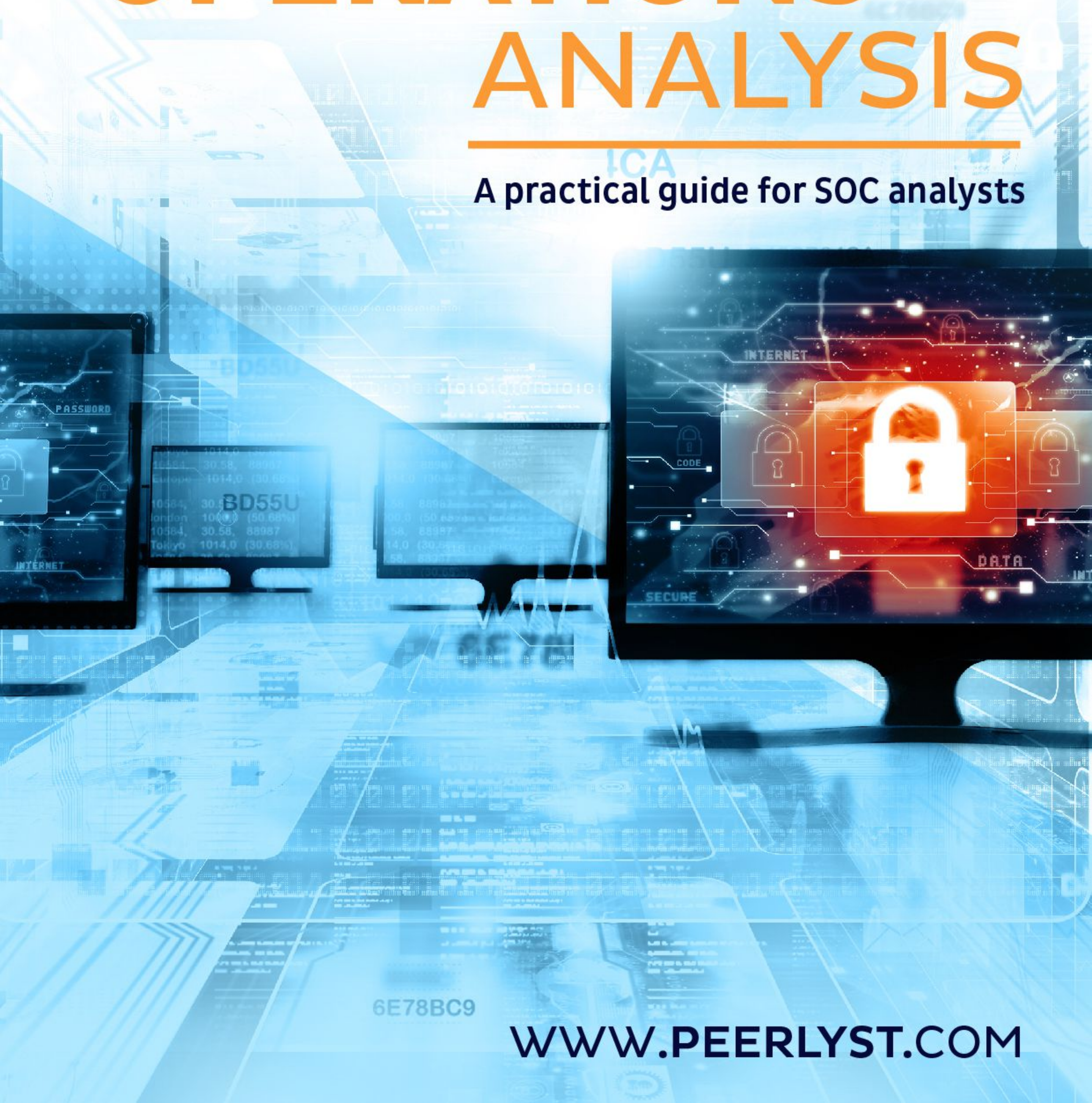
PEERLYST

SECURITY OPERATIONS ANALYSIS

A practical guide for SOC analysts



WWW.PEERLYST.COM

Security Operations Analysis

Security Operations Center (SOC) Analyst Guide

Edited by: Chiheb Chebbi

Table of Contents

Chapter 1: Information Security Incident Response

By Mohamed Marrouchi

Introduction

Identifying and responding to data security incidents is at the center of security activities. The group appointed to security operations is relied upon to monitor the organization's advantages inside extension and respond to security events and incidents, including the identification and examination of what might be considered indicators of compromise (IOC).

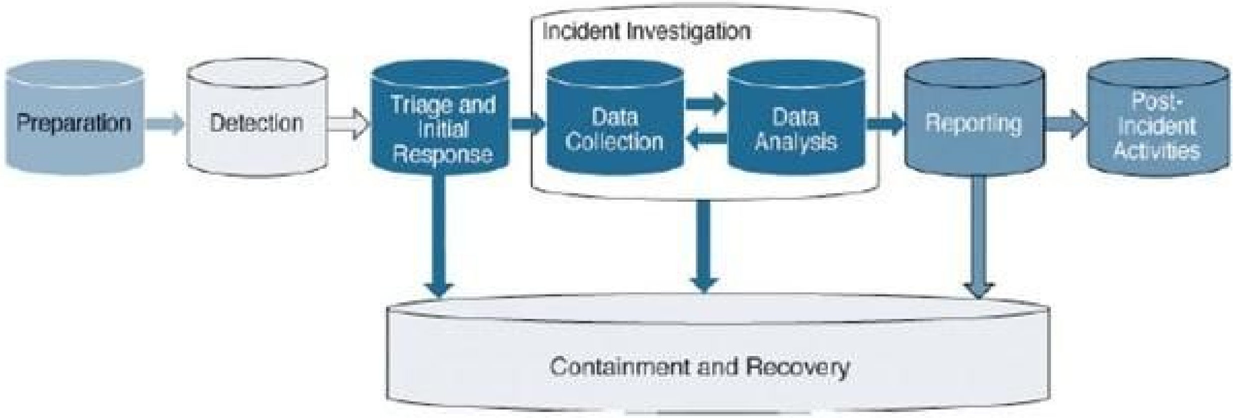
In this chapter we are going to discover the following topics:

1. Incident response Timeline
2. Incident Detection
3. Incident Triage
4. Incident Categories
5. Incident Severity
6. Incident Resolution
7. Incident Closure
8. Post-Incident
9. SOC Generations
10. Conclusion

1.Incident response Timeline

Setting up a SOC to oversee incidents stretches out to cover people, processes, and obviously, technology.

The correct arrangements of steps to pursue and the gatherings to include rely upon the idea of the incident. A run of incident-handling taking care of process pursues the list of steps exhibited in the incident response (IR) timeline in the Figure. We should take a gander at detection, which is the second stop.



2.Incident Detection

Detection alludes to the stage in which an occurrence is watched and revealed by people or technology, and the process that handles the reporting angles.

For the process to be powerful, the accompanying must be documented and formalized:

-Identify the sources, for example, technology and people, that are in charge of detection and reporting incidents response team.

-Identify the channels through which incidents response team ought to be accounted for.

-Identify the means that ought to be taken to acknowledge and process incidents response team reports.

-Identify the prerequisites on people and technology for the process to work.

3.Incident Triage

Incident triage appears to the underlying moves made on a detected event that is utilized to decide the rest of the remaining as per the incident reaction plan. The triage phase comprises of three sub-phases: verification, initial classification, and assignment.

The triage phase is worried about answering different question, for example, the accompanying:

-Is the incident inside the extent of the program?

-Is it another incident, or is it identified with a past reported one?

-What classification should the incident be doled out to?

-What severity level ought to be allotted to the incident?

-Who ought to be appointed to investigate and analyze the incident?

-Is there a time period related with the incident?

4.Incident Categories

Category Number	Name	Description
0	Exercise	This is used when conducting an approved exercise such as an authorized penetration test.
1	Unauthorized access	This represents when and individual gains logical or physical access without permission to a client network, system, application, data, or other resource.

2	Denial of Service(DoS)	This is used when an attack successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources.
3	Malicious code	This identifies when there is a successful installation of malicious software, such as a virus, worm, Trojan horse, or other code-based malicious entity, that infects an OS or application.
4	Scans/Probes/Attempted access	This includes any activity that seeks to access or identify a client computer, open ports, protocols, service, or any combination for a future attack.
5	Investigation	This includes unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review

All security incidents ought to be belonged to a category. The category number distinguishes the sort of the incident and its potential kind of impact. The table demonstrates an example rundown of categories that we use for categorizing incidents.

The incidents may have beyond what one category and that the classification can change as the incident advances or as the examination of the incident unfurls new discoveries.

5.Incident Severity

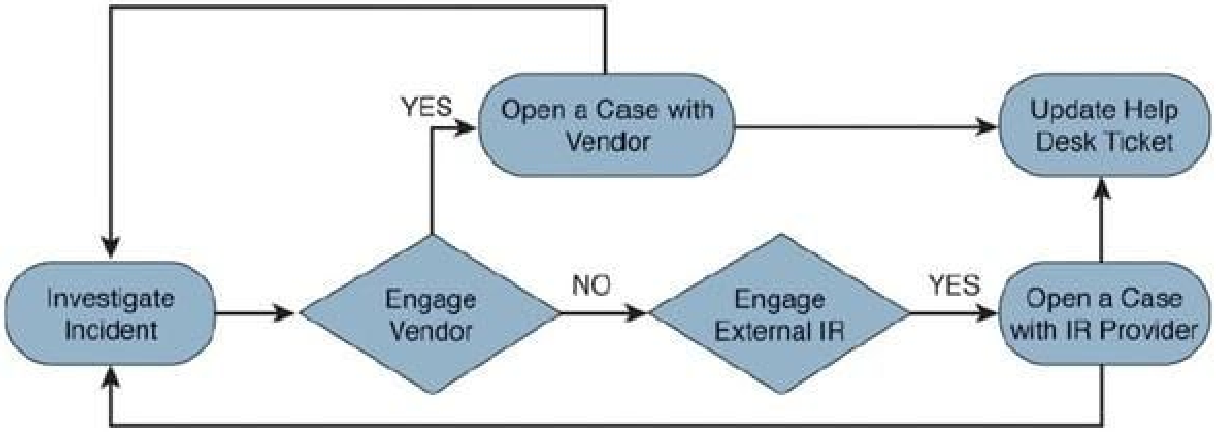
Severity levels depend on the normal or watched impact of an incident. This is utilized for the prioritization of the incident, considering the measure of assets that ought to be appointed, and decides the escalation procedure to pursue.

