How to Build, Run and Measure a SOC?

2022

Cetas

Speed to insigns and action

CONTENT

Email sales@cetascyber.com
cetascyber.com

What is a SOC?

A Security Operation Center (SOC) is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

A SOC acts like the hub taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside. The proliferation of advanced threats places a premium on collecting context from diverse sources. Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon.

SOC Deployment Models

Deployment Models	
Dedicated SOC	Classic SOC with dedicated facility, dedicated full-time staff, operated fully in house, 24×7 operations
Distributed SOC	Some full-time staff and some part-time, typically operates 8×5 in each region
Multifunctional SOC/NOC	A dedicated facility with a dedicated team which performs both the functions of a Network Operations Center (NOC) and a SOC
Command SOC/Global SOC	Coordinates multiple SOCs in a global enterprise (if there are more than one), provides threat intelligence, situational awareness, and guidance
Managed SOC/MSSP/MDR	Many organizations are turning to Managed Security Service Providers (MSSP) to provide SOC services on an outsourced basis. Modern offerings are called Managed Detection and Response (MDR). Managed SOCs can be outsourced completely or co-managed with in-house security staff.

Email sales@cetascyber.com
cetascyber.com

Types of SOCs

There are four possible security operations centers :

The Basic SOC

This SOC focuses primarily on detection rather than investigation. They've invested sparingly in technology due perhaps to a limited budget. Analysts work primarily in a SIEM that was deployed several years ago and it just hasn't been kept up to date. Overall, these technologies offer decent detection capability but there's not much flexibility to tune how they work with additional intelligence or use them for more advanced investigative use cases. Spending time doing investigations or engaging in "hunting" isn't really in the cards at all.

The Intermediate SOC

At this level, the SOC has mastered detection and the technology investments provide reasonably good visibility into the organization. Beyond the basic detection capability of a SIEM fed by event logs, the SOC has deployed a combination of EDR and network forensics technologies that provide advanced threat detection. The team really wants to spend more time being proactive, but "operational reality" makes that difficult.

The Advanced SOC

SOCs that get to this level has made a tremendous investment in tooling to free up their analysts' time. Tier one and two analysts are working primarily in a SIEM. But that's only because they've taken the time to tune their correlation rules and plug some of their more specialized products into the SIEM. They can even pull data from their network and endpoint security products without leaving the SIEM. This improves the quality (and speed) of their investigations. When they escalate incidents, tier three analysts pick them up and pivot directly to more sophisticated analysis tools and consoles.

Email sales@cetascyber.com
cetascyber.com

While good things come in threes, advanced SOCs often add a fourth cadre of analysts called the “hunt” team. They’re not part of the 24x7 rotation. They focus exclusively on finding things their automated detections missed. While they do a little work in the SIEM, they spend most of their time building and running custom scripts to find threats their security products aren’t alerting on.

Lastly, Intelligence analysts make sure that the intel feeding the technology is up to date, ensure it’s not burying shift analysts in useless alerts, and – when serious threats arise – add context so that management understands the risks they’re facing.

Finally, you’ll see engineers whose job is to build software that makes their security products talk to each other. This helps streamline their processes and automate data gathering as best as they can.

