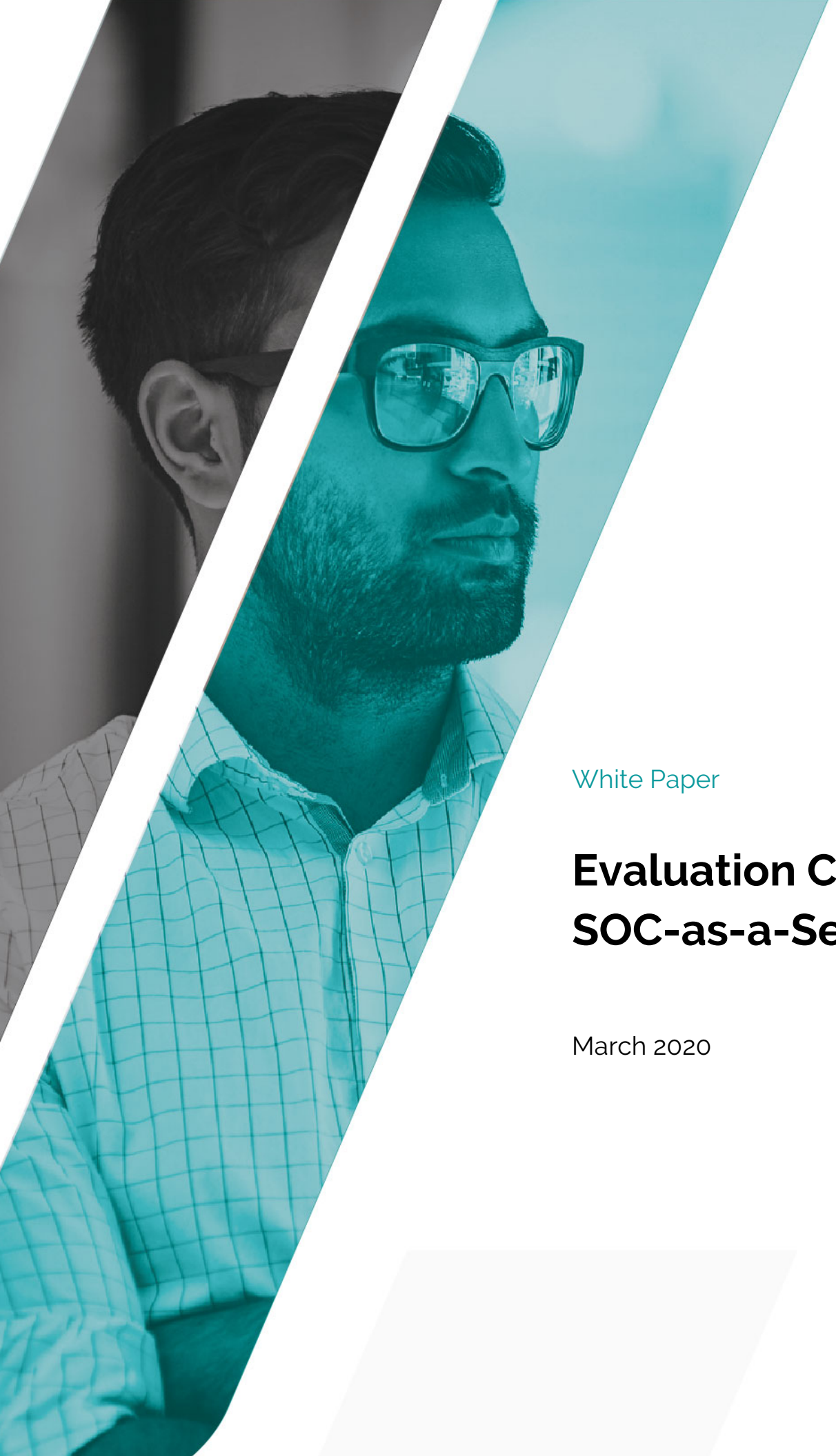

CYSIV

White Paper

Evaluation Criteria SOC-as-a-Service

March 2020

1 INTRODUCTION

A 24/7 SOC is an essential part of an effective cyber security strategy. It identifies, investigates and resolves threats that target your critical infrastructure, sensitive data, intellectual property, and ongoing business operations. The key elements of a modern, world-class SOC are:

- A technology platform that accelerates, and improves the effectiveness of threat detection, hunting, investigation, triaging, case management and remediation
- A team of experts including security analysts and engineers, threat researchers and hunters, data scientists and engineers and incident responders
- Comprehensive and timely threat intelligence and threat research
- Incidence response
- Security device deployment, monitoring and management
- All supported by SLAs, runbooks and playbooks

But building, staffing and operating a SOC with these capabilities is time-consuming, expensive, complex and difficult for all but a few organizations. This is why organizations are increasingly turning to SOC-as-a-Service providers that combine all of the above elements, and deliver them as a service, with consumption-based monthly billing.