Level	**Description**

High	Incidents that have severe impact on operations
Medium	Incidents that have a significant impact or the potential to have a severe impact on operations
Low	Incidents that have a minimal impact with the potential for significant or severe impact on operations

6.Incident Resolution

The lifecycle of an occurrence ought to in the long run lead to some type of resolution. This may incorporate information examination, resolution look into, a proposed or performed activity, and recuperation. The goal of this phase is to find the underlying driver of the incident, while chipping away at containing the incident at the earliest stage conceivable.



The investigation and analysis phase include the exercises attempted by SOC and by different groups with the end goal of:

Identifying exploited systems and accounts

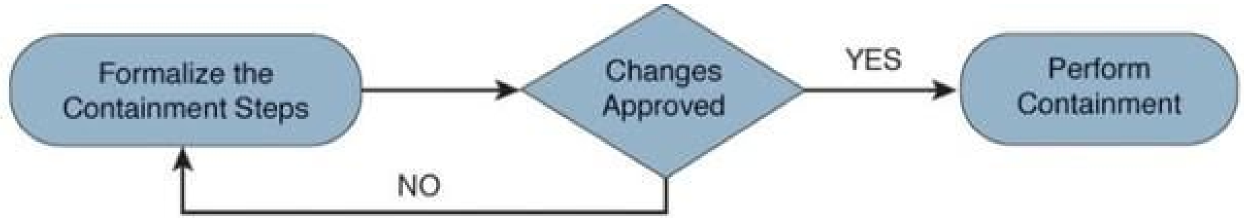
Understanding the effect of the security incident

Identifying unapproved get to endeavors to private information

Understanding the chain of incident that have prompted the security incident

The containment stage includes the activities performed to rapidly stop a security incident from raising or spreading to different networks or systems

The procedure appeared in the figure is an example containment process. We may, be that as it may, continue with containment previously or amid the incident examination.



The correct strides to pursue to contain a security incident shift contingent upon the idea of the incident and business criticality of the asset. Instances of containment activities incorporate the accompanying:

- Disengaging a system from the network
- Moving a tainted system to isolate network
- Halting a process or a service
- Disabling an account
- Including a firewall rule
- Including an intrusion prevention system (IPS) signature/rule that would distinguish and hinder the assault's particular vector.

7.Incident Closure

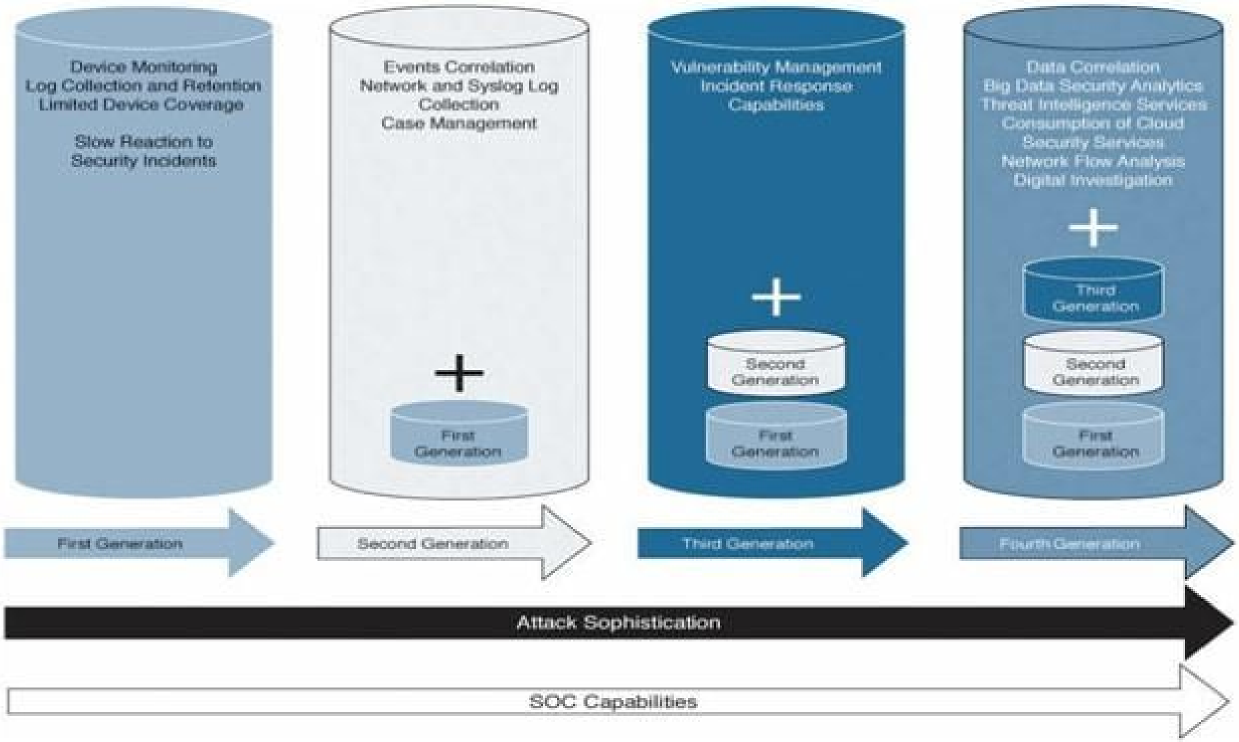
Closing a security incident alludes to the destruction phase in which vulnerabilities that lead to the event or incident have been shut and all the occurrence follows have been washed down. The closure procedure likewise incorporates testing systems to guarantee that the annihilation steps and controls were compelling and that the vectors utilized by the attack don't exist any longer or is insufficient. Predefined activities to consider incorporate applying any last data about the event, its last classification, any outside warnings, and documenting information about the incident.

8.Post-Incident

This is the "lessons-learned" stage in which us look to enhance the IR processes and ponder other people, processes, and technology controls. Post-incident exercises will fluctuate contingent upon the seriousness of the security incident. Important learning picked up from security incident can be valuable to avert/moderate future incident as proactive administrations, for example, improving security highlights of capacities inside protections.

9.SOC Generations

Our comprehension of SOC segments and expected services has changed after some time. This is a reflection of the change in our view of the criticality of information assurance and security activities. This change comes in light of the regularly changing security threat landscape, notwithstanding our undeniably receiving formal information security standards, requiring the foundation and management of a formal security activities model and audit forms.



10.Conclusion

In outline, following an incident response course of events, the SOC group would deal with various basic assignments, from occurrence identification to closure. Each phase of an incident can have its very own process and include different gatherings inside the association. It is significant that the arrangement, plan, and fabricate stages for occurrence response be characterized, reported, and supported by the correct specialists inside the association. incident response is tied in with timing, and the most noticeably terrible time to make sense of duties and incident-handling care of process is during a functioning attack.

References:

- Gregory Jarpey and R. Scott McCoy (Auth.) - Security Operations Center Guidebook. A Practical Guide for a Successful SOC (2017, Butterworth-Heinemann)
- Jeff Bollinger, Brandon Enright, Matthew Valites - Crafting the InfoSec Playbook_ Security Monitoring and Incident Response Master Plan-O_Reilly Media (2015)

- Joseph Muniz, Gary McIntyre, Nadhem AlFardan - Security Operations Center_ Building, Operating, and Maintaining your SOC-Cisco Press (2015)

Chapter 2: An Overview of Knowledge Asset Management for Cybersecurity

By Dana Winner

A recent cyberspace controversy regarding X10 Engineers, triggered by a Tweet from technology start-up investor, Shekhar Karani, generated a "Twitter storm" of hate, as well as some useful discussion. Shekhar represented a widely held view in the Information Technology (IT) industry culture, that a "10X Engineer" is a "great individual contributor". He acknowledged that they may not be good with teamwork. So, what?`` Other IT industry influencers, such as Rob Graham, countered that "10X engineers" are a "diverse" group of people, some of which are "hermits", while some are "outgoing team leaders", some are charlatans and some are "negative-x", i.e. having negative impact on team productivity. He highlighted the negative atmosphere in which engineers are focused on trying to "one-up" each other, competing rather than collaborating. In the Security Operations Center (SOC), collaboration and knowledge-sharing are mandatory for success; 10x collaboration for 10x success.

Collaboration is a major principle and a suite of behaviors that form the core of Knowledge Assets Management (KAM) culture. That collaboration suite of behaviors include dialog/conversation, teamwork, knowledge sharing, human capital development, respect for intellectual property and other concepts that support knowledge development. These KM principles and behaviors are critically important for any Learning Organization, such as a SOC.

Sadly, since the commercialization and commoditization of Information Technology (IT) began in the 1980's, and greatly accelerated in the '90's, thanks to the Internet and World Wide Web (WWW), KM principles and behaviors have been a lower priority for the IT industry. More specifically, the lack of KM culture has been even greater in the cybersecurity industry, in which “hacking” and being a “hacker” are cultural themes which elevate cyber criminals (“hackers”) as a hero and discount the criminal character of that (“hacking”) behavior.

The growth of the Internet in the 70’s and 80’s, and even more so, the WWW in the 90’s and 2000’s, promised exponential growth of knowledge through greater access to explicit knowledge through digitally documented information formatted as text, graphics, images and voice. Hyperbole and hubris are rampant regarding the benefits that the Internet has and is expected to provide. Mark Zuckerberg, CEO of Facebook, exemplifies that hyperbole and hubris, claiming that “Connecting everyone to the Internet is…necessary for building an informed community”. There is general acceptance of the idea that for the industrialized world, and especially the liberal democracies, the economic growth accruing from Internet use has been phenomenal. However, not everyone agrees that connecting to the Internet is a guarantee of learning and development of knowledge. The matrix of the Internet, liberal democracy, is threatened by abuse of its freedoms thanks to abuse of the Internet. The benefits of the Internet are increasingly in question as the cost of cybercrime grows.

Nevertheless, for the largest economies, the Digital Economy contribution to economic growth far outweighs the cost of cybercrime and smaller economies continue to compete for their place in the Digital Economy. Consequently, there is currently little motivation to fundamentally solve the cybercrime problem. We can expect the current trends and behavior to continue until disrupted by extreme conditions, such as cyberwar or economic collapse. Every analysis predicts increasing cybercrime; “the Rules of Engagement have broken”. As we already know, cybercrime will continue to be unfairly externalized to individuals, small-to-medium enterprises and smaller economies, especially as the "Internet of Things" spreads its network of headless, unsecured devices. Every SOC is at the vanguard of this struggle to make the Internet sufficiently safe and secure to fulfill the potential knowledge growth of the Internet. This is a cultural revolution – for better or worse – globally and in each and every SOC.