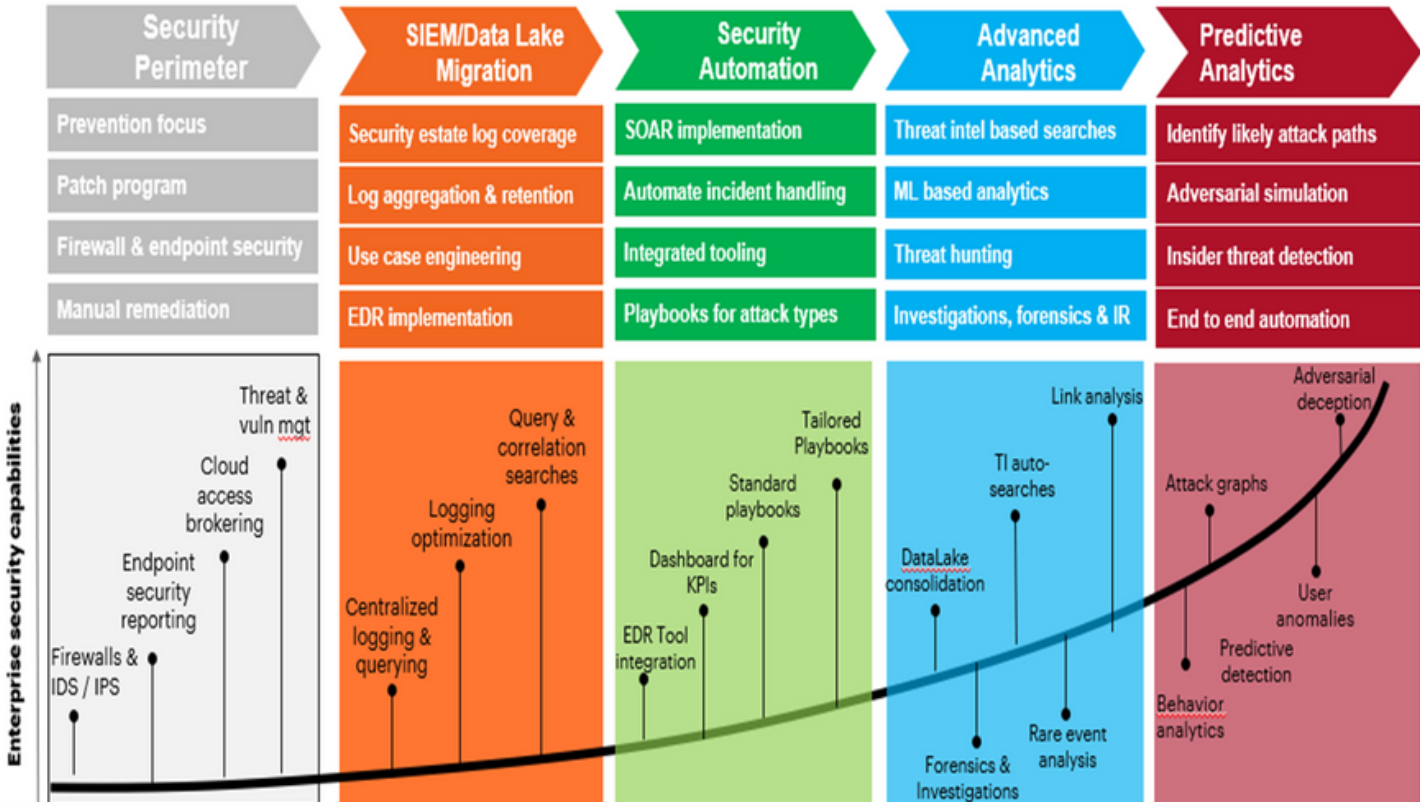
The Learning SOC

Like the advanced SOC, this organization has invested an enormous amount of time and money in automation and analytics. They’re focused on ensuring that humans are doing the security work that only humans can do. Everything else is handled by software.

To that end, they’ve tied their security technologies together with an orchestration framework and pulled in resources from IT to help automate investigation and remediation. As a metrics-driven organization, they watch closely what the ratios are between false positives and true positives, how long it takes to triage and investigate, and how much value they’re getting out of their security investments based on usage.

Security Operations Maturity Model

Different organizations find themselves at different stages of developing their security stages. We define five stages of security maturity. In stages 4 and 5, an investment in a security operations center becomes relevant and worthwhile.



