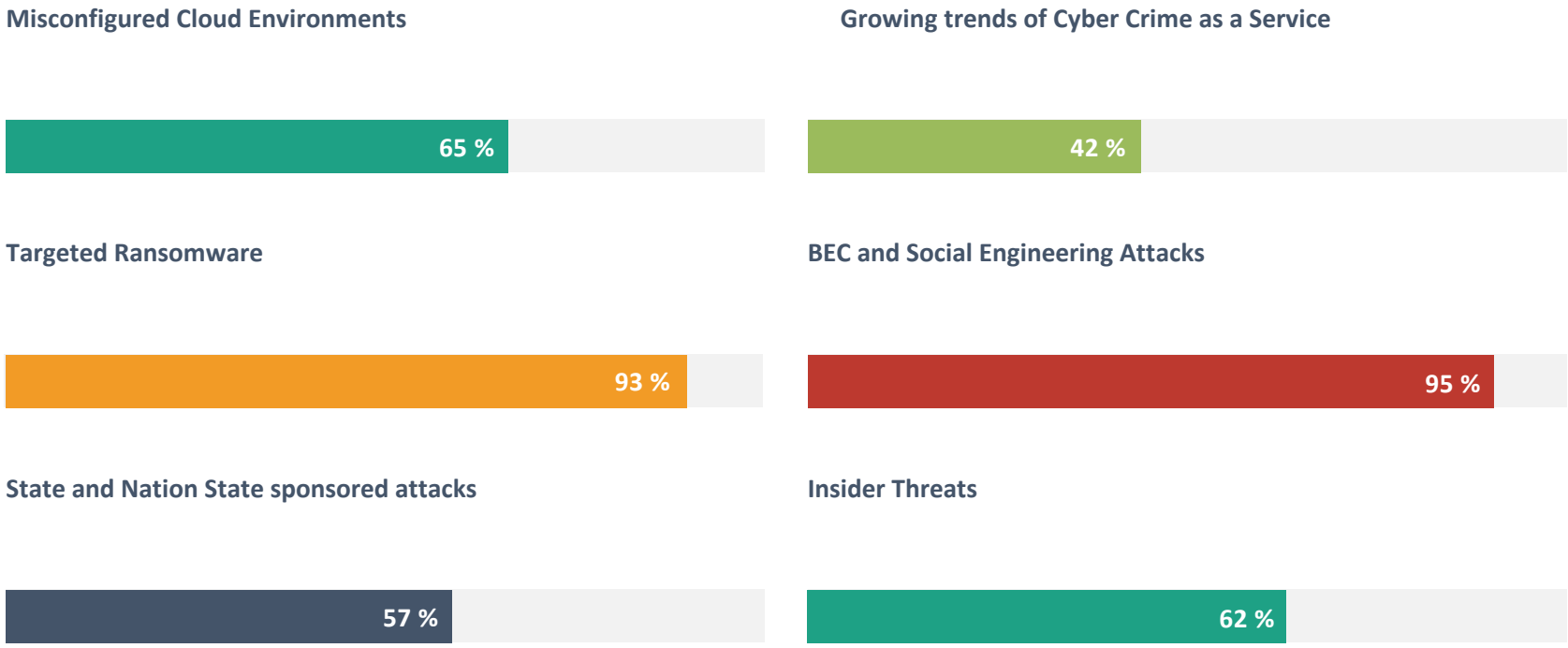
Cyber Security Trends

While businesses continue to adopt preventive measures to detect and thwart cyber attacks, a majority of the times, it's observed that the attackers are still able to penetrate and/or bypass these preventive measures.

The below chart shows the cyber security trends of 2020



Top Challenges faced by a Traditional SOC

IMPORTANCE OF THREAT HUNTING

One of the fundamental problems with cyber security is that most organizations do not realize when they are compromised. Traditional Incident Response plans are typically reactive in nature. In-fact, most of the times, we've been engaged by our customers only after a breach has happened. This approach basically forces the security teams to wait for a visible sign on an attack, and in today's threat landscape, threats are often stealthy, targeted and data-focused.