Looking back over the 70 years of Information Age evolution, contrary to popular opinion, it is apparent that there are aspects of the IT culture that have severely deteriorated. The earliest days of the Information Age were days of making computers do things that seemed almost impossible – like landing humans on the moon 50 years ago when the Information Age was merely 25 years old (Harvard Mark I, 1944). Those amazing deeds were accomplished through humility, knowledge sharing, collaboration, teamwork and diversity.

The KM cultural values are often thought of as "feminine", while the cybersecurity culture is largely "masculine" (more about this later). In the formative era of the Information Age, women invented software. Women were included in the IT workforce for their knowledge, skills and abilities (KSA). Female engagement peaked in the '80's at 30-35% before commercialization shifted the nexus of IT culture to Silicon Valley. These and other related cultural values are in shorter supply in an era of information and cyber **insecurity**, or as Vint Cerf has called it, a Digital Dark Age. If we want to win this struggle to fulfill the knowledge development promise of the Internet, we need to regain the seminal cultural values of the Information Age. Every SOC is well positioned to lead this cultural struggle, to rebuild the cyberspace cultural (values, behaviors) superstructure to take full advantage of the Information Age foundations built in the 40's-80's.

The cyberspace superstructure that we have built on that foundation is not sustainable. Those people who are information and cyber security professionals know that we are in a "no win" situation. We can only estimate risks and spend precious resources to mitigate those risks, just as seismologists can warn and recommend regarding potential for earthquakes and volcanic eruptions. By contrast to those forces of nature, the cyber risk that we are struggling with is of our own making. Doing the same thing again and again and expecting a different result is insane. We have created and continue to perpetrate the culture that simultaneously builds and destroys our global information infrastructure.

The cyberspace culture is building with the dominant hand and destroying with the other hand. When will the destruction become financially intolerable? We have to solve the problem at the root; building on the culture and purpose that formed the Information Age foundation. That KM culture is essential to an effective SOC. Developing cybersecurity strategies, tactics and technologies does not solve the cyber risk problem. "Culture eats strategy for breakfast". We must change ourselves, individually; change our culture, our values, our behavior in cyberspace. By changing ourselves we change the SOC. By changing the SOC, we can drive the change in IT, the enterprise, the nation, the world.

Our first step in this cultural change is to remember the original purpose of our cyberspace adventure. Purpose is an important driver of all principles, values and behavior. Let's step back from our focus on technology, the data, the information. We need to remember why we are managing technology, data and information. **Our purpose is to support knowledge creation and sustainability; know-how, competency, ability, skill and understanding that leads to excellence in performance and productivity**. This is why we manage information and data using electronic digital technology. Clearly, we must drive information management, in all of its aspects and components, to support our Knowledge Assets. The question is, "do we have a framework within which to conduct a Knowledge Assets Management approach to information systems and especially, information and cyber security?" The answer seems to be "No."

Beyond the anecdotal evidence in the twitter-sphere, as reflected in the opening paragraph, we find further evidence in the formal information security frameworks, that the principles of knowledge management and knowledge itself is, at best, assumed, and in reality, is mostly an after-thought. For example, in the "ISO 27000:2018 ISO Information technology — Security techniques — Information security management systems (ISMS) – Overview and vocabulary", the emphasis is not on knowledge or knowledge management. As might be expected, the word count for "information" is high at 318. Another high word count in this introductory document for the ISO27000 series, is "risk" at 174 repetitions. These high word counts reflect the importance placed on explaining these concepts. The word count for knowledge is 6.

Of course, there are many documents in the ISO27000 series and a thorough review might produce a more positive reflection of the importance of knowledge and KM within the context of ISMS, it is not unreasonable to suggest that the ISO27000 overview document does not provide a satisfactory and useful explanation of a knowledge-driven approach to building and sustaining the ISMS, which is a fundamental component of the SOC. So, what framework is available to support knowledge-driven cyber security in the SOC?

The good news is that there is a relevant standard from the International Standards Organization – ISO30401:2018 - Knowledge Management Systems Requirements – that can support the application of a Knowledge Management System (KMS) to the SOC ISMS. What are the primary KMS requirements that can be applied to the SOC ISMS?

ISO30401 describes in the introduction the problem posed by the common confusion between knowledge and information and "for example the view that simply buying a technology system will be enough for knowledge management to add value". The ISO KMS Requirements standard provides guidance regarding the following major components that are unique to this document:

4.2-4.3 Knowledge Stakeholders and Inventory: The organization should identify knowledge stakeholders who are best suited to defining the Knowledge Areas. Create a "list" of the corporate Knowledge Areas, their values and priorities in relation to stakeholders.

4.4 KM System: The organization should formalize their approach to KM into a system of people, policies, processes and tools. Sections 4.5-4.8 define the parts of the KMS

4.5 Knowledge Life Cycle: Knowledge change management supports the (SECI) transformations of knowledge assets within the knowledge areas as it evolves through the stages of the knowledge life cycle: acquiring, applying, retaining and managing knowledge.

4.6 Knowledge transformations: Knowledge is shared (Socialized). It is codified in many ways, including text, digitizing, coding, prototypes, products, processes and more (Externalization). Knowledge is integrated and analyzed from many sources to create new knowledge (Combination). New knowledge is understood and becomes know-how (Internalization). This is known as the SECI model: Socialization, Externalization, Combination and Internalization.

4.7 KM Facilitators: The knowledge life cycle does not happen by nature. Some people are natural in connecting, communicating and knowledge-sharing which are fundamental aspects of collaboration, while other people are averse to all aspects of collaboration. Even those who are adept at collaboration require guidance to ensure that their collaboration supports the corporate strategic goals. For those people who are not natural collaborators, talented coaches can teach attitudes and skills that facilitate most of the less talented collaborators. Dialog and conversation are underestimated skills that require work to develop, especially amongst people who are typically attracted to IT and cybersecurity.

4.8 Learning Organization Culture: create the values that promote knowledge creation and sustainability. This is primarily the responsibility of KMS Leadership (Section 5). The leaders establish Policies, Roles and Responsibilities (Sections 5.2-5.3).

Section 6.1 of the ISO30401 KMS Requirements defines the importance of planning and risk management of the KMS in order to achieve the knowledge objectives. This includes the development of needed resources, especially competency (Section 7) of responsible staff. Sections 8 and 9 define operations and performance measurements. Throughout the document is it clear that “documented information” is subsidiary to and supports knowledge..

SOC Analysis – the subject of this book – is a Knowledge Asset Management Process that creates and sustains the ISMS, i.e. the cybersecurity risk management body of knowledge of an organization. The framework for a Knowledge Assets Management driven SOC, is to apply the ISO30401 KMIS Requirements guidance to the SOC operations, and specifically to the SOC analysis process. It is hoped that the justification for applying ISO 30401:2018 has been so convincing that the reader is how eager for some practical implementation. That response calls for a complete book, not just a chapter. However, there are three KAM strategies that can be briefly described, which might be immediately helpful and effective.

The first of those three KAM strategies is to ensure that Knowledge Risk Management is the foundation for Information and Cyber Risk Management. By placing the emphasis on knowledge rather than information, data and technical infrastructure, it becomes possible to understand which Knowledge Assets (of which the great majority are human capital: tacit knowledge) can be valued and thereby prioritized for protection. Only then can the supporting assets, including the information, data and technical assets, be valued and prioritized. In other words, the value of information and data cannot be estimated except in the context of the knowledge that they support.

By insisting that the leadership estimate the value of Knowledge Assets and conduct Knowledge Risk Assessment, the CISCO will not engage in meaningless estimations of the value of information and data assets, basing Information and Cyber Risk Evaluations on false assumptions. Another benefit of this approach is to place the Human Factor and Human Capital squarely at the center of all Information and Cyber Security strategies, as we all know it should be. By emphasizing the Human Factor, funding of the most effective security strategies and tactics will be more convincingly justified.

The second of those three KAM strategies that could be immediately helpful and effective is to improve the conversation by changing the rhetoric. Words are powerful. Let's begin with the words "hacker" and "hacked". The original of the word "hacker" in modern slang means someone who is "amateur", a "hobbyist", i.e. someone who is not professional and not criminal. This word was first used regarding PC and Internet hobbyists and then stuck with them as some of them evolved into criminal behavior. Now, we need to change our culture to recognize that cybercrime is perpetrated by cyber criminals, not "hackers". We need to change our rhetoric to reflect the reality that what cyber criminals engage is in "crime" not "hacking". We need to stop referring to the people who fight the criminals as "hackers" or "ethical hackers" or "White Hat Hackers" and give them the serious respect of calling then cybersecurity professionals. The SOC is not a place for individualistic "hackers". The SOC is a team of cyber security professionals.

The third suggested KAM strategy is to increase diversity - which is proven to create new knowledge - by attracting more women to the SOC. The great majority of cyber crime is perpetrated by males. Insiders are the greatest cybersecurity vulnerability and IT insiders are the biggest vulnerability. Women are by nature less likely to engage in risky behavior, and therefore engage in cybercrime at a very low rate. As well as being more risk averse than males, as a group, women are more socially-oriented, more prone to communication, networking and information sharing. This is a useful generalization, but should not be the basis for ruling out exceptions. Certainly, many men share these natural talents with women.

Nevertheless, the talents of women are a great addition to IT, and especially to the SOC team. Make a qualified woman responsible for SOC KAM and increase the potential for the SOC to become a Learning Organization.

These three strategic changes are merely a suggested start for how the SOC can become a Learning Organization that is driven by and supportive of Knowledge Assets Management. The SOC should start the cultural change internally, so that each member is recognized as a Knowledge Worker (not a “hacker”) and the SOC becomes a Learning Organization providing professional cybersecurity protection to the enterprise. The SOC should insist on making know-how the supreme purpose of the SOC and then spread this change from the SOC to the Enterprise, and then to the Community, the Nation and the World.

Chapter 3 Introduction to Security Operation Centers

By Prasannakumar B Mundas and Elyes Chemengui

Before building SOC for the company, it is important to understand the needs to have the requirements and plans. Successful SOC is not so easy to implement without the support of all people from all levels. SOC can be implemented with the basic rules and processes but it should include a framework to have a continuous progress.

There are many obvious things which has to be followed by questioning ourselves. By answering these questions we will give the overall idea which helps to cover the gaps using SOC.

What are all current security problems your organization is facing?

It is very important to understand known and unknown security issues from your organization are facing business impacts. These can be affecting your company CIA (Confidentiality, Integrity and Availability). If you have already experienced issues, then list them out or else make standard use cases which will help you to detect and prevent the attacks.

