SOCRadar®

WHITE PAPER

How to Empower Your SOC Team with Cyber Threat Intelligence ?

SOC teams have to monitor, analyze, and manage the great volumes of warnings and alerts created by the networks. It takes too long to go over and investigate these warnings and alerts. Too much alert causes exhaustion and lets analysts take warnings less seriously than required. Many of these are solved by threatening intelligence solutions – helping to quickly and more effectively collect information on incidents, filtering out false alarms, accelerating triage, and promoting incident analysis.

Cyber threat intelligence (CTI) is an innovative method that lets a company gain useful insights into the structural and situation threats associated with the actual threat environment, markets, and industrial processes of the organization.

Threat intelligence will allow the SOC team to determine correctly when preventing attacks and reduce the time taken to detect one. It can also assist the SOC team in determining the urgency to receive executive support.

What is a security operations center?

A Security operations center (SOC) is a centralized unit for the control, identification, and response to security issues and incidents that a corporation may face, whether it is an actual, physical, or virtual organization.

A SOC serves as a node or central control center that uses telemetry from all the infrastructure of an entity, including its networks, equipment, and information centers, wherever these assets are located. The dissemination of advanced threats increases the array of contexts from different sources. In general, the SOC is the point of reference for each case recorded in the monitoring organization. The SOC will determine how to plan and act with each of these cases.

A typical security center monitors a variety of security concerns a company can receive, including possible threats to technologies and resources, as well as employees, partners, and external sources. The SOC then reviews and validates the recorded threat to ensure that it is unfairly favorable. The SOC refers to the security incident to the correct persons or teams for response and recovery if it is considered legitimate and requires a response.

What are the SOC's roles and responsibilities?

The goal of the SOC team is to identify, evaluate, and respond with a variety of processes and technology solutions to cybersecurity threats. A SOC team monitors analyze and manage activities on servers, endpoints, networks, applications, databases, websites, and other technology systems.

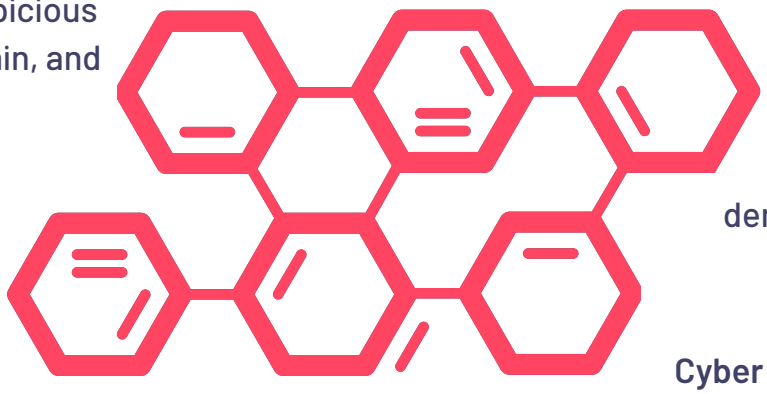
SOC provides a critical analysis layer required to investigate suspicious activities that could lead to a security incident. To avoid simple attacks, technical structures like IPS or firewalls need human experience to respond to serious incidents.

The most critical SOC responsibilities are the following;

Digital Risk Protection
A SOC team responsible to implement and manage security tools for protecting all digital assets, especially critical ones. To achieve this, they also need to investigate suspicious activities, contain, and prevent them.

Attack Surface Management
ASM is continuous surveillance of external digital assets containing, transmitting, or process sensitive data, which are discovered, inventoried, classified, prioritized, and secured.

Identity Access Management
IAM deals with the description and administration of the responsibilities and access privileges of individual Internet users and the conditions in which such privileges are granted (or denied).for the organization.



Incident Response
IR is an organization's technique for reacting to and handling an attack. Incident response. SOC teams are the first responders for cyberattacks in an organization.

Business Resiliency
Company resilience is the ability to rapidly adjust an enterprise to changes while continuing to function and maintaining staff, assets, and brand value. A SOC team is responsible to reduce downtime and ensure business continuity.