Threat hunting is the act of tracking and eliminating cyber adversaries from your infrastructure as early as possible. While it becomes increasingly difficult to eliminate every threat to an organisation, it becomes very important in that case to have an early detection , response and remediation in place

Threat Intelligence and Hunting Meets SOC

Because detecting and hunting threats intelligently is the need of the hour

A traditional SOC doesn't have the required capability to present an enterprise wide view and a correlation engine to hunt, detect and respond to emerging threats

While a traditional SOC is built to on top of a SIEM, where events are ingested and a set of pre-defined rules are used to detect anomalies within an IT environment.

Our TH-SOC integrates threat hunting SOC is built using the MITRE ATT&ACK framework. Our SOC aims to help you not only gain visibility across your entire IT environment, but also help you detect and respond to advanced threats and evading techniques often used by attackers. Our TH-SOC has the following capabilities:

Unified Response Centre

Our integration with multiple threat intel sources will enable responders to conduct a centralized and thorough investigation

Intelligent Correlation and Attack Mapping

We provide a single glass of pane for analysis by supporting ingestion of logs from all sources, cloud, on-premise infrastructure, applications, and containers

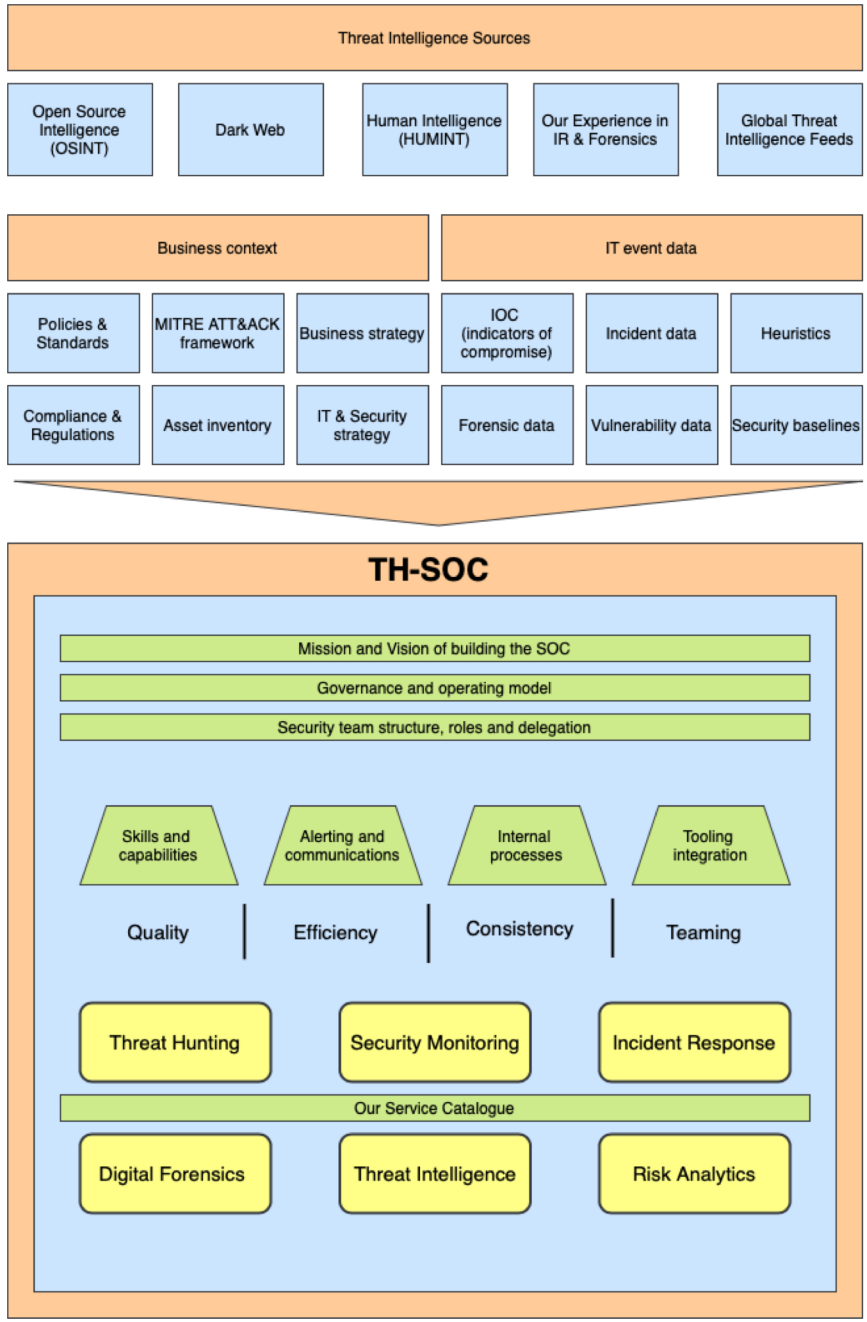
Timeline plotting

We provide the responder with an ability to intelligently predict the timeline from when the first anomaly was detected to the incident occurring in the environment

