

An abstract graphic consisting of several thick, glossy red ribbons that loop and swirl together, creating a sense of motion and depth. The ribbons are set against a light pink background that transitions into a darker pink at the bottom.

HOW INFINITY SOC DELIVERS A ZERO FRICTION IMPLEMENTATION

This document outlines the fast, non-intrusive implementation mechanism of Check Point Infinity SOC, a cloud-based platform that delivers efficient log-less incident analysis for security operations center (SOC). Easily deployed with zero friction, it increases security operations efficiency and ROI while avoiding costly log storage and privacy concerns with a revolutionary event analysis that does not export or store logs.

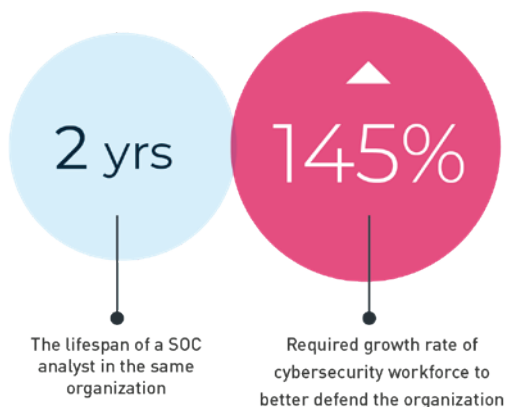
What Is SOC?

The function of the security operations center (SOC) is to monitor, prevent, detect, investigate, and respond to cyber threats around the clock. SOC teams are charged with monitoring and protecting the organization's assets including intellectual property, personnel data, business systems, and brand integrity. The SOC team implements the organization's overall cybersecurity strategy and acts as the central point of collaboration in coordinated efforts to monitor, assess, and hold a strong posture against cyberattacks.

Outsourcing SOC Services

SOC teams are deluged with an infinite number of logs and security incidents as the threat landscape continues to evolve ruthlessly. Unfortunately, Maintaining and cultivating the required skills for SOC takes a significant amount of time and budget as it takes time to become conversant with an organization environment and the security challenges it holds. On top of that, there is an increasing chance of an employee turnover as the lifespan of the SOC analyst in the same organization is a little more than two years¹. This combination makes it hard for an organization to keep up with the turnover not to mention the capital expense (CAPEX) that keeps growing e.g. servers, log storage and backup hardware.

From security perspective, the (ISC)² Workforce Study estimated that the cybersecurity workforce



needs to grow by 145% to close skills gap and better defend organizations worldwide². These are the main reasons why many organizations choose to minimize the cost and operational overhead and close the lack-of-cybersecurity-skills gap by outsourcing SOC services completely or use one of the SOC as-a-service solutions available.

Outsourcing Security Services Onboarding Challenges

On a broader level, involving a 3rd party vendor or an MSSP to partake the SOC or any security related aspects of an enterprise has many benefits e.g. reduced cost, quality of personnel with minimal learning curve and an easy scalable deployment delivered in operating expense (OPEX) mainly.

The main challenges of using any of the outsourced solutions revolve around the onboarding process which includes a full data sharing agreement with the chosen vendor. This is mandatory in order to be able to deliver superior security services but might lead to increased operational costs (in order to ensure alignment with both data and security regulations). Furthermore, in order to improve SOC operational efficiency, additional tools need to be implemented inside the network in order to increase the volume of logs and audit trails for the analysts to consume. This means additional overhead. The main challenges in the onboarding process are explained in the following sections.

Sharing Enterprise Sensitive Data

In the world of cybersecurity there are two premises: 'Data privacy is at the heart of every business' and 'almost every business has experienced or will experience a data breach in the near future'. Those are the main reasons why organizations take an extra step and counter cybersecurity threats by establishing SOC systems on top of their existing solutions to monitor their systems and detect potential security incidents.