Cyber Security Strategy
Since a SOC team has first-hand experience with the cyber incidents and has more technical knowledge than any other department within the organization about the vulnerabilities, they are responsible to help upper management to develop security strategies for the organization.

What are the challenges for SOC teams?

Operational security centers are also the first line of protection for corporate interests and cybercrime. Nonetheless, despite their value, SOCs face four challenges to continue to be the flood barrier between the business and potential vulnerabilities.

Increasing volumes of security alerts: Alert fatigue

With the huge number of security warnings issued, a lot of security alarms consume precious analyst time. Quite frequently, time is wastefully spent to sort and assess the trueness of the warnings, frequently leading to notifications being ignored or to the harmful consequences being lost on the net. As you would possibly imagine, researchers will be better prepared to operate on more advanced alerts and proactively attempt to search to reduce the time from violation detection to resolution

Managing too many tools

When SOCs take a wider range of security systems, controlling all the information generated from the increasing number of data sites and sources is becoming more and more difficult. A traditional safety operations center that uses many different technologies that are understandably difficult to individually track and manage. Therefore it is critical to have a single central source and forum to synthesize all the information produced, and to be able to effectively manage, track and quantify security operations and response processes through the overall security environment.

Making critical decisions

SOC teams will have to make certain choices very quickly in the case of potential intrusions, which means they have to make very critical decisions in a very short time. Urgent requirements for validating which incidents are genuine threats and prioritizing incidents based on their risk. Relating events and programs to particular threats is very difficult. Most of the time SOC teams feel the responsibility of the company's cost when they make wrong decisions.

Why is an effective SOC necessary?

It is important for a committed management team that has the job of continuously tracking security operations and events and reacting to problems, regardless of the size or intent of a company. Within a cybersecurity team, the different duties may be highly complex, and a SOC should not only function as a tactical console to enable team members to execute their daily tasks but also as a strategic core to keep the team informed of broader, longer-term security trends.

How SOC teams use CTI?

The cyber threat intelligence (CTI) is an analytical system or technology to respond to and occur on cyber menaces and attacks based on heterogeneous and detailed data on cyber threats and incidents. CTI is a robust information technology. CTI deals with both the quantity and quality of cyber incidents through preemptive detection that enables SOC teams, even before they happen, to detect them.

Types of threat intelligence for SOC teams

According to Gartner, there are four types of CTI which are tactical, technical, strategic, and operational. It is important to understand the differences among them and the specific ways these are used when building a SOC.

Technical; Data on different IOCs is to be collected (IP address, phishing email header, hash checksum). IOC (Indicators of compromise: clue of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network).

SOC analysts learn clues about attacks through technical intelligence and share this information, allowing new rules to be written for the organization's existing security products.

Operational; Details of an incoming specific attack. Based on automatic updates to the SIEMs, IDSs, vulnerability scanners, and other SOC resources SOC analysts are informed of the current threats in their system.

Tactical; Attackers' methodologies, tools, and tactics. SOC administrators use situational cyber intelligence to consider and identify the techniques and prevention capabilities and strategic objectives of the offensive attacks.

Strategic; High-level information on changing risk. SOC admins or managers review their cybersecurity plan and real-world risk to better understand adverse intentions and trade, make more informed business decisions and ensure alignment.

Use Cases

Focus on actionable alarms: The legacy threat intelligence solution provided only feeds and IOCs which were not actionable. But organizations started to need more and more the latest intelligence about themselves. With real-time intelligence on threat actors, botnets, and malware, as well as data from the dark web and the deep internet, organizations need to detect phishing domains targeting their customers. The SOC analyst has to spend considerable time extracting specific threats from the external threats he actively collected. It takes hours to take advantage of OSINT tools.

For instance, e-commerce companies face two main types of phishing: attacks against their customers and employees. SOC teams try to get feeds on phishing domains that can target company employees. On the other hand, they do continuous training and simulations to prevent phishing. However, 90% of these domain names appear to be targeting customers outside of their environment to steal credentials or sell illegal products using the brand name. When attackers successfully perform the attack, the company's costs include the reimbursement of stolen loyalty points, time to regain customers' trust, and handling the customer's complaints which can often extend to social media.

