10 Habits

of Effective SOCs and How to Avoid a Lousy SOC

LMNTRIX

BE THE HUNTER | NOT THE PREY

Over the years the SOC has become a dirty word, as enterprises with multi-million-dollar SOCs continue to be breached, while their teams drown in noise, false positives and alert fatigue. SOCs have such a bad reputation that in recent years most enterprises have started renaming them to distance them from the negative connotation. You can find them being called Cyber Defense Centres, Threat Intelligence Centre, Cyber Threat Intelligence Centre, Security Defense Center, Security Analytics Center, Network Security Operations Center and variety of other combinations, however no matter what they're called now, they all share the same mission and same struggles.

Most enterprise SOCs struggle to maintain high-quality skills/talent as their turnover is very high, since team members leave shortly after being trained and those who gain experience soon leave for higher paying consulting gigs. When you combine this with security budget constraints and skills shortage, most enterprises end up with exhausted and burned-out junior analysts acting mostly as seat warmers, instead of analysts capable of fighting of advanced threats.

Central to every SOC is the SIEM that has proved expensive to own, complex to operate and being demoted in most enterprises to a glorified syslog server. The SIEM is also the root cause of alert fatigue that has delivered nothing more than a false sense of security to enterprises for more than 20 years. And they continue to get breached, while their SIEM sits in the corner quietly eating the enterprise IT budget, year after year.

Aside from basic log management and compliance use cases, SIEM's have been such a failure that vendors (over the past few years) have resorted to add many other features in hopes of making it do something useful. These includes adding UEBA, SOAR, Threat Intelligence, ML, or completely renaming it to XDR and trying to distance themselves from the legacy SIEM - the only thing they haven't thrown at the SIEM domain is the kitchen sink.

69% of SOCs
Say their analysts are drowning in Alert Fatigue
Ponemon 2019 SOC Survey

So how do you run an effective SOC? A well-oiled machine, a fun place to work that has near zero attrition and global reputation for providing the best experience and learning environment for staff. And most importantly - a SOC that has near zero false positives and alert fatigue?

If the above issues resonate with you – read on to hear what we do at LMNTRIX in operating our SOC, so you can “SOC” the right way too.

Habits of Effective SOCs

Adversary Simulation Drills

Engage your team in regular Adversary Simulation drills. This will not only test your existing detection and response capabilities, but it will also help in the enhancement of the skillset of security analysts and incidence responders. Start by using alreadyavailable tools – open-source or commercial, these will help kickstart this habit as a routine process. Over time this can evolve into more detailed and deliberate probes from Red Team members who would simulate attacks like current threat actors. Integrating these in the form of war games can also help as team-building skills.

Innovative Teams

Encourage the team members to innovate and facilitate them with all their requirements that will let them turn ideas into innovations, like useful tools or processes that can be adopted by the team. Team members may come up with new ideas to optimize workflow, things that can be automated, building in-house detection techniques, or, integrate detection rules shared by the community into your detection workflow.

73% of SOCs
Say increasing workload was the cause of analyst burnout
Ponemon 2019 SOC Survey

Malware Analysis

Having team members that are skilled in Malware Analysis is important. Even if your SOC uses an automated sandboxed malware analysis tool, it is necessary to have someone skilled enough to interpret the results and put the pieces together to facilitate the deep-dive investigation of attacks, forensics, and hunts. Even if you do not have a specific product that does this task, a malware analyst on the team should be skilled enough to analyze samples manually, create detection signatures and make reports for incidents or hunts.

Lab Playground

SOCs should have a lab environment for testing new detection techniques. You do not want to test something new on a production system. Build and validate in a controlled lab environment and assess the outcome. A lab environment is also important for internal testing of new attacks. Perform the forensics and incident response in the lab and make notes that are useful to update existing process workflows of DFIR. Lab environment also lets you train team members or let them play around and learn on their own, whichever fits best for your team.

Playbooks

Playbooks are a useful tool for a SOC that is prepared for almost every scenario. Playbooks are scenario-based flow charts of processes that define what actions are needed to be performed and what decisions are needed to be taken as the process flows. This includes decision branches as well. These can be given out as handouts to team members for orchestration of workflow, or can use it in the SOAR platform for automation of processes. Playbooks should be updated regularly, as the underlying process followed by the team evolves. This is very useful in guiding low-level analysts and defining automation tasks.

Automation

Process optimization is at the core of any successful team. Process optimization intends to reduce or eliminate time waste, resource waste, unnecessary costs, bottlenecks and errors, while achieving the goal of the process. Automation of the SOC processes is one of the widely talked topics in the security industry, but not every SOC is doing it. Integrate all your solutions and program your workflow into the process automation tool. Let the software take care of the processes with fewer errors. This will let the team focus on digging deep into investigations, hunt data analysis, and other important decisions.