When choosing the appropriate SOC-as-a-Service partner, there are a number of important factors to consider, including the SOC technology platform used, its architecture and key features and capabilities, the quality and richness of the threat intel it leverages, the team of experts made available, and the licensing and pricing model.

This document provides a set of important criteria, in the form of questions, that an organization can use when evaluating one or more prospective providers of SOC-as-a-Service.

2 SOC TECHNOLOGY PLATFORM

In the past, most organizations relied on a Security Information and Event Management system (SIEM) as the foundation or core of their security operations. Increasingly, enterprises and MSSPs alike have recognized that a modern technology platform must go beyond the basic capabilities of a traditional SIEM and combine a broad range of essential functions in a single technology platform. There are a number of important aspects to the platform to be considered.

2.1 Architecture

As the world shifts to managing security posture across campus, remote, data center and cloud environments, it's important to ask whether the architecture of the platform that is the foundation for SOC-as-a-Service is up to the task? The way the platform was architected will define its ability to provide the level and quality of service that has become standard in today's modern, cloud-first world.

- Is it a modern, cloud-native architecture?
- Is it a previous-generation, on-premise SIEM?
- Is it cost-effective for low to extremely high Event Per Second (EPS) rates?
- Does the platform architecture support complex, global environments both in terms of performance, maintainability and scalability?
- Does it provide high-availability, failover and redundancy capabilities?

- Does it support rapid release of new features or enhancements?
- For MSSPs: Does the platform support multi-tenancy?
- Dedicated or shared cluster: Is there an option of storing data on a dedicated cluster (typically more expensive, but with greater privacy/security), or a s hared cluster?

2.2 SIEM / Data Lake

Does it enable search efficiently against massive amounts of data captured from a variety of sources, to quickly identify the data most pertinent to forensic investigation? Specifically, does it:

- Support high-scale indexing and storage of forensic data for months or even years?
- Use big data architecture to allow storage of source data in its historical or original form?
- Allow data to be moved to the cloud to take advantage of lower storage costs?
- Provide precise and rapid access to data through high-performance and centralized searches on both structured and unstructured data?
- Meet the anticipated events per second benchmarks during normal and peak times, and support any expected growth?

2.3 Advanced Data Pipeline

An advanced data pipeline ingests logs, data and other telemetry from as many relevant sources as possible. This ensures analysts have a comprehensive and clear picture of what's going on and allows them to more confidently identify genuinely suspicious or malicious activity that warrants closer scrutiny. In general, the more data available, the better that analysts will be able to make important correlations, reduce false positives and improve the confidence in the detections to be investigated. Does the platform support the ingestion of a broad range of data sources and types? Specifically, which of the following systems can feed logs or relevant contextual data to the platform:

- **Security controls**: Data generated by security infrastructure and tools, including:
  - Network IPS/IDS
  - Firewall
  - Endpoint protection platform
  - Server / Workload / Container security
  - Web proxy
  - Email security
- **Infrastructure, monitoring and authentication**: Data used to augment security control data sources; rich endpoint (server/desktop/laptop/ workstation) and user activity data, including:
  - Endpoint detection and response
  - Windows security / Windows process launch / Sysmon / Linux system
  - Active Directory (AD) authentication / Domain Controller / Linux auth
  - IAM / SSO
  - DHCP / Static IP
  - DNS
  - NAT / VPN / Proxy
  - Cloud audit trail
  - Network metadata
- **Log Reduction**: Do they provide a means for streamlining or reducing the logs consumed to help reduce storage (EPS) costs?

2.4 Auto-Enrichment

Enrichment with critical contextual data helps both the system and analysts more quickly and accurately understand the security context and impact of a detection. Which of the following contextual data sources is used to enrich the data:

- **IP attribution** to determine a host's IP address at a point in time, to increase correlation of events generated by the different data sources?
- **Active Directory** object properties to determine a user's role in the organization or the security context of a host?
- **IP address geolocation** data to determine whether network communication is with a known cyber terror organization or nation state, for example?
- **Configuration** data to confirm whether a version of the software/OS running on a system is vulnerable to a detected threat?
- **Asset classification** data to help prioritize the investigation of suspicious detection on a production server, for example, over a development server?
- **Vulnerability scan results**, to ensure time isn't wasted investigating detections for systems that have already been patched (physical/virtually) to shield a vulnerability?
- **Cyber intel** with dynamically assigned confidence scores to assess the maliciousness of a detected threat, as well to identify the Tactics, Techniques and Procedures (TTPs) of a threat actor?

2.5 User and Entity Behavior Analysis (UEBA)

- Does the platform fill in the context of users (peers, title, reporting manager) regardless of the source of the identify (email, directory username)?
- Does the platform leverage machine learning methods to augment and enhance rule-based threat detections with user and entity behavior analytics?