AI based analytics

Our AI embedded into this platform will be able to churn the data being ingested into our platform and help the security team predict potential entry points that could lead to an incident

Our TH-SOC architecture and design



Our Threat Intelligence Sources

OSINT

The purpose of integrating OSINT is to gather more information about the threat/adversary

DB of blacklisted/malicious hosts

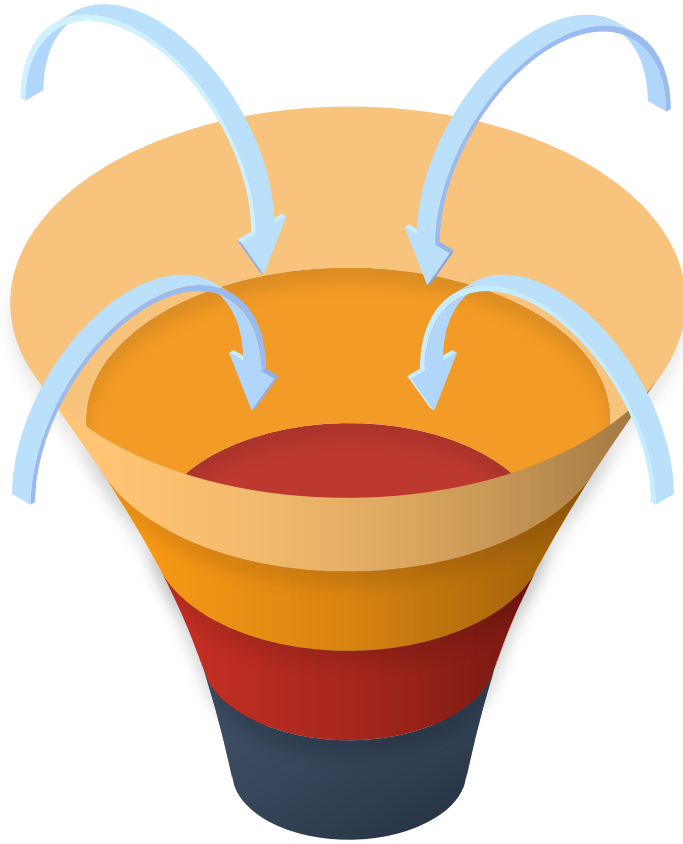
As soon as an anomaly is detected in terms of a suspicious IP or a process, we want to enable the responder(s) to quickly identify whether the Source/Destination IP address is a known malicious address, or if the processes hash is that of a known malware/APT