List out the existing problems and impacts so that your implementation of SOC can resolve it. It is good to think about future problems as well, but it is mandating to cover the existing one.

"*Cybersecurity is a shared responsibility, and it boils down to this: in cyber security, the more systems we secure, the more secure we are all*" - Jeh Johnson

What is your short-term vision and long-term vision?

Define your goals and visions which will support your business and compare your visions with the Risks which might your organization faces. Set the new goals for limited time to evaluate the progress.

What does it take?

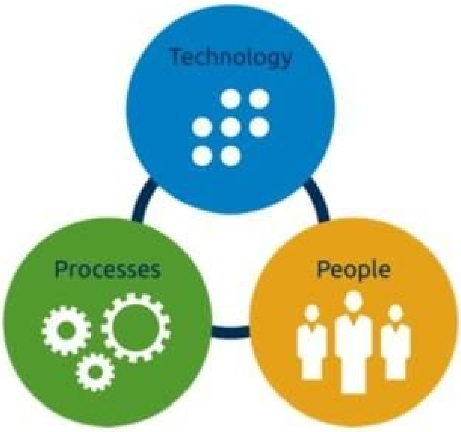
Obvious thing is, it needs your precious time, people, process and product (Technology) and governance. There are some things which your organization can handle, and some cannot. In this case, needs to understand and list out those tasks/resources which can be outsourced.

What do we need?

Understanding the environment (Network), employees and resources which are needs to be monitored. Then, Calculate the budget which can be allocated to SOC. Then plan, evaluate and divide the budget for technologies and people to run the SOC without any diversions.

From the beginning, it is good to have a framework which will help to implement the process. It is recommended to use ITIL framework (Life Cycle) which will help to define, design, transiting and the execution of the process including continuous improvement. Now we will see how the basic rule of SOC implementation starting with People.

The significant components of a SOC , appeared in the figure, are people, processes , and technology.



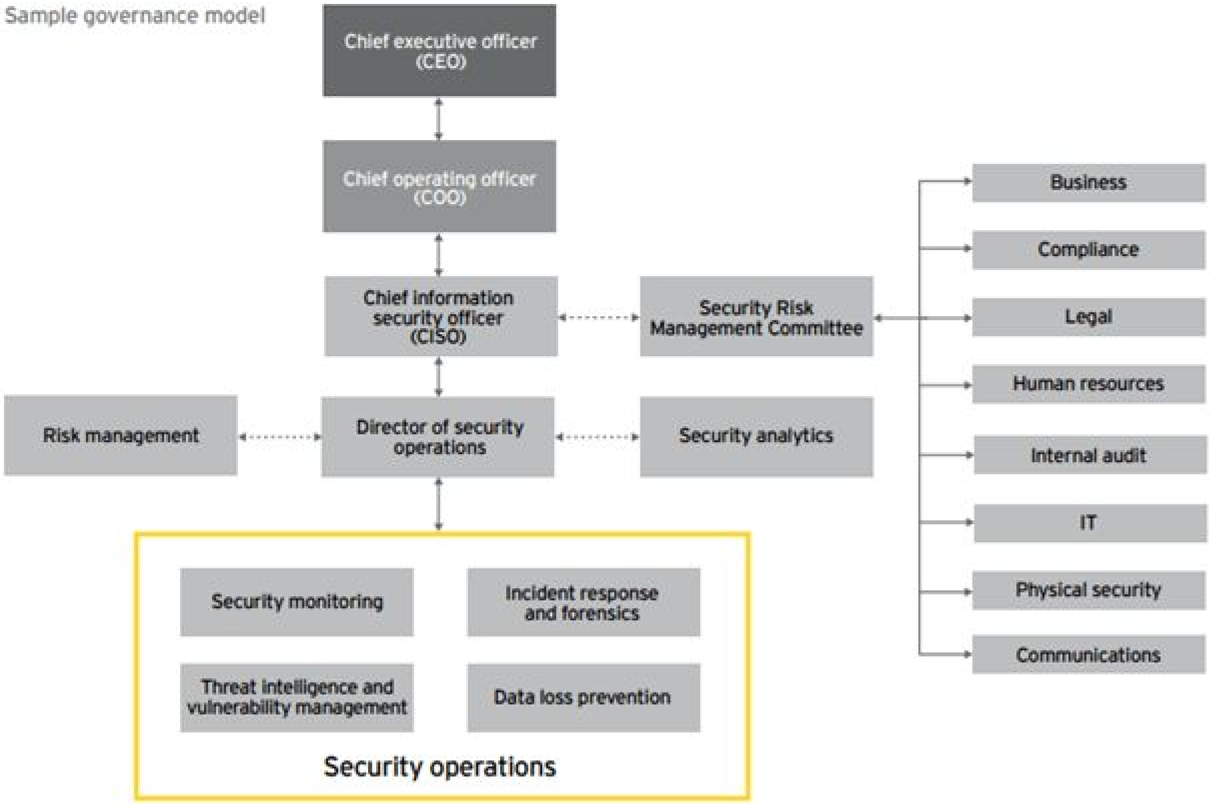
People:

SOC requires people who work in all the levels of management operations. It is good to have or adopt the governance model which will help to construct the team which will run the operation smooth and efficient manner.

People are required with a different kind of knowledge and experience in the various security domains including as below:

- Business.
- Compliance.
- Legal.
- Human Resource.
- Internal Audit.
- IT.
- Physical Security.
- Communication.
- Dedicated specialized security analyst team (Offensive and Defensive).

Below is the Organizational hierarchy for handling security which will cover all the levels of management to track the security in all aspects. From the ITIL framework, we can make use of the RACI model to have the design of Responsible, Accountable, Consulted and Informed.


Sample governance model
Chief executive officer (CEO)
Chief operating officer (COO)
Chief information security officer (CISO)
Security Risk Management Committee
Risk management
Director of security operations
Security analytics
Business
Compliance
Legal
Human resources
Internal audit
IT
Physical security
Communications
Security monitoring
Incident response and forensics
Threat intelligence and vulnerability management
Data loss prevention
Security operations

The SANS Institute (www.sans.org) classifies the roles people play in a SOC into four job titles:

- Tier 1 Alert Analyst – These professionals monitor incoming alerts, verify that a true incident has occurred, and forward tickets to Tier 2, if necessary.
- Tier 2 Incident Responder - These professionals are responsible for deep investigation of incidents and advise remediation or action to be taken.

- Tier 3 Subject Matter Expert (SME)/Hunter – These professionals have expert-level skills in network, endpoint, threat intelligence, and malware reverse engineering. They are experts at tracing the processes of the malware to determine its impact and how it can be removed. They are also deeply involved in hunting for potential threats and implementing threat detection tools.
- SOC Manager – This professional manages all the resources of the SOC and serves as the point of contact for the larger organization or customer.

The core SOC team should be talented having deep technical knowledge in all the security domains to detect, investigate and prevent security incidents. They should be capable of analyzing a large volume of data and Core team should have escalation Matrix with defined levels based on the responsibilities, capabilities, knowledge, and experience. Designations can L1 (Junior), L2 (Senior), L3 (Lead) and Consultant and Manager. Additionally, it would be great if there is a team formed and aligned properly. For example, the Red Team (Offensive security), blue team (Defensive Security), Compliance Team and Risk Identity management Team soon. These all teams work together to have the proper security to the organization and the business.

The most important part of people in SOC is their roles and responsibilities. To understand these, you just need to answer three simple questions.

Who are they?

Some people, they work for Mission, vision, and values, those are top-level executive officers such as CEO and COO. Some people they work for Governance and Operations, those are all CISO and Director of Security. Some people they work for an organization, roles, and other responsibilities and they are SOC core teams such as Managers, Leads, Seniors and Juniors.

How do they work?

All people will have their own uniqueness and talents. These talents will be identified and placed in required positions as mentioned in the Organization hierarchy. All people will work using their skills, capabilities, communications, processes, technology, and tools. Every person or the team should be working by maintaining the quality, efficiency, consistency and team spirits.

What do they do?

Every person will have his defined set of tasks to do. SOC team is basically working majorly on two categories and those are Operations and Service.

1. Operations: Security Monitoring, Information Security Incident Response, and Risk Reporting and Analytics.
2. Services: Digital Forensic and Malware Analysis, Threat and Vulnerability Assessment and Monitoring Technology Optimization.

It is important to hire the required people based on the tool and work experience. It is better to match technology which you are using and their experience. It might cut down your training cost.

The day of a Tier 1 Analyst starts with observing security ready lines. A ticketing framework is every now and again used to enable investigators to choose alarms from a line to research. Since the product that creates cautions can trigger false alerts, one employment of the Tier 1 Analyst may be to check that an alarm speaks to a genuine security episode. At the point when check is set up, the episode can be sent to specialists or other security work force to be followed up on, or settled as a false caution.

In the event that a ticket can't be settled, the Tier 1 Analyst will forward the ticket to a Tier 2 Analyst for more profound examination and remediation. On the off chance that the Tier 2 Analyst can't resolve the ticket, she will forward it to a Tier 3 Analyst with inside and out learning and risk chasing aptitudes.

<u>Process:</u>

Most of the time SOC works on various processes which need to be followed by the team to keep the operations smooth and tracked. Instead of having various processes, can have few processes which are well defined and can be followed in a good way to make the operations easy and efficient manner. Let's see what all processes can be used to implement and make the SOC successful.

- Incident response plans: Every SOC should have the process of how to detect, investigate, remediation and prevention of threat.
- Playbooks for all types of Cyber Attacks: incident response plan should also contain the process/steps/procedures to respond to a specific type of threat.
- Incident Escalation Matrix: Every response plan should be there in place and should be escalated to the next level based on the criticality.
- Security policies and guidelines: Every process/task/procedure should have security policies and guidelines to avoid future legal actions.
- Incident investigation report: Every occurred incident should be investigated and well documented for further reference. It can be for the compliance or the investigation reference.
- Change management: Keeping the change management process in place can avoid confusion of incident which is monitored by the Blue team and incident response team.
- Roles and responsibilities of a team and team members: It is best practice to define all the roles and responsibilities of the team so that those can be useful when it is required.
- Threat/Asset/Risk management: As an on-going process it is recommended to maintain the Threat management (Defense in Depth)/Asset management and Risk management process which helps blue to understand the monitoring environment.
- Continuous improvement processes: It is good to have other continuous improvement processes such as regular review of security controls, awareness/Training programs etc.
- The process to connect SOC with other teams such as DevOps, IT, Patch management etc.

Technology:

It is the most confusing part of understanding the needs and choosing the proper technology which suits for feature requirement and cost.