But not every organization has the resources to set up an internal SOC by employing a sizable number of SOC analysts and security personnel and using dedicated hardware and software. Some choose to

¹ Kelly Sheridan, 2020, For Mismanaged SOCs, The Price Is Not Right, Retrieved from <https://www.darkreading.com/risk/for-mismanaged-socs-the-price-is-not-right/d/d-id/1336864>

² (ISC)², Strategies for Building and Growing Strong Cybersecurity Teams, Retrieved from <https://www.isc2.org/Research/Workforce-Study#>

OUTSOURCING SECURITY SERVICES ONBOARDING CHALLENGES

Sharing Enterprise Sensitive Data



outsourcing their entire SOC services or outsourcing only the SOC platform (as-a-service).

Every SOC vendor that offers managed SOC services or SOC platform as-a-service, receives raw logs from the enterprise for monitoring and analysis purposes as they are the key source of information for analysts. This dependency might create compliance or confidentiality issues as some organizations can't share logs that unveil sensitive information regarding their network, endpoints and cloud e.g.

- Entire internal segmentation and layout
- Hosts names and user names
- Internal business-related files and sensitive repositories
- Application usage (include sensitive categories and applications employees are using)
- All network assets and entities (databases, Servers, endpoints and desktops)

Cost of logs Delivery

Gartner claims: "creating some form of internal security operations capabilities — is a costly and time-consuming effort that requires ongoing attention in order to be effective"³. This is one of the reasons why enterprises are opting for managed or outsourced SOC via a 3rd party vendor. But what seems like a controlled cost solution has hidden disadvantages when it comes to sending logs to a 3rd party vendor. The complexity of the IT infrastructure, the diversity of the environment (whether expands to mobile and cloud) and the organization headcount has a material

Cost of Logs Delivery



effect on the log volume sent for SOC analysis. The higher the log numbers, the costlier the SOC is to maintain in terms of infrastructure, scalability and security as cost is usually extrapolated by events per second (EPS), number of protected assets or type of SOC services/Package.

Security and Regulations Considerations

Outsourcing an imperative part of the security operations like SOC means all raw logs will be directly fed to the analysts systems in real-time and stored for analysis outside the enterprise perimeter. As SOC analysts rely heavily on scanning raw logs, it is necessary that confidential and strategic data regarding the network (both on-premises and cloud based), endpoints and the entire workforce will be under the jurisdiction of that 3rd party vendor. The implications of this necessity can be broken in to two perspectives.

Shared Security Responsibility

The 3rd party SOC vendor is responsible of all aspects of security related to the enterprise data it holds (with not involvement from the enterprise). It means that enterprise data is no longer stored on-premises thus access is gained from the outsourcer SOC framework. The risk of unauthorized disclosure where sensitive information is exposed to unauthorized personnel is out of the control of the enterprise. Moreover, If the SOC framework was

Security & Regulations Considerations



³Siddharth Deshpande (October 12 2007). Security Operations Centers and Their Role in Cybersecurity. Retrieved from <https://www.gartner.com/en/newsroom/press-releases/2017-10-12-security-operations-centers-and-their-role-in-cybersecurity>

breached, the enterprise data will be compromised.
Data Localization Regulations

Over the past few years many countries have made a noticeable progress with regards to enacting laws and set regulations concerning data localization and data sovereignty to make sure personal data regarding citizens (mainly related to Personally Identifiable Information – PII) will not leave the country e.g. chapter 5 (article 44) of the GDPR⁴. This means that all personal data will stay stored or will be processed in-country only. This creates a logistical and legal complexity when employing the services of an international 3rd party SOC vendor that stores all data for analysis in an external location outside the permitted region.

It's time for a change: Log-less Analysis Solution

Whenever Check Point security gateway (whether on-premises or cloud-based) or enforcement point (residing on endpoint or mobile device) encounters a suspicious activity, it queries Check Point ThreatCloud in order to determine whether this is indeed a malicious act or not. ThreatCloud is a collaborative network and cloud-driven knowledge base that delivers real-time dynamic security intelligence to security gateways.