Threat Hunting

A mature Threat Hunting process followed by the team defines how advanced and experienced the Threat Hunting team is. Hunting Maturity Model provides a basic framework of defining how capabilities of a Threat Hunting team are categorized in the maturity model. In general, if your team is routinely collecting data for hunts and applies data analysis techniques created by the community, or applies its own data analysis techniques - your team should be ranked on the higher end of the Hunting Maturity Model. Threat Hunting team should continuously stay updated with the latest threats and hunt accordingly.

53% of SOCs
Do not have ability to gather evidence and investigate source of threats
Ponemon 2019 SOC Survey

Threat Modelling

Use Threat Modeling as a prequel to Threat Hunting process. Your team should also be aware of the attack surface it is dealing with. Threat Modelling will help your team identify areas that attackers could use to infiltrate, move laterally, escalate privileges, and exfiltrate data. Let your team think like a hacker. They will come up with ways the attacker might execute an attack, as they already know the infrastructure internally. The data gathered at the end of Threat Modelling should help your Threat Hunting team customize their hunt and start looking for threats accordingly.

Threat Intelligence

Threat Intelligence is important for preparing for an attack that might take place. Evaluate the quality of your Threat Intelligence feeds regularly. You do not want to be given noisy intelligence data. Moreover, isolated Indicators of Compromise do not provide much value. Look for Threat Intelligence that provides feeds that are enriched with attacker TTPs and attribution as well. The devil you know is better than the devil you do not.

Fancy Products

Big Data Analytics, Machine Learning, Artificial Intelligence – many still consider these are buzz words thrown around to generate hype. But if you and your team know what you are doing, you will understand how beneficial these technologies are. Having talented staff who can translate a security challenge into a data analysis challenge might help you buffer into using these products efficiently. Make sure that they contribute to the operations and performance of the team.

Avoid being a Lousy SOC

The market is littered with lousy SOCs. You can identify them from outside. In most enterprises their SOC is a SIEM with a bunch of security guys - trying to make sense of all the alerts once they spend many months making it work. Larger enterprises with larger SOC investments, together with security savvy teams, have different struggles which range from skills and budget shortages to scalability issues. The following are common mistakes we see with many SOCs, that you can avoid if you know what to look for.

Lack of visibility

If you do not see the data, you will not see any threats. Having limited visibility into the organization means you are missing out on key areas of detection. The last thing you want is a blind spot in your security monitoring capability. However, growing data volumes are requiring organizations to take a more strategic approach to data security management. Going forward, enterprise organizations need to be more strategic in how and why they are collecting data. To avoid redundancy they need to be clear about what's needed for threat detection and which data is required for forensic analysis and investigations.

Decisions need to be made about how much data needs to be online or available via fast storage, how much real-time processing is required, and how, where, and for how long to store the historical data required for threat investigations.

97%

of the behaviors executed did not have a corresponding alert generated in the SIEM

LMNTRIX 2018 Survey of 350 Global Enterprises

SIEM-centric SOCs

In reality, there are still a lot of classic SIEM-based (actually, SIEM-only) SOCs where the analysts appear to be visible, but via SIEM. On a daily basis they only check logs. And they only get logs their SIEM vendor wants them to see. Usually, this is due to the fact that the line analysts have no access and even no impact on the detected content. This means that they are confound by alerts, and don't have a chance to setup them. Bad for a reliable SOC.

A LOGS-ONLY APPROACH TO DETECTION ISN'T WORKING

83%

Percent of incidents that not took weeks or more to discover

99%

Percent of successful attacks went undiscovered by logs

LMNTRIX
Survey of 350
Global Enterprises

SLA and Compliance-led SOCs

To ensure compliance with the legal, and regulatory requirements, you will have to establish certain security policies. These security policies will define principles, rules, and guidelines which the management wants the employees to follow. There is nothing worse than a compliance-led SOC, that was procured solely for the purpose of pleasing the annual compliance audit. In many cases these policies are too basic and inappropriate. Paying attention to these compliance requirements may distract your team from tracking real threats and uncovering vulnerabilities.

False Positives

Another word for alert fatigue. Your SOC team should be fine-tuning the detection techniques early on (especially MSSPs), so that they are not flooded with false-positive data. Having a lot of false positives means having to spend more time triaging them.

Lack of skilled team members

Your team is not just the products you have acquired to run the SOC, it is also the human analysts that operate these products and perform analysis. You might already be aware of L1, L2, L3 level categorization for analysts, but what good is having an experienced L3 candidate (spent few years triaging alerts) that does not possess critical skills, such as Incident Response or Digital Forensics.