Deep Web Intelligence

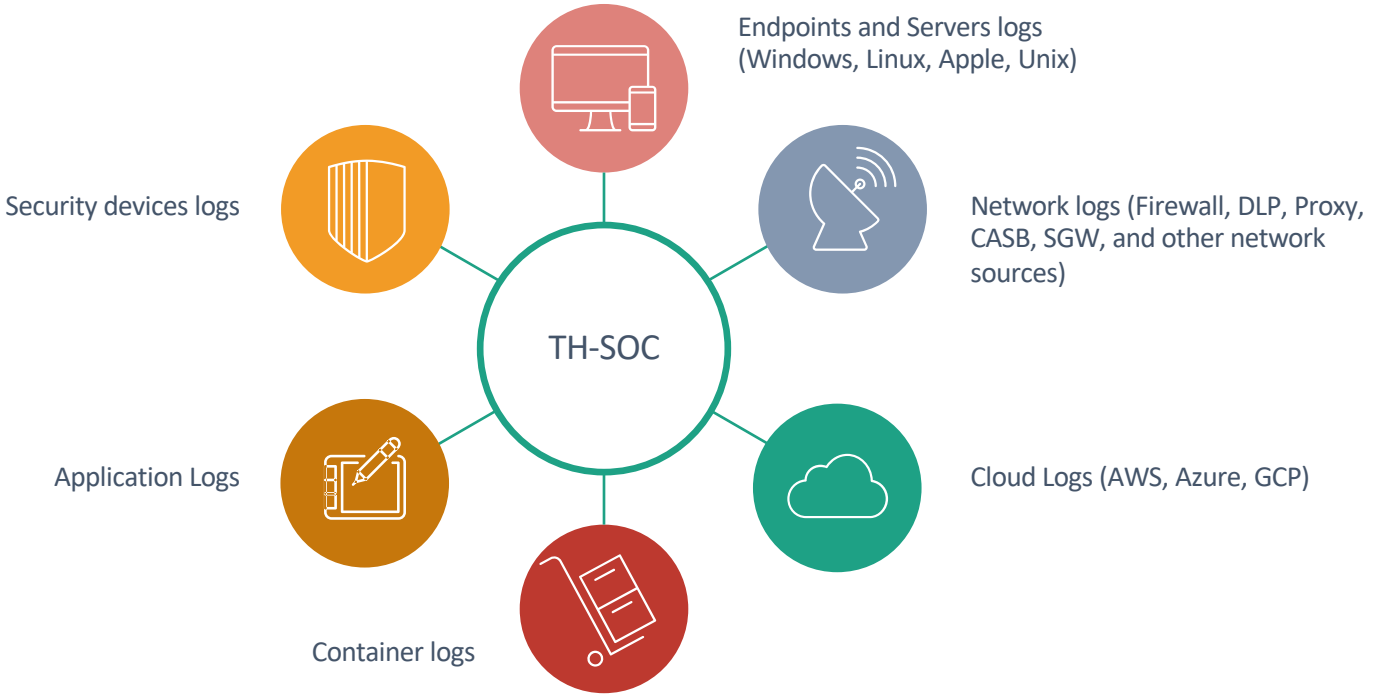
Our deep web intelligence will enable the responder to fetch further details about the host/IP addresses in question. It'll provide information such as whether the email addresses of the business, or names of their employees and other such data is available on the deep web.

Data compromise intelligence

Using sources such as HaveiBeenPwned and DataHash, we want to provide the responder with further intelligence to understand the impact of the breach so that an appropriate action can be taken to respond and remediate the threat



Input Log sources



But Wait – we go a step further

Our TH-SOC not only helps responders detect anomalies, but also helps them automate response actions, and maintain the security posture of their IT environment

Centralized Asset Inventory

A centralized inventory of all your assets that might be spread across the cloud, on-premise data centers, and even micro-services

Intelligent Threat Hunting

We provide threat feeds from various sources that provide insights to the responder regarding the flagged anomaly

Endpoint Behavior Analytics

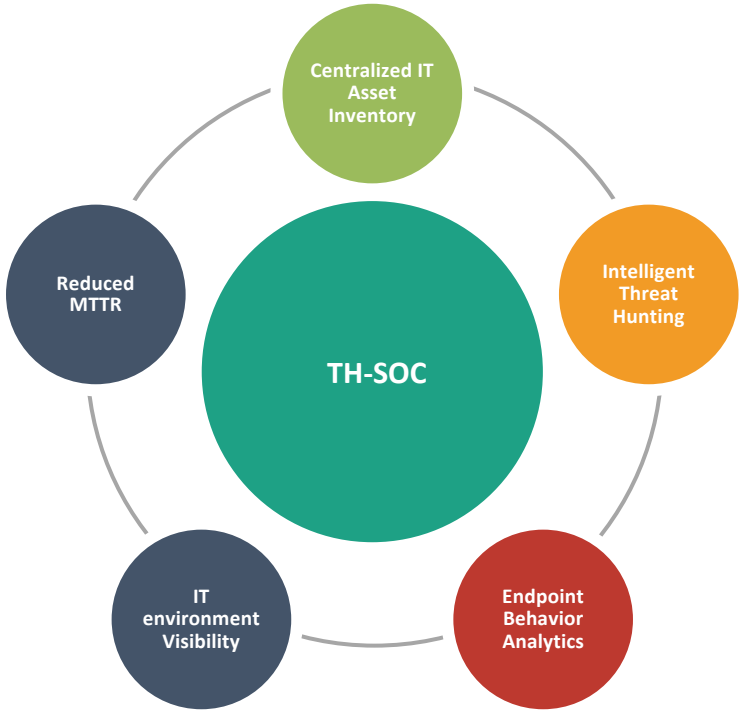
We provide intelligent insights into how endpoints are behaving and help responders detect a rogue endpoint that may be the source of the origin for the incident