Check Point Infinity SOC circumvents the inherited challenges described earlier by using data from the queries sent by Check Point security gateways

to ThreatCloud. Each query includes connection-related data only so no private data is shared as it is irrelevant to ThreatCloud big-data analysis process. Infinity SOC automatically analyzes the queries' meta data (e.g. time of connection, connection rate, patterns and more) in order to identify malicious behavior and provide relevant insights, triage of alerts and remediation instructions accordingly.

What is Infinity SOC

Check Point Infinity SOC is a unique cloud-based SOC platform that provides 99.9% precision rate in exposing and shutting down only real threats from millions of logs and alerts powered by AI based incident analysis. It enhances response to severe threats with automated triage, using ThreatCloud threat intelligence repository and offers a single-click remediation. It also offers a centralized portal with a Google-like search for any indicators of compromise (IoC) to obtain rich, contextualized threat intelligence that includes geographical spread, targeted industries, attack timeline and methods. All these exclusive investigation tools were developed by Check Point's Research Team to expose and investigate sophisticated cyber-attacks, including deep-link searches on social media and open-source intelligence (OSINT) to find and surface relevant information from web pages and documents for a deeper investigation.

AI based Incident Analysis

Existing detection tools do not provide SOC teams with the certainty they need to detect critical attacks quickly

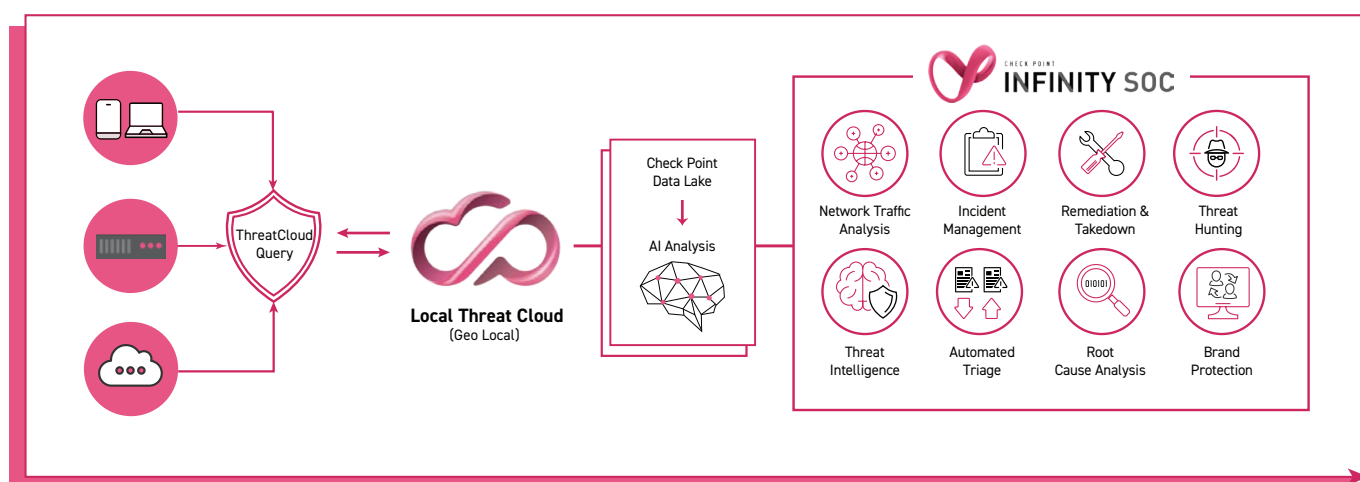


Figure 1: Infinity SOC – Analysis flow and SOC Services

⁴European Parliament and Council of European Union (2016) Regulation (EU) 2016/679. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e4227-1-1>

enough Methods like 'rule-based' or behavior analysis (anomaly detection) either miss critical incidents too often or create too many false positives. Infinity SOC leverages a multi-layered approach to detection:

- Enterprise-wide visibility: analyzing network, cloud, endpoint, mobile, and IoT events over an extended period of time.
- External threat visibility: leveraging ThreatCloud's global visibility into real-time internet traffic to detect external threats outside the organization.
- Threat Intelligence: enriching every alert with threat intelligence and the power of ThreatCloud, and connecting the dots with big data

analysis to uncover the most sophisticated attacks like APTs.