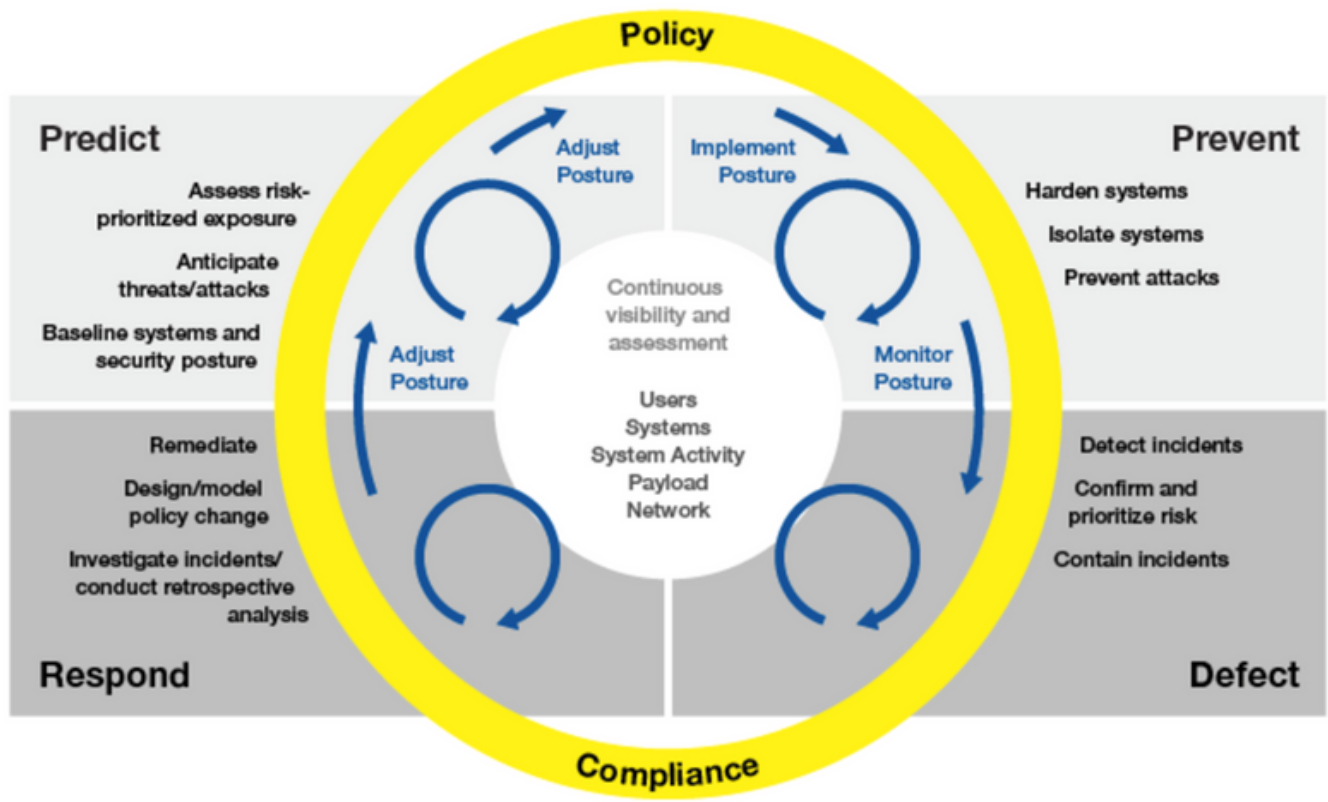
Steps to Build a SOC

1. Build an adaptive SIEM architecture
2. Develop your security operations center strategy
3. Design your SOC solution
4. Create processes, procedures, and training
5. Prepare your environment
6. Implement your solution
7. Deploy end-to-end use cases
8. Maintain and evolve your solution

1. Build an adaptive SIEM architecture

Many enterprise IT security teams spend much of their time focused on preventing a cyberattack. In doing so, they have implemented an "incident response" mindset rather than a "continuous response" where systems are assumed to be compromised and require continuous monitoring and remediation.

The adaptive security architecture is a useful framework to help organizations classify existing and potential security investments to ensure that there is a balanced approach to security investments



2. Develop your security operations center strategy

The key to developing your strategy is to understand the current state of your organization.
Assess your existing capabilities at first, limit your scope to core functions:

- Monitoring
- Detection
- Response
- Recovery

Delay non-core functions until your core functions are sufficiently matured.
Identify and define business objectives.

