as a business decides to put their digital trust into the hands of an outside team.

Onboarding process

A vulnerable phase will follow any engagement of a SOCaaS provider. That is, the provider must configure its tech stack to work within a new client's environment, and the client must ready its network for the deployment of monitoring protocols by the new provider. Testing and implementation of a template for gathering and acting upon insights will follow during the next phase of the ramp-up period.

Enterprise data security

Securing a customer's network is one thing, but ensuring the data is safe on the SOCaaS provider's side is another altogether. Therefore, it's critical for a customer to do their research to find a provider whose own defenses are fortified to protect the enterprise data of all of its clients. This essentially becomes a supply chain issue, and should be handled with all the considerations that come with that approach.

Cost of log delivery

Full access and autonomy to a provider's operations – as concerns a specific customer – can be expensive for that customer. While it is technically the information generated by that customer's network, the operations and actions the SOCaaS provider is taking are their own. When taking this into consideration, it's clear why gaining full access to log data can be pricey for a security organization.

Compromise Assessment

Dark Web Investigation

Sandex
CONNECTING THE DOTS

Benefits

- Proactively determine if a network has been compromised
- Identify areas of risk to better protect against a future attack
- Obtain results in weeks, not months
- Experience limited impact on system resources through a scalable and efficient process — launched through dissolvable scripts
- Receive assessment coverage of all operating systems

81%

The number of data breaches involving stolen or weak passwords has risen from 50% to 81% during the past three years.

Source: 2017 Verizon Data Breach Investigations Report (DBIR)

Compromise Assessment

Prevent Future Attacks by Determining If a Compromise Has Already Happened

Can an organization truly know whether or not it has been compromised? How easily can the extent of a breach be identified? Cyberattacks have become increasingly sophisticated and the sheer number of connected devices presents an unprecedented opportunity for threat actors.

DigitalEra's Compromise Assessment evaluates an organization's security posture to determine if a breach has occurred or is actively occurring. The assessment can determine when, where, and how a compromise occurred, and provide tactical recommendations for preventing another attack. By integrating artificial intelligence into tools and processes, our experts secure environments while swiftly identifying a compromise, resulting in a preventative security approach.

Service Overview

A Compromise Assessment utilizes a methodology for identifying environmental risks, security incidents, and ongoing threat actor activity in a network environment. The assessment identifies ongoing compromises and uncovers the malicious access and usage of the environment. The goal is to detect and stop any active security incidents quickly and quietly.

The assessment is composed of three phases — with each phase more targeted — and addresses core problems such as:

- Data exfiltration and sabotage
- Command and control activities
- User account anomalies
- Malware and persistence mechanisms
- Network, host, and application configurations

About

- World-renowned experts work synergistically across our practice areas to deliver consistent, best-in-class services anywhere in the world
- Incorporates artificial intelligence into tools and processes to more efficiently and effectively secure the environment to prevent attacks from happening
- Utilizes multiple techniques to collect information, assess data, provide a risk profile, recommend actions, and highlight notable strengths for an organization
- Techniques are designed to not impact the client's operations in any way
- Integrated practice areas: ThreatZERO™ Services, Incident Containment and Forensics, Red Team
- Services, Industrial Control Systems Security, IoT and Embedded Systems, and Training

How It Works

Any organization can participate in a Compromise Assessment, regardless of which security solutions they are currently using. DigitalEra security experts will conduct assessments that include three main phases:

Phase 1 — Initial Assessment

In this phase, self-delegating and human readable scripts are pushed out to endpoints either through dissolvable scripts using the customer's existing software deployment or through a DigitalEra agent. These scripts assist in gathering key data that helps in searching for anomalous behaviors and conditions that are indicative of malicious activity or correlate to risks in the environment. The output from these scripts is then forwarded to the cloud for both manual and automated analysis to determine hosts of interest.

Phase 2 — Targeted Assessment

Targeted scripts are deployed to hosts of interest identified in Phase 1. Network logs are collected to gather more in-depth data and analysis related to the behaviors and activity previously identified. It is also determined whether the findings from Phase 1 were false positives or indicate malicious activity. Script output is again forwarded to the cloud for analysis; however, it includes forensic artifacts to facilitate the validation that attacks have taken place or are underway. Containment strategies and other options moving forward are identified and communicated to the organization.