IT environment Visibility

Our threat detection and response platforms aims to help you get complete visibility on the extent of the breach

Reduced mean-time-to-respond

Our platform will enable responder to swiftly respond to incidents, thus reducing the time required to respond to an incident. We also automate response actions such as blocking or deleting of files, processes, or even network traffic



Our Process of Threat Hunting & Response

STEP 01

Continuous ingestion of logs from multiple sources

STEP 02

Pre-processing of this data by our intelligent parsers

STEP 03

Integrate TI meta-data into the parsed information

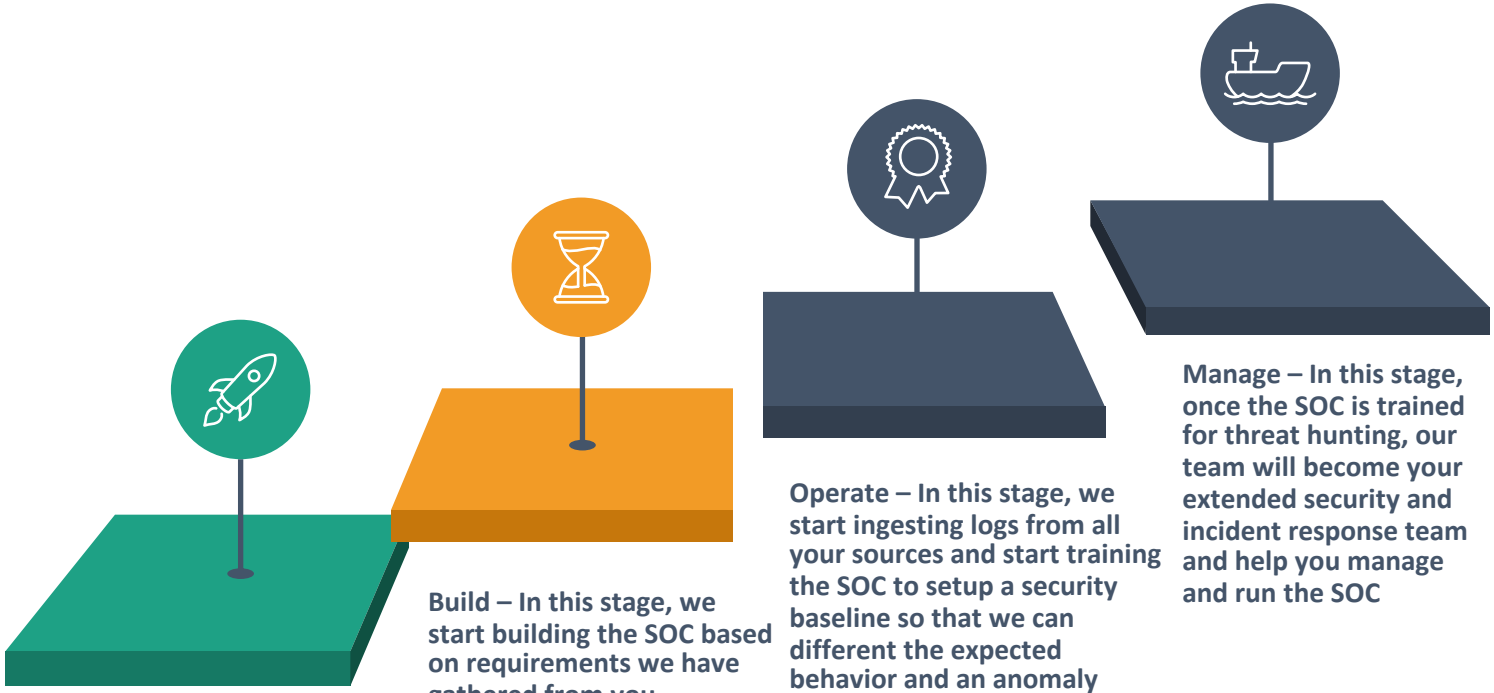
STEP 04

Create intelligent dashboards for IR to view on a near-real time basis

STEP 05

Continuous monitoring and threat emergence prediction

Our DBOM delivery model



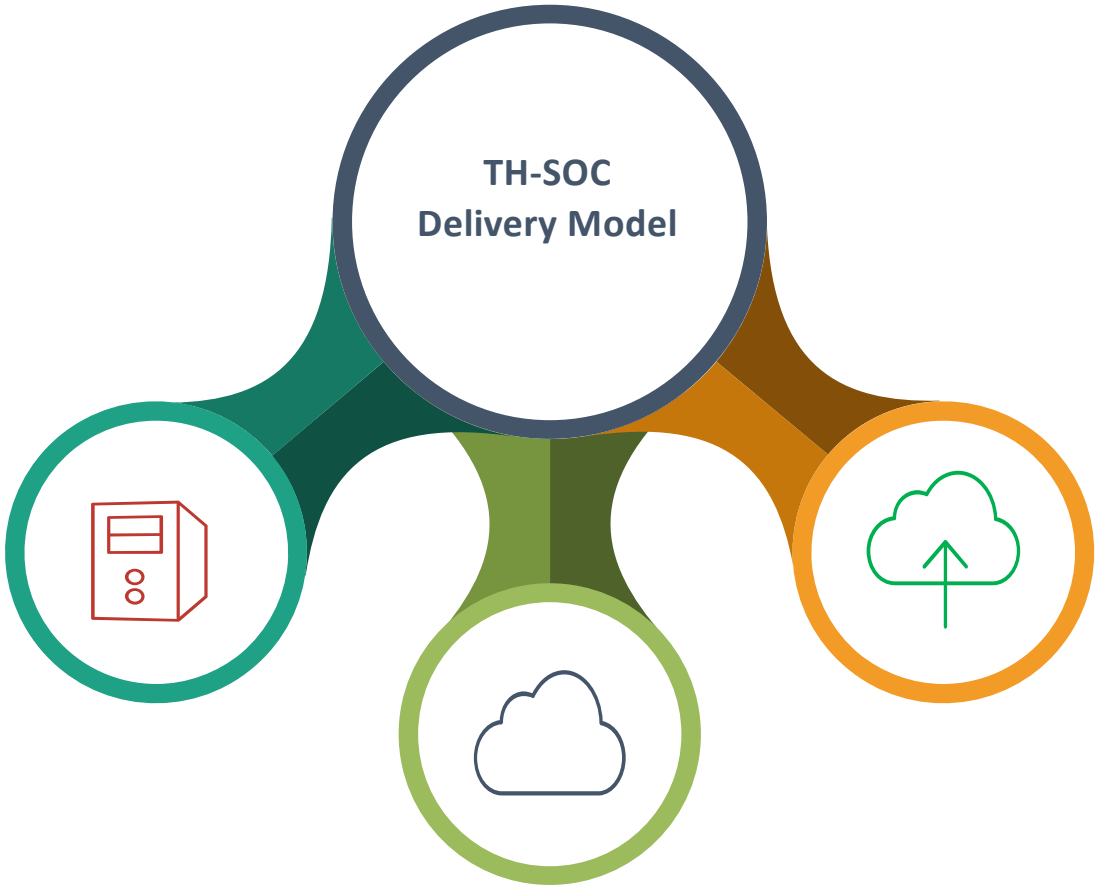
Design – In this stage, we study your requirements so as to start building a SOC as per your requirements

Build – In this stage, we start building the SOC based on requirements we have gathered from you

Operate – In this stage, we start ingesting logs from all your sources and start training the SOC to setup a security baseline so that we can different the expected behavior and an anomaly

Manage – In this stage, once the SOC is trained for threat hunting, our team will become your extended security and incident response team and help you manage and run the SOC

Our DBOM delivery model



Deploy in your Data Centre

For customers who are wanting to run a SOC on their own Data Centre, we support deploying on-the-floor SOC.

In this case, we will help you deploy, setup, configure and manage the SOC for continuous threat hunting ,detection and response purposes.

Deploy in your cloud environment

For customers who want the flexibility and features of the cloud, we support deploying on-the-cloud SOC.