For choosing technology and products or tools, there will be experience required to measure the product from all the perspective. There are few important measurement points need to be noted before choosing the product and technology.

The requirement for your network: Decide what are all your network loopholes and then decide whether you require controls or detectors. Better to use defense in depth model to figure out the present challenges.

- Features: the present market will provide various products for each solution, it is good to have more feature which will satisfy your basic needs and more can be chosen based on the recommendations.
- Cost: Calculate the cost of the required device, technology which provides more features and less cost. Adjust the budget or the device but choice should excellent. There are some cases where you might require an Intrusion detection system but if you get the intrusion prevention system in the same cost then go for it. Choosing options among many will be confusion.
- Support: Excellent support for the technology or the product can help to use the technology in an efficient manner for the best results. Getting support from the vendor will give you overall details about products and ideas to use it as per the requirements.
- Ease of use: Getting more featured product is good until the user know how to use and it can be configured or handled in a good manner if it is easy to use or self-guiding.

- Review: There are many ways you can review the product for choosing a good one. Compare all the above key points to each device and definitely, you might get a good product. The offline and online review can be considered.

What are the most devices/technology which is used by SOC for securing your network?

- System Level: Anti-Virus, Anti-Malware, DLP (Data Loss Prevention) and Disk locker etc.
- Network level: SIEM, firewall, IDS, IPS, VPN, WAF, VAS, HoneyNet, Spam Filters, Web filters etc.
- Physical level: Biometrics, Passcode tokens, and Security cameras etc.

After having all in place, just following the ITIL lifecycle can maintain continuous improvements on the operations and security.

Summary

Security Operations Centers (SOC) are responsible for preventing, detecting, and responding to cybercrime. SOCs consist of people following processes to use technologies to respond to threats. There are four main roles in the SOC. Tier 1 analysts verify security alerts using network data. Tier 2 responders investigate verified incidents and decide on how to act. Tier 3 SME/Hunters are experts and are able to investigate threats at the highest level. The fourth role is the SOC managers. They manage the resources of the center and communicate with customers. Customers can be internal or external. A SOC may be operated by a single company or may provide services to many companies. Finally, although network security is extremely important, it cannot interfere with the ability of the company and its employees to fulfill the mission of an organization.

Chapter 4 Open source tools for Security Operations

By Prasannakumar B Mundas

As we know there are many things included for building SOC. From a technology standpoint, it is very important to have open source tools for identifying threats as well as for cost reduction. From the DID (Defense in-depth) standpoint there are many devices and technologies that need to be used to build the SOC. As per the industry experience below is the technologies can be used for building proper SOC to monitor the threats to detect the anomaly to safeguard the company.

Mainly since most of the attacks come from external sources, it is very important to use proper controls at the perimeter of the network. By using the open source products we can reduce the cost of the product and support is not mandatory.

IDS/IPS: Intrusion detection system is very important which is required to monitor the traffic for identifying or detecting the anomaly and attacks. Snort is one of the open sources network-based intrusion detection/prevention systems which can perform real-time traffic analysis with packet logging on internet protocol networks. Snort has 5 important components which help to detect the attacks.

- Packet Decoder
- Preprocessors
- Detection Engine
- Logging and Alerting System
- Output Modules

By using the above components, Snort can detect the network-based attacks or probes including operating system fingerprinting attempts, semantic URL attacks, buffer overflows, SMB (Server Message Blocks) and stealth port scans. And, it can also detect web application attacks such as SQL Injections,

Since Snort is just an engine it requires GUI for ease of use if you are not very familiar with the command line, so it is good to configure Snorby as well requires normal web server application such as Apache.

Snorby will be helpful in analyzing the alerts which are triggered by snort. It helps to see alerts, alert matching criteria.

Tip: Make sure all signatures are updated for detecting and preventing emerging threats. These can be open-source or paid signatures (Depends on a budget).

For more details please refer to https://www.snort.org/.

Vulnerability Scanner (OpenVAS): For being proactive security guy it is most important to have vulnerability scanner so that scan and confirm whether any assets are running with critical vulnerabilities which can lead to any security breach or attack. A vulnerability scanner is a product which has various updated scripts which are useful to identify the vulnerabilities in a system or applications. Performing regular scans on the systems especially the external facing systems or systems which are connected to the internet and patching those regularly.

Tip: For every update or deployment it is mandatory to make sure all the systems or applications patched for existing vulnerabilities.

There are various tools which are open-source with limited licensing such as OpenVAS. Regular update of NVT is useful to detect the emerging vulnerabilities.

An OpenVAS engine can use with GUI Greenbone and Barnyard database for populating results in UI. It can scan all the system in the network and it is good to have authenticated scan using domain credentials. Greenbone provides options for creating credentials, hosts, tasks, and schedules in the user interface. For more details refer to http://openvas.org/

For effectiveness, it is better to use emerging tools such as caldera intelligent tool which can be used to emulate the adversary behavior and this is developed by MITRE. For more details please refer to https://www.mitre.org/research/technology-transfer/open-source-software/caldera.

Some of the other tools are:

Maltego (https://www.paterva.com/web7/buy/maltego-clients/maltego.php): Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for the discovery of data from open sources and visualizing that information in a graph format, suitable for link analysis and data mining.

Vega (https://subgraph.com/vega/): Vega is a free and open source web security scanner and web security testing platform to test the security of web applications. Vega can help you find and validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information and other vulnerabilities. It is written in Java, GUI based and runs on Linux, OS X, and Windows.

Nessus (https://www.tenable.com/products/nessus/nessus-professional): Nessus widely used effective vulnerability scanner with more features.

HoneyNet: Nowadays, attackers are getting smarter every day, so it is good to have honeynet to see and analyze the attack patterns which are tried by the attackers to know and defending. It is a very important technology which is mandatory to trick the attacker and safeguarding the assets. You can use Honeynet as internal honeynet or external honeynet as per the requirement. Just mimic the used services to avoid the actual attacks. HoneyNet has mainly 4 components such as mentioned below.

- Nova user interface
- Honeyd engine
- Haystack
- Quasar

For more details about the Honeynet please refer to https://www.honeynet.org/

HIDS (OSSEC): OSSEC: Open Source HIDS SECurity is a free, open-source host-based intrusion detection system (HIDS). It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, time-based alerting, and active response. It provides intrusion detection for most operating systems, including Linux, OpenBSD, FreeBSD, OS X, Solaris, and Windows. OSSEC has a centralized, cross-platform architecture allowing multiple systems to be easily monitored and managed. OSSEC has a log analysis engine that is able to correlate and analyze logs from multiple devices and formats.

For more details please refer to https://www.ossec.net/ and https://github.com/ossec/ossec-hids

Network Monitoring tool: Nagios Core, is a free and open source computer-software application that monitors systems, networks, and infrastructure. Nagios offers to monitor and alerting services for servers, switches, applications and services. For more details please refer https://www.nagios.com/products/nagios-core/attachment/visibility-2/

Red team activities: It is good to use Kali Linux or Backtrack operating systems which are having all the tools which are required for vulnerability and penetration testing.

Kali (https://www.kali.org/downloads/): Kali Linux is an advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments. It is the net version of Backtrack.

Commando VM (https://www.fireeye.com/blog/threat-research/2019/03/commando-vm-windows-offensive-distribution.html). Commando VM is the new Penetration testing Opensource Virtual Machine build on Windows Operating system with full of penetration testing tools inbuilt and it was built by FireEye.

Forensic: For being more in forensic like malware analysis, and recovery, there are various Microsoft tools and other open source frameworks as mentioned below:

Cuckoo sandbox framework (https://cuckoosandbox.org): Cuckoo is a dynamic malware analysis framework which provides end to end analysis of malware with the formatted report and it supports various plugin such as VirusTotal, IDS, and Yara, etc.

Remnux (https://h11dfs.com/the-best-open-source-digital-forensic-tools/): Remnux is open source reverse engineering virtual machine built with various reverse engineering tools inbuilt.

Ghidra (https://www.nsa.gov/resources/everyone/ghidra/): Ghidra is a software reverse engineering (SRE) framework developed by NSA's Research Directorate for NSA's cybersecurity mission. It helps analyze malicious code and malware like viruses and can give cybersecurity professionals a better understanding of potential vulnerabilities in their networks and systems.

Threat intelligence sharing platforms: Threat intelligence sharing platform play an important role in detecting attacks and infections based on the indicators of compromises. It can be integrated into your log management and network monitoring tools to have proper prevention and detection in place.

MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing and abbreviated as Malware Information Sharing Platform which built using various tools technologies such as MySQL, PostgreSQL, Shell script and Python, etc.

For more details please refer to https://www.misp-project.org/ and https://github.com/MISP/MISP

Reference links would be more helpful for going further such as hardware and software requirements. There are some of the open source tools which can be used based on the requirement and SOC capabilities. These are shortlisted based on ease of use and industry experiences. To run the SOC smooth and cost-effectively, these tools play important roles.

Chapter 5 Threat Intelligence

By Digit Oktavianto

Latest trend of threats in information security landscape become more sophisticated since attacker now prefer and focus on targeted attack rather than random attack. The degree of threat sophistication is expanding very rapidly and giving serious impact on individuals, businesses and governments. As a result, cyber defense technique is becoming increasingly significant to anticipate the evolving threat. Traditional defense mechanism such as monitoring, detection and preventive program is not sufficient enough and most of the time fails to detect new kind of attack using unknown malware variants and attack that perform evasive maneuver. Cyber threat intelligence concept offer deep insight, provide the ability to recognize and act upon indicators of attack and compromise scenarios in a timely manner. Threat intelligence also described as evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

Several questions that came up after the incident occur will be : what kind of attack, when did it happen, where was it found, how can the attacker breach into our system, and who is the attacker. Suddenly the entire organization become more reactive and seems to be concerned about security issue after the incident occurred. But it is too late, the attacker may have been hiding in our system for several days, weeks, months and collects all sensitive information or steal confidential document from your company. The sooner you can adapt to the latest type of attack, the more you can learn how to protect your system. The threats to our national security and economic interests in the cyber arena vary in identity, objectives, assets, and capabilities. Their range can stretch from disruption, to simple theft, to taking down critical infrastructure, to disrupt government functions. The advantage almost always lies with the threat. Ability and intent of these actors become important distinctions to the defender's action [1].