- AI-generated verdict: running AI-based incident analysis on top of the aggregated information (from all the layers mentioned above) to accurately determine whether the event relates to malicious activity. Infinity SOC AI-based engines have been trained and validated by some of the world's largest SOC's.

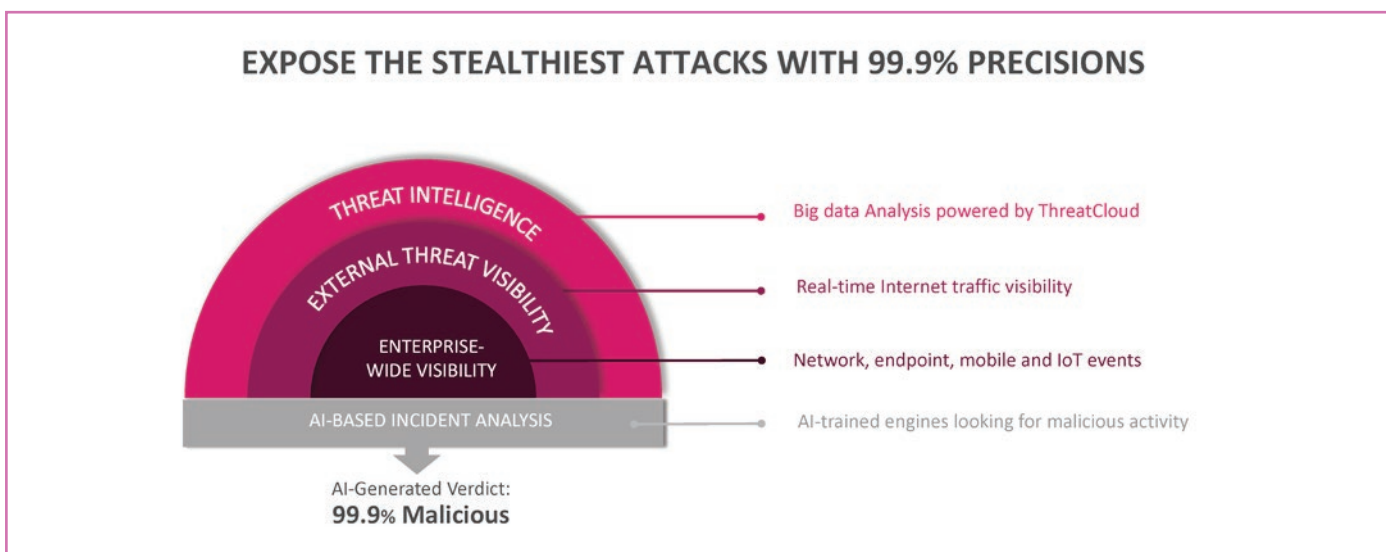


Figure 2: unmatched visibility into threats inside and outside the organization

Why Customers Should Consider Infinity SOC

With its inherited integration with any of Check Point security framework and tools used by enterprises and security teams, Infinity SOC offers a simple, unique onboarding process to enable AI based incident analysis with automated triage and a single-click remediation. Dedicated or internal security teams can use the tools provided by Infinity SOC to perform in-depth investigations with highly processed threat intelligence including global spread, attack timelines and patterns. Infinity SOC addresses the following customers challenges:

Zero Friction

Most of SOC products rely on endpoint or network

sources, which mean hard implementation labor switching or adding a SOC product to the existing infrastructure. Infinity SOC does not require the deployment of additional endpoint agents or redesigning infrastructure to securely send business critical data to a 3rd party vendor. The onboarding process includes allowing Infinity SOC to use the gateway identifiers and statistics already sent to ThreatCloud.