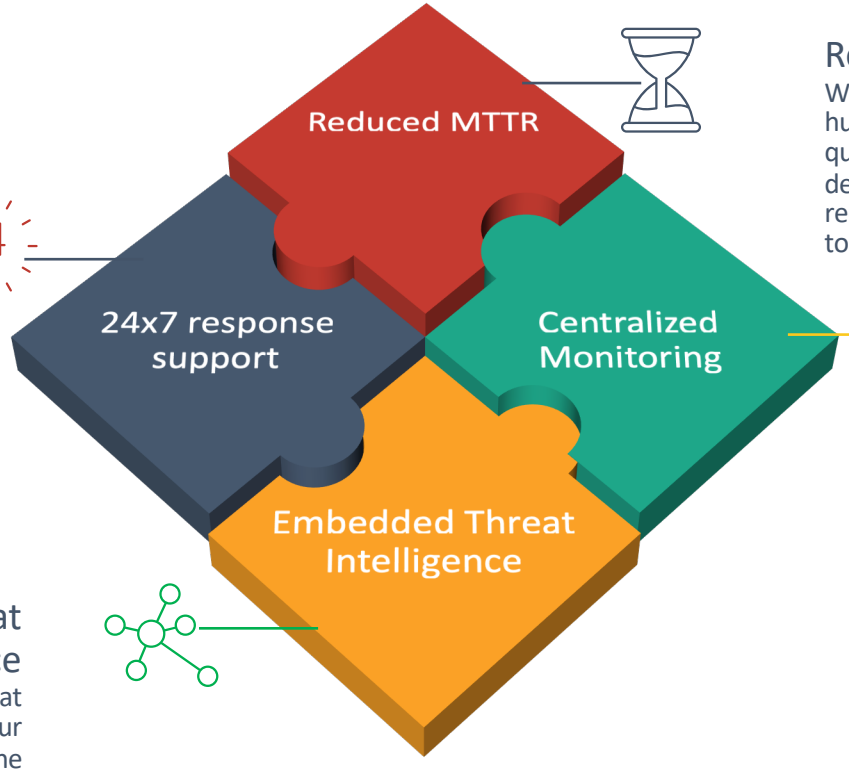
In this case, we will help you deploy, setup, configure and manage the SOC in your own cloud environment. In this case, we will manage the SOC for you for conducting threat hunting, detection and response purposes

Deploy in our cloud environment, use it as a service

For customers who want the flexibility and features of the cloud but do not have a cloud account and do not want an overhead to maintain a cloud account. We will deploy the SOC in our cloud environment and give it to you as a deployed and fully managed service

Our Managed Threat Hunting SOC

Value additions of TH-SOC



Reduced MTTR

With our continuous threat hunting capability, we enable a quicker incident/threat detection, overall resulting in reduced mean-time-to-respond to incidents

24x7 response support

Our team of security analysts will always be on standby to quickly detect and respond to incidents

Centralized monitoring

The TH-SOC will become a central platform for monitoring and detecting threats across your overall IT environment that may consist of your data-center, cloud environments and even application data

Embedded Threat Intelligence

By embedding our threat intelligence feeds with your event data being ingested into the platform, we provide an enhanced ability to detect anomalies and threats

Our SLAs and response time

Request Type	Response time	Triage time
Severity 1	30 Minutes	Within 45 Minutes of alert generated
Severity 2	60 Minutes	Within 75 Minutes of alert generated
Severity 3	90 Minutes	Within 100 Minutes of alert generated

Severity type and description

Severity type	Description
Severity 1	A critical incident with a very high impact on the business. For example, a data breach where customers PII information is stolen
Severity 2	A major incident with significant impact on the business. For example, a ransomware attack where your computers are locked
Severity 3	A minor incident with low impact on the business. For example, A virus of malware infection on an independent workstation that is not connected to your corporate network or an evidence of port-scan

Support Helpdesk

Support type	Description
Email	report@trixter
Call	+91-7045658564 (For Severity 1)

RACI Chart

RACI Chart Response tasks	L1 responder	L2 responder	L3 responder	Response Manager
Identify potential Malicious events	R	R	C	A
Malicious traffic/events hunting			R	A
Collect & Document supporting logs		R	R	A
Triage	R	R		A
Initiate deep response			R	A
Analyze host machine			R	A
Create and update activity checklist		I	R	A
Document Investigation analysis		I	R	A
Lessons learned and reporting		R	R	A