That's why SOC teams need an autonomous solution that leverages big data technology to process data collected from the surface, deep, and dark web sources, including code repositories, social media, chat sites, sticking sites, and deep/dark web black markets.

Automatically collect, verify and prioritize external threats: SOC teams must always be aware of external threats and be able to inform their organizations of these threats.But with the current workload, data collection processes create a really big workload. On the other hand, false positives harm the operational processes of companies. Among the thousands (or millions) of alarms, alerts, and events, which ones really matter? CTI can deliver the hard work for SOC teams with enriched intelligence that allows you to apply smarter research and improvement processes. By mapping alarms and events to threat intelligence, SIEMs, log management, and security analytics tools can achieve machine-speed first-line alarm prioritization. For example, SOC teams can create SIEM rules that match observable threat indicators found in the corporate network and target the threat intelligence business sector, geographic areas of operation, software applications, or infrastructure components that link these indicators to threat actors or campaigns. When matches are found, SIEM automatically increases the priority of this alert or event, allowing SOC teams to "take into account" threats to their business. This frees SOC analysts from the labor-intensive task of sorting out tens of thousands of low-level and irrelevant alerts every day.

Detect forgotten assets and monitor attack surface in real-time: SOC analysts often have limited monitoring visibility in cloud environments, which hinders their ability to effectively discover malicious activity. However, they must determine the blind spots by following the changing attack surface all the time. Because there is a constant vulnerability regarding the assets that companies use, the company shuts down it, but another one continues to be published. It is one of the important duties of SOC teams to follow this situation and report it to the relevant departments, but it is not that easy. For example, the possibility of the presence of an unknown digital asset, an open RDP port, or vulnerability that could be exploited by adversaries was keeping the SOC team up at night.SOC teams are now aware that it is difficult to manage security risks associated with the changing attack surface while dealing with other routine manual analysis and review tasks, and the need for automation is evident. Attack surface management helps SOC teams gain additional visibility and context regarding the severity of unknown external-facing digital assets in an automated manner.

SOCRadar provides SOC teams unified digital risk protection and threat intelligence platform

SOCRadar combines attack surface management, digital risk protection, and threat intelligence capabilities to support SOC teams.

SOCRadar ThreatFusion provides actionable insights into future cybersecurity threats with a big data-powered threat investigation module to assist in searching deeper context, real-time threat investigation and analysis. SOC teams, threat intelligence analysts, and incident response teams can integrate with SIEM and SOAR platforms to leverage threat flows such as IOCs, malicious IP addresses, DDoS attackers, APT groups using SOCRadar to improve their security posture.

SOCRadar RiskPrime builds on industry-leading instant phishing domain identification, internet-wide scanning and compromised credential detection technologies by aggregating and correlating massive data points into actionable intelligence alerts. SOCRadar constantly discovers its outside-facing digital assets to eliminate blind spots and shadow IT risks, and informs SOC teams with fast and targeted intelligence.

SOCRadar AttackMapper provides insight and visibility into these assets to discover and monitor everything related to your organization on the Internet to bring the enormous scale of your attack surface into focus. Through SOCRadar's advanced internet-wide monitoring algorithms, AttackMapper provides SOC teams with direct visibility into all internet-facing technological assets in use as well as assets attributed to IP, DNS, Domain, and cryptographic infrastructure.

Start your free trial now !

Sign up for a test drive to try out SOCRadar free for 14 days.

SOCRadar®

Gartner peerinsights™ 4.9 ★★★★★ OUT OF 5 STARS IN 7 REVIEWS AS OF 06/2020

4000 Legato Road, Suite 1100
Fairfax, VA 22033 USA

+1 (571) 248-4598

info@socradar.io

www.socradar.io

SOCRadar delivers intelligent digital risk protection platform against sophisticated cyber attacks for organizations of any size. Its portfolio of digital assets and perimeter monitoring platforms hardened with targeted threat intelligence – all automated and supported by a global team of qualified intelligence analysts – provides unparalleled visibility, management, and protection of digital risks. Prioritized, up-to-date, and relevant cyber threat insights empower customers to take action starting from the reconnaissance stage of the cyberattack life cycle