Flexible Framework

Infinity SOC is a scalable, flexible cloud-based platform that relies on ThreatCloud, a real-time threat intelligence derived from hundreds of millions of sensors worldwide, enriched with AI-based engines and exclusive research data from the Check Point Research Team. Since Infinity SOC ingests data and meta-data from enforcement points' queries,

alignment with any data security or sovereignty laws, regulations and corporate policies is achieved effortlessly as:

- No business-critical data is sent off-premises.
- All ThreatCloud queries are automatically saved in the relevant region the customer is obliged to legally.

Increase effectiveness by using automation and simplification of SOC processes

Real-time investigation and AI based incident analysis is provided to security teams and analysts within a cloud-based platform. In addition, various widget-driven investigation dashboards are available for searching on any IOCs to obtain rich, contextualized threat intelligence that includes geographical spread, targeted industries, attack timeline, and methods e.g. example-campaign files, communication files, typical file names used, and network activity commonly associated with the IOCs)

Threat Cloud Queries

ThreatCloud Query vs. Raw Log:

When a host, user, IoT device or any kind of network asset tries to connect or communicate with a domain or IP address and encounters a suspicious response (e.g. downloading malicious file, browsing to a dubious site), the security gateway (or enforcement point) queries ThreatCloud whether the suspicious entities are indeed malicious or not. This query is not saved in Check Point Threat Cloud by default.

By changing the gateway properties in the security management to allow saving and analyzing the query, Check Point Infinity SOC is able to run its unique Machine Learning modules to alert and triage the malicious activity that has been detected. The query contains the following structure of data: In the data sent you can see the following important fields:

- Source IP – obfuscated (can be deobfuscated only in the GW level) – Real IP of the host is not needed thus not sent.
- Host – the malicious location the source IP was connecting to
- Destination IP – the destination of the Malicious Host

```
<entry sigID="319970" sourceIP="b4bbc4c271b0d76c5400ccbeb6f58435"
destinationIP="122.11.14.1" engineType="3" destinationPort="80" numOfAttacks="51" tran_proto="6"
payload_length="265" start_time="1594711322" end_time="1594711322" bot_name="Trojan-Spy.WIN32.aa"
host="suspicioussite.xyz" path="/abc.crl" user_agent="Microsoft-CryptoAPI/10.0" http_resource=""
http_server="" _http_referrer="" _http_location="" _http_content_type="" _http_content_disposition=""
_http_x_requested="" _http_via="" _http_content_length="" _http_method="GET" _http_status="" _http_
authorization="" _http_hff_header="122.11.14.1" http_url="http://suspicioussite.xyz/abc.crl" _
dns_question_rdata="" _dns_answer_rdata="" _dns_authority_rdata="" _dns_additional_rdata="" dns_host=""
_ftp_user_name="" _file_name="" _file_extention="" _file_type="" _file_md5="" protectionId="" sigName=""
CVElist="" DescriptionUrl="" attackInfo="" attackName="" vendorsHex="" />
```

Figure 3:ThreatCloud Query Example

Conclusion

For many SOC teams, finding malicious activity inside the network is like finding a needle in a haystack. They are often forced to piece together information from multiple monitoring solutions and navigate through a daily overload of alerts with little or no context. The result: critical attacks are missed until it's too late.

Infinity SOC uses the power of AI to accurately pinpoint real attacks from millions of daily logs and alerts, expose and shut down attacks faster, before damage spreads. Easily deployed as a unified cloud-based platform with zero friction (avoiding costly log storage and privacy concerns), it increases security operations efficiency and ROI.

Start a free trial now at portal.checkpoint.com or to get more information about Check Point Infinity SOC, please visit us at <https://www.checkpoint.com/products/infinity-soc/>