3. Design your SOC Solution

- Choose a few critical security use cases (e.g., phishing attack)
- Define your initial solution based on these use cases. consider that your solution must be able to meet future needs.
- A narrow scope will reduce the time to initial implementation which will help you achieve results faster.

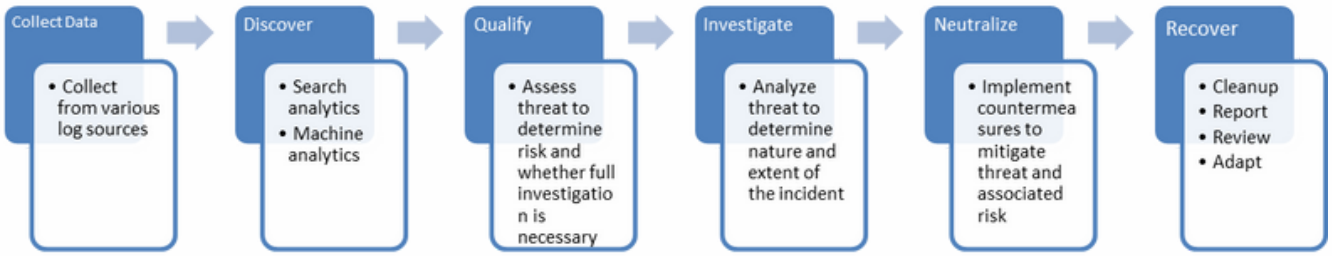
1. Define your functional requirements. (Be sure these are tied to business objectives.)
2. Choose a SOC model based on your functional requirements.
3. Design your technical architecture.

a) Choose your Threat Lifecycle Management platform
b) Identify business and information systems to be integrated
c) Define your workflows
d) Pinpoint areas for automation
e) Test the architecture

4. Create processes, procedures, and training

It's important to make sure that all six phases of the Threat Lifecycle Management Framework are covered.

TIME TO DETECT	TIME TO RESPOND



5. Prepare your Environment

Before deployment, make sure crucial security elements are in place:

- Ensure SOC staff desktops, laptops and mobile devices are secure
- Put secure remote access mechanisms in place for SOC staff
- Require strong authentication

6. Implement Your Solution

Take full advantage of your technology to minimize the workload on your staff:

1. Bring up your log management infrastructure.
2. Onboard your minimum collection of critical data sources.
3. Bring up your security analytics capabilities.
4. Onboard your security automation and orchestration capabilities.
5. Begin deploying use cases to focus on end-to-end threat detection and response realization.

7. Deploy end-to-end use cases

- Your tech is in place and your capabilities are deployed.
- Now implement your use cases across your analytics and security automation and orchestration tiers.
- Test your use cases rigorously over a variety of shifts and during shift changes.

8. Maintain and evolve your solution

A SOC isn't something to turn on and stop thinking about. It requires ongoing maintenance, such as:

- Tuning to improve detection accuracy
- Adding other systems as inputs or outputs
- Reviewing the SOC model, SOC roles, staff counts

Core Responsibilities of a SOC

A SOC team has two core responsibilities:

Maintaining security monitoring tools – In modern SOCs maintaining security monitoring tools also a responsibility of security engineers which was not there in conventional SOC. The team must maintain and update tools regularly. Without the correct and most up-to-date tools, they can't properly secure systems and networks.

Investigate suspicious activities – The SOC team should investigate suspicious and malicious activity within the networks and systems. Generally, your SIEM or analytics software will issue alerts which the team then analyzes and examines, triages, and discovers the extent of the threat.

Here are some of the core processes SOC teams carry out:

Alert triage – The SOC collects and correlates log data and provides tools that allow analysts to review it and detect relevant security events.

Alert prioritization – SOC analysts leverage their knowledge of the business environment and the threat landscape to prioritize alerts and decide which events represent real security incidents.