To develop a serious plan for combating cyber criminal, company needs to understand the basic capability and readiness of their infrastructure. Old approaches such as intrusion detection systems, anti-virus, is no longer sufficient to combat the modern attack. Organizations need to take a more proactive approach on their cyber defense mechanism than reactive mechanism. Cyber threat intelligence has an important role to help organization combating the cyber security threat. Cyber threat intelligence (CTI) is an advanced process that enables the organization to gather valuable insights based on the analysis of contextual and situational risks and can be tailored to the organization's specific threat landscape, its industry and markets[2]. Threat intelligence is not intrusion detection system, not a firewall that can block attacks in real time, not an antivirus that match signature the bad program and eliminate it from your system, but in fact threat intelligence is a method that represents the collaboration of information and providing data on potential threats with a deep insight of network structure, operations, and activities.

References

- Intelligence and National Security Alliance, "Cyber Intelligence: Setting the Landscape for an Emerging Discipline," *INSA Online Whitepaper*, p. 17, September 2011.

- Ernst and Young, "Cyber Threat Intelligence - How to Get Ahead of Cybercrime," 2014.

Chapter 6: Incident Handling

By Mohamed Mouldi Chaouch

Introduction

Nowadays cyber threats are growing day by day, there is no way to protect the business strategy of organizations rather than planning and preparing to prevent security incidents.

The incident handling process has several phases going from preparation to Post-incident activity.

It is important to note the skills sets for the incident handling and incident response. Incident Handlers need to be a good communicator and it is necessary to have project management talents. Incident Response must have good knowledge of technical parts like networking, malware analysis, forensics, etc.

1. Preparation

The preparation phase involves establishing and training an Incident Response Team and acquiring the necessary tools and resources.

a - Preparing to handle incidents

This phase as its name implies deals with preparing a team to be ready to handle an incident at a moment's notice.

There are several key elements to have implemented in this phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident.

These lists are the organization's incident handler's needs:

+ Incident handler communications and facilities:

- Contact information.
- On-call information
- Incident reporting mechanisms
- Issue tracking system for tracking incident information, status, etc.
- Smart-phones.
- Encryption software.
- War room for central communications among team members.
- Secure storage facilities.

+ Incident analysis hardware and software:

- Digital forensic workstations and/or backup devices.
- Laptops.
- Spare workstations, servers, and networking equipment, or virtualized equivalents.
- Blank removable media.
- Portable printer.
- Packet sniffers and protocol analyzers.
- Digital forensic software.
- Removable media.
- Evidence gathering accessories.

+ Incident analysis resources:

- Port lists.
- Documentation.
- Network diagrams and lists of critical assets.
- Current baselines.
- Cryptographic hashes.

+ Incident Mitigation Software:

- Access to images of clean OS and application installations for restoration and recovery purposes.

b - Preventing Incidents:

- The goal of this phase is to prevent overwhelming the incident response team with incidents; because this can lead to slow and incomplete responses.
- The incident response team can be advocates of sound security practices, but they are not responsible for securing resources.
- The team can play a key role in risk assessment and best practices for securing networks, systems, and applications.

2. Detection and Analysis

This phase is to determine whether the incident is really occurring and analyze its nature.

a - Attack Vectors:

Incidents can occur in countless ways, so to facilitate the work we must define a basis of attack vectors to provide a classification for incidents, then go through it to handling more specific attacks, we mention some of it ;

- External/Removable Media.
- Attrition (brute force attack against an authentication mechanism, impair or deny access to a service or application).
- Web (XSS, SQLI).
- Email.
- Impersonation.
- Improper Usage.
- Loss or Theft of Equipment.

b - Signs of an Incident:

The major challenge for the response team is the accuracy in detecting incidents, there are three factors which make this so difficult:

- Multiple ways to detect incidents (Automated detection (IDPSs, log analyzers, etc.) and manual detection (problems reported by users)).
- The volume of potential signs of incidents is very high.
- Deep & specialized technical knowledge.

Signs are identified using many different sources, the common are computer security software alerts, logs, publicly available information, and people.

Signs of an incident fall into one of two categories:

+ Precursor: Precursor is a sign that an incident may occur in the future. Examples of precursors are:

- An announcement of a new exploit that targets a vulnerability of technologies used by the organization.
- Log entries that show the usage of a vulnerability scanner.

+ Indicator: Indicators is a sign that an incident may have occurred or may be occurring now like:

- A system administrator sees a filename with unusual characters.
- A host records an auditing configuration change in its log.
- Multiple failed login attempts from an unfamiliar remote system.
- Alerts from security devices.

c - Incident Analysis:

Incident detection and analysis will be conducted efficiently when all of our precursors and indicators are accurate, unfortunately, this is not the case because of different reasons:

- IDS may produce false positive alerts.

- Incorrect indicators provided by users.
- Correct indicators, but has other errors than a security incident like human errors.

So these are recommendations for making incident analysis easier and more effective:

- Profile Networks and Systems: Profiling is measuring the characteristics of expected activity so that changes to it can be more easily identified (monitoring network bandwidth usage to detect if there is an unsuspected traffic)
- Understand normal behaviors to easily recognize the abnormal behavior, to gain this knowledge is to go through reviewing log entries and security alerts.
- Create a Log Retention Policy: this may be helpful when log entries show reconnaissance activity or previous instances of similar attacks, and when incidents may not be discovered for months or more.
- Perform Event correlation: Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.
- Keep all host clocks synchronized to facilitate the event correlation task.
- Maintain and use a knowledge base of information: aggregate documents, spreadsheets, significance and validity of signs into a database that provide flexible and searchable mechanisms for sharing data among team members.
- Run packet sniffers to collect additional data that matches specified criteria.
- Filter the Data: filter out categories of indicators that tend to be insignificant or show only the categories of indicators that are of the highest significance.
- Seek assistance from others(internal information security staff, external like CSIRT…) when the team is incapable to determine the cause and nature of an incident.

All these recommendations can aid the team to determine the incident’s scope, the origin of the incident, and how the incident is occurring.

d - Incident Prioritization:

Handling incidents should be prioritized based on three factors:

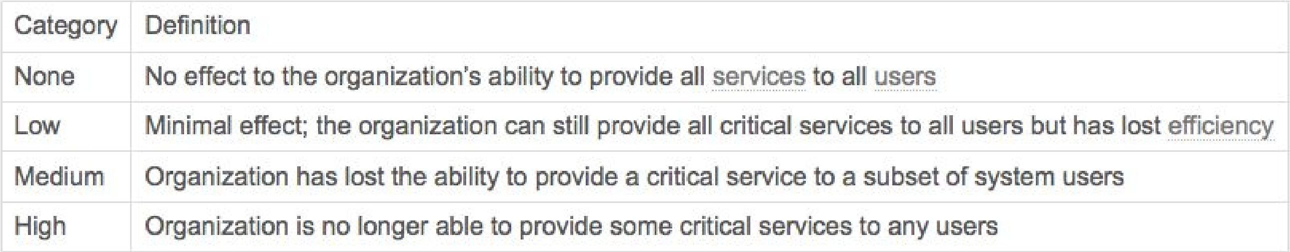
- Functional Impact of the Incident: Incident handlers should consider how the incident will impact the existing functionality of the affected systems and the future functional impact if the incident is not immediately contained.
- Information Impact of the Incident: Incident handlers should consider how this incident will impact the organization's overall mission.
- Recoverability from the Incident: Incident handlers should consider the effort necessary to actually recover from an incident.

Combining the two first impacts determines the business impact of the incident, for example, a DDOS attack against a public web server may temporarily attrition the service, whereas unauthorized root-level access to a public web server may result in the exfiltration of personally identifiable information (PII).

For the recoverability from the incident, the team may intervene when there is a high functional impact and low effort to recover from this.

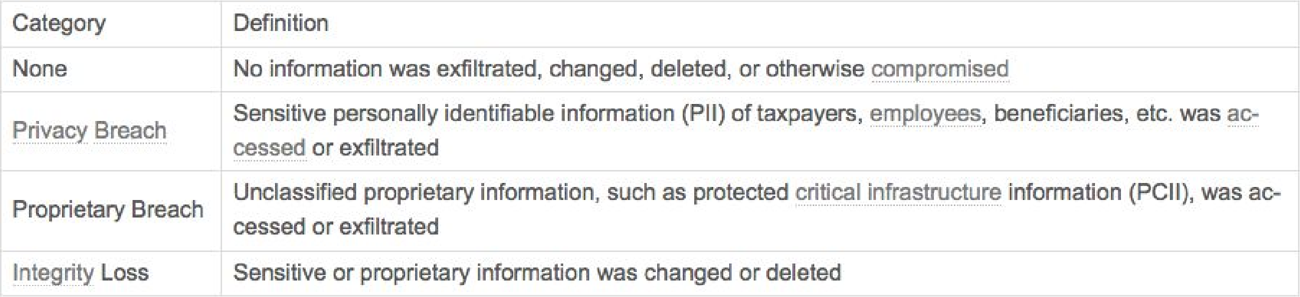
The organization can rate the incidents to better prioritize, this is are tables to rate the factors:

Table 1: Functional Impact Categories



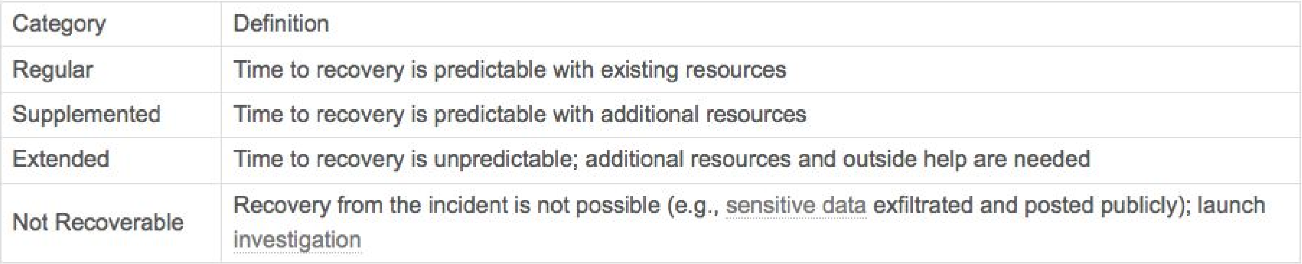
Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Table 2: Information Impact Categories



Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Table 3: Recoverability Effort Categories



Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Organizations should also establish an escalation process for those instances when the team does not respond to an incident within the designated time. People may have personal emergencies. The escalation process should state how long a person should wait for a response and what to do if no response occurs. Generally, the first step is to duplicate the initial contact. After waiting for a brief time the caller should escalate the incident to a higher level, such as the incident response team manager. If that person does not respond within a certain time, then the incident should be escalated to a higher level of management. This process should be repeated until someone responds.