2.6 Automated Threat Detection

- Does the platform leverage a blend of supervised and unsupervised machine learning, rule-based and signature-based criteria, and behavior pattern-match detection methods to automatically identify potential threats?
- **Security Monitoring and Triage**: Alerts the Customer and/or escalates Critical and High severity Security Incidents to Incident Management or Change Management for corrective action, as required?
- **Threat Investigation**: Investigate security incidents to document observables, determine root cause, and impact to compromised systems?
- **Incident Management**: Provide end-to-end support and handling during security incident management: from detection, investigation, containment and remediation, to post-incident activity?
- Can case communication be completed with via email, the technology platform or integration with the Customer's own case management system?

2.7 Integrated Threat Intelligence

Does the platform and process leverage threat intelligence to identify malicious behavior and increase protection over time? Which of the following threat intel sources are leveraged:

- Shared indicators of compromise (IOCs)?
- Open-source intelligence (OSINT)?
- Paid sources?
- Intelligence from thousands of commercially deployed security products
- Intel from Trend Micro Zero-Day Initiative (ZDI) – the world's largest vendor-agnostic bug bounty program for disclosing zero-day vulnerabilities?
- Intel from a top tier research lab, such as Trend Micro Research Labs?

2.8 Cyber Intelligence Sharing Platform

Cyber intel is more powerful when it can be shared amongst a network of industry peers. The threats facing a company in one industry/sector, for example, are often the same ones facing another.

- Does it allow the gathering, sharing, and storing IOCs of targeted attacks, and tactics, techniques and procedures (TTPs)?
- Can it be deployed locally and integrated with the partner's own central threat sharing platform for anonymous intelligence sharing?
- Can anonymized IOCs be shared amongst a network of industry peers to better identify and alert contributing members of the key threats to prioritize?

2.9 Case Management Integration

- Does it provide workflow capabilities, tight integration with existing case management systems (e.g., RSA Archer, Servicenow), transparency, and seamless communication and collaboration during detection handling and incident management?
- Does it provide case management in the same screen as the incident investigation?
- Does it provide case management tailored to the needs of security incident response and security health?

2.10 Dashboards and Reporting

- Does it provide a range of dashboards that are aligned with the needs of different stakeholders (analysts, executives, SLA tracking)?
- Does it provide customizable reports that support compliance requirements?
- Does it provide persona-based information for efficient management?

3 SOC EXPERTISE AND ACCESS

- Which of the following experts do they provide access to, as part of the service:
  - Data scientists?
  - Data engineers?
  - Security analysts?
  - Security engineers?
  - Threat researchers?
  - Threat hunters?
  - Incident responders?
- Do they provide unlimited access to security experts via the case management system, email, and/or phone? Or is it limited to email only, for example?

- Are these experts willing and able to provide knowledge sharing with your security operations team, to elevate their overall proficiency?
- Do they operate and act as a virtual extension of your security operations team?
- Do they provide investigation and remediation support?
- Do they get exposure to a wide range of client situations, and share knowledge such that their level of expertise and insights is constantly improving? Or are they limited and focused to one client?
- Are SOC analysts supported by threat hunters and data scientists that actively work with client data to develop and apply new uses cases that improve detections while reducing false positives?

4 ADDITIONAL SERVICES

Do they provide the following related managed security services:

- **Deployment and Onboarding**: The deployment of any required products (security controls and software required in support of the SOC technology platform)?
- **Health Monitoring and Alerting**: Monitoring of the availability and health of any required products, with alerts if one or more health parameters fall below a threshold?
- **Health Management**: Configuration of any required product system settings for optimal performance and corrective actions, agreed to in advance, on behalf of the Customer?
- **Security Management**: Management of any required products by applying software patches and pattern updates, and policy changes, for optimal protection, agreed to in advance, on behalf of the Customer?
- **Change Management**: Coordination of configuration changes to any required products following a mutually agreed Change Management process?
- **Penetration Testing and Application Assessments**: Testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit?

5 LICENSING AND PRICING

Are there any capital costs associated with the SOC-as-a-Service provided?

For any licenses that may be required in support of the SOC-related services, such as endpoint or server security controls, or network IPS devices, when and how are these license fees charged:

- At the beginning of the contract, with a flat fee in advance, regardless of whether the licenses are actually used during that period
- Or only once the licenses are actually deployed, based simply on the licenses consumed during the previous billing period?
- What is the minimum term (period), for a committed contract?

6 ABOUT CYSIV SOC-AS-A-SERVICE

Cysiv addresses each of these requirements. Cysiv provides SOC-as-a-Service to enterprises that need to better manage cyber risk by accelerating and improving the process of detecting, investigating and remediating threats, and of managing critical security controls.

Cysiv uniquely combines all the elements of a proactive, 24/7 threat hunting SOC–including security and threat experts, global intel, processes and playbooks, and technology–with a managed security product stack, and delivers them as a service, with consumption-based, monthly billing.

Cysiv's cloud-native, next-gen SIEM overcomes the limitations, deployment challenges, and frustrations associated with traditional solutions. It combines essential technologies and functions into a single co-managed platform, and leverages advanced data science techniques to automate the time-consuming, complex but critical activities and processes for truly effective threat detection, hunting, investigation, and remediation.