Phase 3 — Forensic Assessment

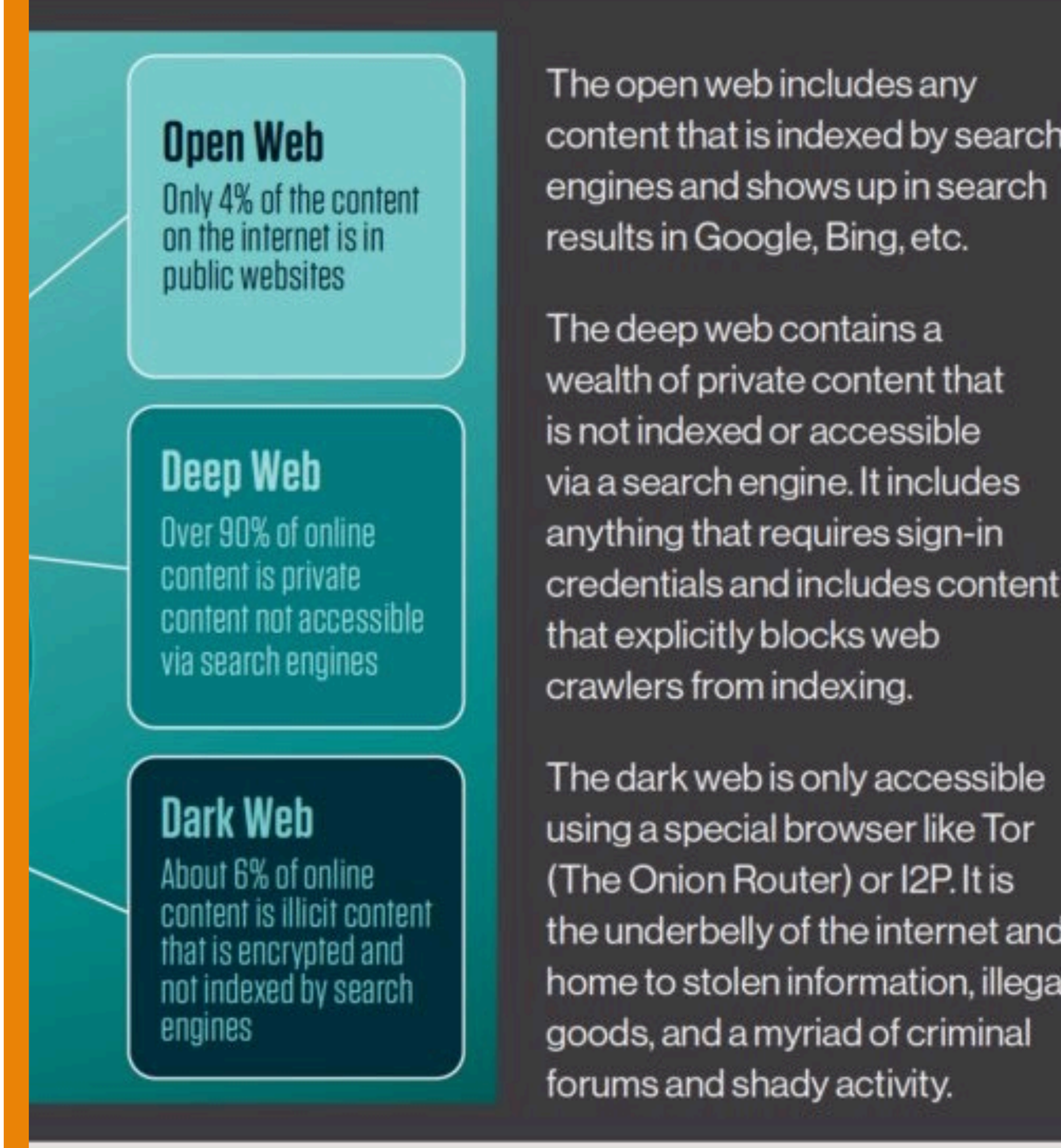
If, according to internal corporate policies, certain computers require retention for legal or other purposes, or if more scientific/technical analysis is necessary, then activities will include a full bit-by-bit disk copy of those computers, including memory dump, for related analysis. As with Phase 2, any new information is utilized to identify additional systems of interest from the Phase 2 database, and subsequent analysis is then conducted.

Deliverables

At the conclusion of the assessment, a comprehensive report is provided to the executive team that details:

- A list of vulnerabilities detected
- The risk state of the environment
- Strategic and tactical recommendations for remediation

How confident are you in knowing whether or not your organization has been compromised? Contact DigitalEra team to learn how a Compromise Assessment can help you identify and eradicate security vulnerabilities




3D Managed Application Security Testing
Unlimited Protection

3D Managed Application Security Testing.