3. Containment

This phase is to contain the breach to stop spreading and cause further damage to your business.

a - Choosing a Containment Strategy:

Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decision making. Criteria for determining the appropriate strategy include:

- Potential damage to and theft of resources.
- Need for evidence preservation.
- Service availability.
- Time and resources needed to implement the strategy.
- Effectiveness of the strategy.
- Duration of the solution.

b - Evidence Gathering and Handling:

Evidence should be collected according to procedures that meet all applicable laws and regulations that have been developed from previous discussions with legal staff and appropriate law enforcement agencies so that any evidence can be admissible in court.

All the evidence must be logged:

- Identifying information (MAC address, IP address, hostname, etc.).
- Information of who collected or handled the evidence during the investigation (phone number, Email, Name, Title).
- Time and date of each occurrence of evidence handling.
- Locations where the evidence was stored.

c - Identifying the Attacking Hosts:

These are the most commonly performed activities for attacking host identification:

- Validating the attacking host's IP address.
- Researching the attacking host through search engines.
- Using incident database.
- Monitoring possible attacker communication channels

4. Eradication

Eradication is the way to eliminate components of the incident, the team must go through identifying and mitigating all vulnerabilities that were exploited, identifying all affected hosts, systems should again be hardened and patched, and updates should be applied.

Eliminating attacker residuals includes:

- Removing malware such as backdoors, rootkits, malicious kernel-mode drivers, etc.
- Thoroughly analyze logs to identify credential reuse through remote desktop, SSH, Vnc, etc.

Improving defenses includes:

- Configuring additional router and firewall rules.
- Obscuring the affected system's position.
- Null routing.
- Establishing effective system hardening, patching, and vulnerability assessment procedures, etc.

5. Recovery

In recovery, administrators restore systems to normal operation such as restoring systems from clean backups, tightening network perimeter security.

Take the system through any validation process you have before putting it into production.

6. Post-Incident Activity

This is where you will analyze and document everything about the breach.

This is are the different forms that must be completed:

a - Incident Contact List:

This form should contain the contact details of the organization's:

- CISO/CIO.
- SPOC of: the incident handling or CSIRT team.
- Legal department contact.
- Public relations contact.
- ISP SPOC.
- Local cyber-crime unit.

b - Incident Detection:

This form should contain information such as:

- Information about the first person who detected the incident
- The incident summary (type of incident, incident location, incident detection details, etc.)

c - Incident Casualties:

This form should contain information such as:

- Location of affected systems
- Date and time incident handlers arrived
- Affected system details (hardware vendor, serial number, network connectivity details)

d - Incident Containment:

This form should contain information such as:

- Isolation activities per affected system (date and time the system was isolated, way of system's isolation)

- Back-up activities per affected system (handler that performed the restoration, back-up details, etc.)

e - Incident Eradication:

This form should contain information (one form per affected system is advised) such as:

- Handler(s) performing investigation on the system
- Incident root cause analysis if discovered
- Actions taken to ensure the incident root cause was remediated and the possibility of a new incident eliminated.

This form can be extremely helpful in improving security measures and the incident handling process, it provides a reference that can be used to assist in handling similar incidents, and these reports are good material for training new team members.

At the end, these are the major steps to be performed in the handling of an incident it may vary based on the type of incident.

+ **Detection and Analysis checklist**:

1. Determine whether an incident has occurred

1.1 Analyze the precursors and indicators

1.2 Look for correlating information

1.3 Perform research (e.g., search engines, knowledge base)

1.4 As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence

2. Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)

3. Report the incident to the appropriate internal personnel and external organizations

+ **Containment, Eradication, and Recovery**

4. Acquire, preserve, secure, and document evidence

5. Contain the incident

6. Eradicate the incident

6.1 Identify and mitigate all vulnerabilities that were exploited

6.2 Remove malware, inappropriate materials, and other components

6.3 If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them

7. Recover from the incident

7.1 Return affected systems to an operationally ready state

7.2 Confirm that the affected systems are functioning normally

7.3 If necessary, implement additional monitoring to look for future related activity

+ **Post-Incident Activity**

8. Create a follow-up report

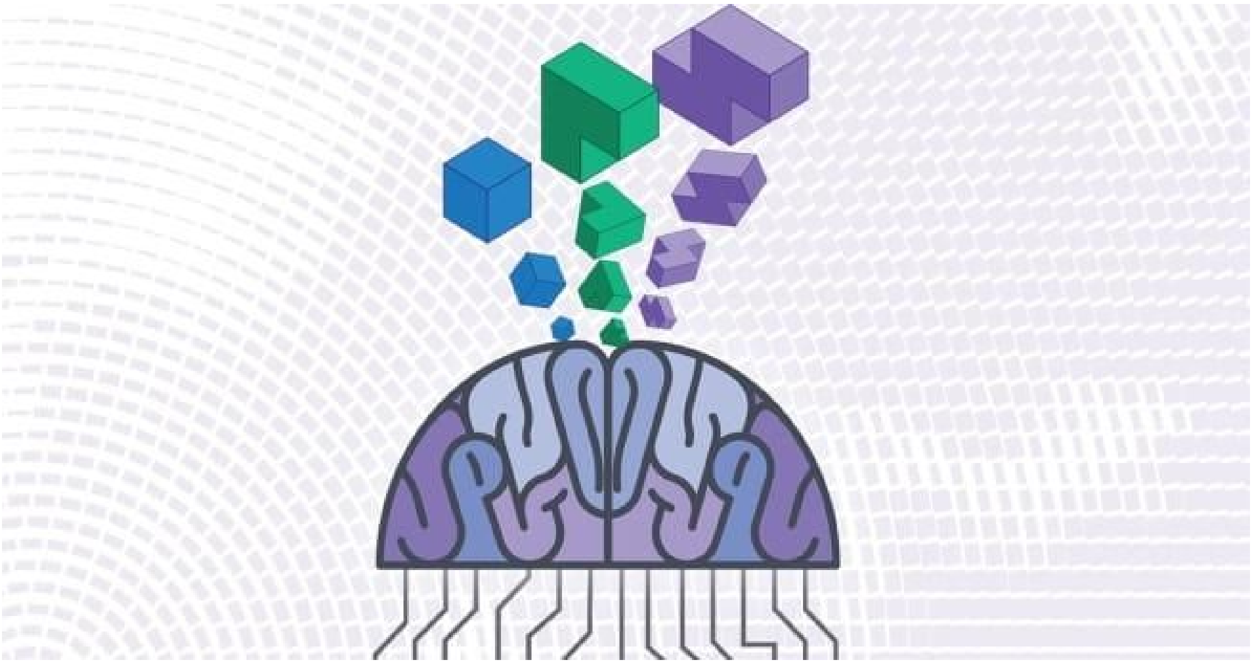
Summary

This chapter describes the best practices when we go through an incident, how to Prepare for it, know what to do when it happens, and learn all that you can afterwards

Chapter 7: Threat Hunting

By Ali Ahangari

Imagine you are familiar with the most common techniques for threat hunting. As a starting point, you need suitable data to start the hunting process. In this post, I will explain the most common datasets every hunter would need them. These datasets fall into two main categories: Network Data, Endpoint Data.



Network Data

- Network session data

Contains information on network connections between hosts. Critical metadata associated with network connections include the source IP address, destination IP address, destination port, start time of the connection, and end time/duration of the connection. Includes Netflow, IPFIX, and similar data sources.

- IDS/IPS logs

IDS/IPSs can collect connection-based flow data and application protocol metadata (HTTP, DNS, SMTP).

- Proxy logs

HTTP data that contains information on outgoing web requests, including Internet resources that internal clients are accessing.

- DNS logs

Contains data related to DNS domain resolution activity, including domain-to-IP address mappings and identification of internal clients making resolution requests.

- Firewall logs

Connection data that contains information on network traffic at the border of a network, focused on blocked connections.

Endpoint Data

- Process execution metadata

Contains information on processes run on specific hosts. Critical metadata associated with process execution includes command-line commands/arguments and process filenames and ID.

- Registry access data

Contains data related to registry objects, including key and value metadata.

- File data

Information on stored file and artifacts kept on a local host. This can include when files were created or modified, as well as size, type, and storage location information.

Possible Indicators in Endpoint Logs

Endpoint Logs may consist of many data sources including, but not limited to, Anti-Virus Logs, Windows Logs, HIDS Logs.

But what should hunters look for in Endpoint Logs? In a sense, what threats can we find in Endpoint logs?

You, as a threat hunter, may look for the following indicators in the logs:

- Suspicious New Process Creation
- Suspicious Registry Modifications
- Suspicious Access an Object
- Identify potential 0-day exploits
- Attacks on Windows Applications
- Suspicious Schedule Task Usage
- Suspicious Services Usage
- Suspicious Account Usage
- Suspicious Network Share

- Suspicious Group Policy Change
- Suspicious Windows Firewall Changes
- Remote File Copy
- SSH Hijacking

These indicators are only as a sample of many other possible ones.

What we are looking for in AV Logs

Before doing so, It's necessary to mention that Anti-Viruses sometimes can not detect malwares but they record logs process calls, changing files, and so on. This is where threat hunting plays a key role, detecting possible threats from what AVs didn't.

Now, I want to explain items that you can find in AV logs. These items include but not limited to:

- Identifying known password dumpers, droppers and backdoors (Both Deleted and not deleted)
- Detecting execution of binary from users APP Data directory
- Identifying process launching without parent process or services (e.g. Svchost.exe launching without Services.exe being its parent process)
- Identifying scheduled jobs to perform known malicious behavior
- Investigating alerts for executable on web or application server

- looking for process launch from odd directory locations

By doing so, you, as a hunter, can find valuable things that AVs didn’t.

Good and Bad Examples of Threat Hunting

Respondents provided brief descriptions of their threat hunting processes. Here are some examples of good processes:

- Good Examples of Threat Hunting
  - Starting with tools, Techniques or Procedures (TTPs) or a vulnerability, develop hypotheses to determine whether our infrastructure is impacted, and then test those hypotheses.
  - First, baseline the environment for normal activity. Create a hypothesis based on the kill chain. Utilize ATT&CK framework for TTPs. Run IOC sweeps from threat intel reports.
  - Gather intel, develop a hypothesis, create a scope and execute the hunt.
  - Form a hypothesis or use evidence from intel, then determine the best way(s) to find activity on the network or hosts, both for the current point in time and for future events
  - Identify a hypothesis of what to hunt for, review documentation of past hunts, peer review the proposal, notify the team and begin work, collect and normalize data, analyze data, identify findings, take immediate action for any detected intrusions and declare the incident, and determine non-immediate adjustments to controls and detection mechanisms.
  - A threat hunting process starts with generating hypotheses (assuming we have been breached in a given way) and then verifying the hypothesis by hunting for the related indicators in all relevant data sources using log analysis and then marking the hypothesis as true or false in the end.