Remediation and recovery – Once an incident gets discovered, SOC personnel will reach out to the stakeholders and perform continuous follow ups for mitigating the threat, cleaning affected systems, and recovering them to their normal working condition.

Reporting – An important function of the SOC is to document the organization's response to an incident. And to report analytics, Incident Trends, Analyst Performance, Log source health metrics etc.

Email sales@cetascyber.com
cetascyber.com

Keys Performance Metrics

It is important to track how effective a SOC is both over a short current timeframe (day, week) as well as a longer period (month, year.)

Comparing to industry peers can also be very useful if such data can be sourced.

The following are a list of some useful metrics. Don't be afraid to add more.

Metric	Definition	What it Measures
Mean Time to Detection (MTTD)	Average time the SOC takes to detect an incident	How effective the SOC is at processing important alerts and identifying real incidents
Mean Time to Resolution (MTTR)	Average time that transpires action and neutralizes the threat	How effective the SOC is at gathering relevant data, coordinating a response, and taking action
Total cases per month	Number of security incidents detected and processed by the SOC	How busy the security environment is and the scale of action the SOC is managing
Types of cases	Number of incidents by type: web attack, attrition (brute force and destruction), email, loss or theft of equipment, etc.	The main types of activity managed by the SOC, and where preventative security measures should be focused

Email sales@cetascyber.com
cetascyber.com

Analyst productivity	Number of units processed per analyst-alerts for Tier 1, incidents for Tier 2, threats discovered for Tier 3	How effective analysts are at covering maximum. possible alerts and threats
Case escalation breakdown	Number of events that enter the SIEM, alerts reported, suspected incidents, confirmed incidents, escalate incidents	The effective capacity of the SOC at each level and the workload expected for different analyst groups.

Email sales@cetascyber.com
cetascyber.com

Introducing Cetas Autonomous Incident Responder:

With the companies moving to cloud at a rapid pace, investing in new technologies to run their business better, remote work becoming mainstream due to pandemic etc.- the challenge of IT and security teams to secure digital ecosystems has increased many folds. Given the amount of data (volume, velocity) and complexity, it's impossible to detect malicious behavior from human beings alone.

We have seen what are the challenges/blind spots of SIEM and Cetas AIR not only overcomes these challenges, but automates it.

Cetas cyber helps you to Detect, remediate and respond to incidents that matter across entire attack surface in Minutes. At Cetas Cyber, we automated the SOC lifecycle to detect and respond to real threats that matter using AI and simplify security operations.

Cetas Cyber with a team of seasoned **Cyber Security and AI and ML experts** has built a state of the art, next generation **Autonomous Cyber Security platform**. Our platform is tried and tested and is already being used by customers to,

- **Full Spectrum Security:** Secure all your applications and data sources, build a robust defense against cyber threats across the entire attack surface and improve your security posture.
- **Deploy Autonomous Cyber Security:** Gain 24*7 security cover, automatically detect, respond and hunt threats in real-time with speed and accuracy.
- **Enhance SOC performance:** Automate SOC lifecycle and mimic cognition of security analysts, augment your security teams with AI-driven cyber security to increase productivity and efficacy.

Email sales@cetascyber.com
cetascyber.com

Cetas Advantage

No-Code Platform: Simply Cyber Security with a No-code platform, build and deploy models quickly and easily to handle and hunt threats

Rapid ROI: Build and deploy strong security defense rapidly with AI models that can detect and neutralize threats in real-time, and maximize returns while investing minimum efforts.

AI that is Real: Provide 360° coverage with deep genetic algorithms to build autonomous models that continuously self-learn, rank order effectiveness, and activate when relevant threats are encountered.\

Metrics

95% - Drop in false rates - Reduce noise, focus, and Prioritize the critical threats

200% increase in productivity - Gain maximum throughput from your security operations along with increased precision

90% - Decrease in MTTR - Be quick and agile in identifying and neutralizing threats and mitigating security risks

Email sales@cetascyber.com
cetascyber.com