Lack of Defined Process

Even if you did not hire amateurs to run your SOC, not having a defined process for the SOC to operate will turn your SOC into a lousy SOC. How to not let that happen? Start with the basics – define roles and escalation matrix. Define workflows for each role. Formalize processes for – Incident Handling, Investigation, Forensics, Incident Response, Threat Hunting, etc.

Lack of data sharing

Your team should be able to collaborate freely within the team. This also includes sharing of relevant data across platforms, or tools to enrich or add context to an incident. There might be different tools in place, such as – Network Intrusion Detection System, Endpoint Intrusion Detection System, Threat Intelligence Aggregator. etc. Teams should be able to share or lookup data across all the platforms. Otherwise this model is simply not scalable, as the process becomes inefficient and hiccups are introduced in the form of human delays.

Fancy products

As explained earlier, these are your Big Data Analytics, Machine Learning, and Artificial Intelligence based products. If your team is not using these products wisely – they will not have any ROI. A common situation is not having a clear hypothesis of what needs to be analyzed. Your team needs to translate a security question into a data analysis question. Feeding data into these products and hoping that magically some sensible output is derived - will not help your team.

$1.27
million dollars
wasted
responding
to erroneous
or inaccurate
malware alerts
2017 Ponemon
Global Average
Cost of Data Breach

Jumping into the Threat Hunting Trend

If you are blindly following the trend of adopting Threat Hunting, your team will drown in the myriad of data and end up wasting their time. Your team needs to know what this is all about and they need to know what they are looking for. These are the two basic things your team needs to know to get started, even if you lack a skilled threat hunter in the team.

Missing threats

Your team is missing actual threats. It could be the detection technique is not good enough, or the attackers have found a way to bypass the detection and your team has not caught up with this bypass. Or it could drown your team in false positives. A good way to tackle this problem is to categorize events by linking them to TTPs in the MITRE ATT&CK, so that your team can prioritize findings selectively.

High MTTR (Mean Time to Respond)

MTTR is an important Key Performance Indicator (KPI) for the SOC to track its performance. This defines how quickly your team responds to a threat. For MSSPs and in-house SOCs, it is important to have a quick MTTR. This not only shows how efficient the team is, but is also seen as a positive ROI by the management. Your team could end up having very high MTTR due to multiple reasons – lack of detection capability, lack of proactive threat hunting, spending too much time triaging alerts etc.

No Training Drills or Lab Playground

In the end, you also need to let your team grow its skillset. Training Drills test competencies of the team members. It also pushes the team members to learn and improve the necessary skills. Not having a lab playground means that you are probably testing your detection techniques on the production system. If you have not broken the system yet, you will end up breaking the production system in the future. Keep a separate environment for all sorts of testing. Not having a lab playground also means your team is not testing or training on new attacks. A team that is not staying up-to-date is the least prepared for when an attack happens.

Lack of automation

As we mentioned above – any automation is good for your environment. The software can take care of your processes, thus eliminating time waste, resource waste and unnecessary costs. On the market there are SOAR tools (Security Orchestration, Automation and Response), i.e. set of software programs that can enable you to collect data about security threats from multiple sources and respond to low-level security threats without human assistance. The goal of using SOAR tools will be to improve the efficiency of your digital security operations.

Summary

There is no magic security solution; the tough truth is that you can't prevent 100% of the possible attacks. Establishing a dedicated SOC will provide you constant monitoring of your digital assets and faster response to the potential threats. However, the steps towards a successful SOC are not easy. In order to improve and keep the efficiency of your SOC - you have to follow certain best practices:

- Understand the Role of the SOC – your personnel should concentrate on real monitoring and analysis of incidents, not on ad-hoc daily tasks that will obstruct them.
- Supply the SOC with state-of-the-art infrastructure – involve firewalls, endpoint protection solutions, SIEM solutions, data collection tools, security probes etc.
- Employ Skillful Security Analysts and try to keep them. Also, choosing a proper SOC manager is strongly advisable.
- Apply Automation - integrate your solutions and program your workflow into the process automation tool. Let the software take care of the processes with fewer errors.
- Lab playground and Playbooks – these will enable you to perform experimental forensics and incident response, and scenario-based flow charts of processes that define what actions should be performed and decisions to be taken.
- Threat Modeling and Hunting – Modeling will help your team identify areas that attackers could use to infiltrate, move laterally, escalate privileges, and exfiltrate data (think as a hacker); Hunting means your team is routinely collecting data for hunts and applies data analysis techniques created by the community, or applies its own data analysis techniques.

BLIND SPOTS IN THREAT DETECTION & RESPONSE

24%
Have Visibility into Attacks

8%
Can Quickly Detect Attacks

11%
Can Quickly Investigate Attacks

LMNTRIX
Survey of 350 Global Enterprises