All your web, mobile, source code, and network testing needs, bundled into one subscription

Overview

Today's security professionals and software developers must do more in less time, all while keeping applications secure. To mitigate risk and address compliance requirements, your software security initiative must include application security testing. But what if your team lacks the resources or skills to apply AppSec testing effectively across your continually evolving application portfolio?

The Synopsys 3D Managed Application Security Testing (AST) subscription gives you the application and network testing coverage you need to achieve your risk management goals by bundling all managed AST assessment types (dynamic application security testing (DAST), penetration testing, static application security testing, software composition analysis, mobile application security testing, secure design review, and network security testing) into one annual subscription at a fixed cost.

Key benefits

- **Flexibility.** Apply risk-based testing to your application portfolio (e.g., penetration testing on high-risk applications versus DAST on low-risk applications). Plus, you can change the application to test, the test type, and the test depth.
- **Coverage.** Test applications and networks you might miss due to resource constraints.
- **Consistency.** Get the same high-quality test results for any application or network, any time.
- **Enablement.** Go step by step through your test results and get help developing a remediation plan best suited to your needs.
- **Scalability.** Get scalable testing delivery through our Assessment Centers without compromising manual reviews.
- **Comprehensiveness.** See a thorough analysis of results and detailed reporting, and then get actionable remediation guidance from our blended manual and tool-based assessment approach.

Adapt rapidly to your evolving testing requirements

Reduce your risk of a breach by identifying and exploiting business-critical vulnerabilities with on-demand security testing expertise

To keep your applications secure, you need continuous access to the people, processes, and technologies that allow you to scale efficiently and scan with speed. With our 3D Managed AST subscription, you can test any web or mobile application or external network, at any depth, any number of times (one test at a time). The results: unrivaled transparency, flexibility, and quality at a predictable cost, plus the data you need to remediate risks effectively. Our Assessment Centers give you continuous access to teams of security testing experts with the skills, tools, and discipline to analyze your applications any time. You can close testing gaps, conduct testing at any depth, and quickly scale to manage high-demand testing periods.

Perform 7 types of assessment

Our 3D Managed AST subscription combines multiple testing tools, automated scans, and in-depth manual tests to give you the most comprehensive application security evaluation. You can change the application or external network to test, as well as the type of assessment and depth of test (one test at a time), as your risk profile and testing requirements evolve. If you need to test more than one application at a time, just purchase another subscription or an individual managed application security test.

Dynamic Application Security Testing (DAST)	Penetration Testing	Static Application Security Testing (SAST)	Mobile Application Security Testing (MAST)	Network Security Testing
Identify security vulnerabilities while web applications are running, without the need for source code.	Extend DAST using multiple testing tools and in-depth manual tests focusing on business logic to find vulnerabilities and then try to exploit them.	Systematically scan and apply in-depth manual tests to identify and eliminate common to critical software security vulnerabilities in your source code.	Combine traditional static and dynamic testing techniques to discover security vulnerabilities in iOS and Android applications and corresponding back-end components.	Detect common to critical security vulnerabilities in your external network and systems through automated scanning with manual triaging.

Software Composition Analysis	Secure Design Review
Perform a component-level scan on source or binary code to generate a bill of materials that contains open source vulnerabilities, remediation guidance, and license information. A team of experts also performs a triage of results to remove false positives.	Assess the security of an application's architecture, deployment, and DevSecOps pipeline. Assessments are based on proven AppSec best practices.

Address challenges

Emerging threats across your environment, dynamic application portfolios, and shifting business requirements call for an application security testing plan that adapts rapidly to change and fits your specific risk profile and testing requirements. The 3D Managed AST subscription helps you:

- Measure, refine, and manage risk from software defects
- Address your changing application portfolio (with newly provisioned, updated, or retired applications)
- Meet compliance requirements such as PCI DSS and GDPR
- Tackle your lack of in-house expertise or resources to handle compelling events
- Embed security testing in your development workflows

Focus on actionable solutions

We'll never leave you with a laundry list of bugs. At the end of each assessment, our experts conduct a readout call with the appropriate development or security team to review each vulnerability identified during the assessment, answer questions, and discuss actionable mitigation and remediation strategies.

Scale to your business needs

Even if your application portfolio or testing requirements grow, your expenses won't. The 3D Managed AST subscription is a great way to simplify procurement and budget planning.


Sandex
CONNECTING THE DOTS