These are examples from respondents that are just performing intrusion detection - not threat hunting:

- Bad Examples of Threat Hunting
  - Notice an alert in the system and slowly tear it apart from endpoint to endpoint.
  - Spend a lot of time reviewing logs from the SIEM and formulating custom queries in the SIEM.
  - Analyst watches logs and endpoint events. Non-baseline behavior or triggered events create a potential incident. Analyst reviews network traffic and isolates potentially affected systems. Standard IR rolls from there.
  - Team's entire operation is constantly monitoring the environment to establish its baseline. As soon as they detect something odd or they are made aware of something risky in their environment (such as a malicious IP address communicating with us), they start an analysis on that resource: network behavior, processes behaviors, logs and possible strange evidence through the filesystem and registry.
  - Analysts have antivirus deployed on most endpoints. The signature that has been triggered the most is investigated and hunted for its root cause, and they try to reduce its count by next week.
  - Threat hunting is triggered by SIEM alerts or AV alerts.

Common Misunderstandings About Threat Hunting

According to Sqrrl, there are 3 common mistakes when it comes to threat hunting.

1. Hunting can be fully automated

Hunting is not a reactive activity. If the main human input in a hunt is remediating the result of something that a tool automatically found, you are being reactive and not proactive. You are resolving an identified potential incident, which is a critically important practice in a SOC, but not hunting.

Hunting requires the input of a human analyst and is about proactive, hypothesis-based investigations. The purpose of hunting is specifically to find what is missed by your automated reactive alerting systems. An alert from an automated tool can certainly give you a starting point for an investigation or inform a hypothesis, but an analyst should work through an investigation to understand and expand on the context of what was found to really get the full value of hunting. To put this another way, hunters are the network security equivalent of beat cops; they search for anomalies by patrolling through data, rather than investigating a call in from dispatch.

2. Hunting can only be carried out with vast quantities of data and a stack of advanced tools

Though it may seem like a new term, security analysts across a variety of sectors have been hunting for years. Basic hunting techniques can still be very useful and effective in helping you find the bad guys (e.g. you can perform basic outlier analysis, or “stack counting”, in Microsoft Excel). An analyst who wants to begin threat hunting should not hesitate to dive into some of the basic techniques with just simple data sets and tools. Take advantage of low hanging fruit!

3. Hunting is only for elite analysts; only the security 1% with years of experience can do it

There are many different hunting techniques that have differing levels of complexity. However, not all these techniques take years to master. Many of the same analysis techniques used for incident response and alert investigation and triage can also be leveraged for hunting. The key to getting started is simply knowing what questions to ask, and digging into the datasets related to them. You learn to hunt by doing it, so if you're an analyst who has never hunted before, don't be afraid to dive in.

Ref: https://sqrrl.com/media/Your-Practical-Guide-to-Threat-Hunting.pdf

A Sample Scenario For Threat Hunting

Two main purposes to this case study scenario are:

- To learn technical hunt concepts
- To gain a better understanding of a practical hunting process

Consider a company that hasn't recently identified any malicious behavior on the internal networks. Hunter decides to proactively hunt on the networks. In this sample, he/she uses the organization's most recent cyber risk assessment report to determine priorities and select the assets to hunt on first.

The hunting phases that the hunter follows are:

- Preparation
- Investigation
- Adversary Removal
- Synopsis of the Hunt
- Reporting

Preparation:

- Determine high priority assets:

Before proactive hunting starts, the hunter needs to decide which assets should be the initial focus of the hunt. This can be gained from cyber risk assessment report of the company. The hunter reviews the highest-priority group of IT functions in the report and translates those functions, which are described from a business perspective (e.g., "credit card processing systems"), into the corresponding IT asset information that the hunt team needs: IP addresses, hostnames, process names, usernames, etc.

- Review available IT assets and networks information:

The hunter asks for the company's latest IT network maps and asset inventory information. He will need to confirm as needed which assets of interest are currently connected to the network and to get more information on these assets, such as knowing which major applications each asset is authorized to run, which assets have used the organization's networks in the past and what software they should be running.

- Understand what's considered normal activity:

A hunter who knows what's normal for an organization's assets and networks will be much better prepared to spot deviations from the norm. the hunter is new to the company, so it's worth spending time talking with system administrators, incident responders, and other IT staff members to learn more about normal activity. This can be as simple as knowing what the typical work days and hours are for people in different roles within the company (e.g., standard users, managers, developers, system administrators.) This can also be complex, including gathering detailed information on which assets people in each role may access, and which applications are whitelisted (allowed) or blacklisted (prohibited) on the company's assets.

- Configure and deploy hunt sensor software:

For operational reasons, the company might choose an on-demand deployment strategy or Enterprise-wide deployment. We suppose the company has chosen the first one. The hunter is responsible for ensuring that the hunt sensor software is deployed to all the assets included in the initial round of hunting and also configuring the default settings for the hunt sensors.

- Investigation:

So far, the hunter has completed all the preparatory activities. It's time to investigate the selected assets for the presence of adversaries. This investigation is documented in four parts:

- scoping the investigation
- gathering and analyzing information
- expanding the investigation
- reprioritizing the hunt

Scoping the investigation

Because there's no evidence of compromises or other malicious activity involving these assets, the first step in this investigation is to scope the work by selecting which aspects of each asset will be examined initially. The hunter determines that the most important things to look for all involve the execution of processes and services. These characteristics may fall into three groups:

Currently running processes and services

The hunter needs to examine the full path of the executable for each currently running process and service, to include the executable's filename. Questions to be answered include:

1. Should this executable be running on this machine? Does its full path seem reasonable? For example, is the executable running from the appropriate system or application directory?

2. Which user ran the executable? Does this seem reasonable?

3. Was the executable run from the command line? If so, what were the command line arguments?

4. Does the code in the running process or service exist in a file stored on the asset's disk? If no, why doesn't such a file exist?

5. If the code is in a stored file, does the file's hash match the vendor's hash for the file? Does this file exist on other assets, is it in the same location, and does it have the same hash as the copies on the other assets?

6. Which network connections are bound to the process or service? For each connection, the IP addresses and ports used by both endpoints must be noted.

7. Does it appear that all the loaded modules (executables and DLLs) indicated by the Process Environment Block (PEB) and import tables for a particular process or service are appropriate?

8. Are all registry keys associated with the process or service in the correct locations?

9. Do all open file handles (the files that the process or service is reading from and/or writing to) make sense?

Recently run processes/services

The hunter also needs to examine the available information about processes and services that were recently executed. Such information is available from the "Prefetch" folder and the registry keys for Application Compatibility Cache (ShimCache).

This information must be evaluated to see if the processes and services run on the asset make sense. For example, did the full path of the executable seem reasonable?

Processes/services set to run in the future:

The executables slated to be run can be identified in one of two places:

- Registry auto-run keys. The purpose of these keys is to list executables to be automatically run in the future, such as when the asset is rebooted or when a local user logs in.

- Scheduled tasks. Users can schedule a particular executable to run in the future and designate the date and time when it will be started.

Gathering and analyzing information

At this point, the hunter has defined the scope of the investigation but hasn't yet collected the necessary information within that scope. The company's hunt sensor software can automatically do this work on the hunter's behalf, speeding up the hunt considerably. Remember three key concepts to keep in mind:

- Assume that the asset has already been compromised.
- Look for compromises at any phase of an attack, from an initial exploit to implants that the adversary is no longer utilizing.
- Consider how an adversary would think and react.

The hunter quickly discovers that the primary web server has a running process that seems suspicious. The hunter also takes a closer look at the compromised web server. Additional information to be obtained includes the following:

- The usernames for all users currently logged into the server
- The open file handles for all suspicious processes and services executing on the server
- A copy of each file stored on disk that's related to the suspicious processes and services
- A memory dump for each suspicious process or service
- A packet capture of all network traffic for the server

Reprioritizing the hunt

While the hunt sensors are collecting and analyzing more information, the hunter receives an alert from the hunt sensor on the company's most critical database server. This alert indicates the presence of an unknown persistent service on that server, so he immediately reprioritized hunting to focus on the database server.

Throughout the hunt, hunters must constantly reprioritize their focus based on updated risk assessments, their understanding of the value of particular assets, and the security event information provided by hunt sensors and other enterprise security controls.

A quick review of the current and recent hunt sensor monitoring within the database server indicates that the server has an established, encrypted connection to an external IP address.

The hunter can see that a large amount of data is being transmitted from the database server to the external IP address, and that the service associated with the network connection is the same service that generated the unknown persistent service alert.

Adversary Removal

All evidence points to an adversary exfiltrate sensitive data from the company via the compromised database server. The hunter must act as quickly as possible to stop the compromise by disrupting the exfiltration communications. Possible methods for handling this situation include the following:

- Suspend the thread or threads associated with the exfiltration. Pat must consider the likelihood that the activity is malicious and the criticality of the service being compromised by the thread.
- Kill the service associated with the exfiltration. The hunter would rather suspend the thread than kill the service because the latter can cause a significant disruption to operations. On the other hand, the entire service could be malicious, in which case suspending the thread won't be an effective form of remediation.
- Disable network access. Isolating the database server from other servers prevents further exfiltration and blocks the adversary from accessing the database server. Of course, this isolation also prevents all operational use of the database server, which will cause major production outages.

In this case, the hunt sensor indicates that there's a single malicious thread responsible for exfiltrating data, and the service in question isn't malicious. This makes the decision easy.

Pat orders the database server's hunt sensor to suspend the malicious thread. This action breaks the connection between the database server and the adversary while avoiding any disruption of the critical services that the database server provides to the company's customers, employees, vendors, business partners, and contractors.

Synopsis of the Hunt

Let's fast forward to the end of the hunt investigation and recovery actions related to the compromised database server. Here's a synopsis of the most noteworthy actions:

1. Based on information provided by the hunter and the database server's hunt sensor, the hunter searched all assets across the enterprise for the following:

a. Any network connections involving the same external IP address that the database server was connected to and from which data was exfiltrated.

b. Any files with the same filenames and/or file hashes as the malicious files found on the database server

c. Any registry keys matching the malicious registry keys found on the database server

2. The search for these characteristics identified an additional compromised asset: a Microsoft Exchange server. This server had the same malicious thread, executable file, and registry keys found on the database server, but the executable on the Exchange server was not currently running.

3. The company's incident response team forensically collected all files on the two servers associated with the malicious services, and they initiated chain of custody procedures. The files were turned over to the company's malware reverse engineers for further analysis.

4. The hunter removed all of the malicious files (including executables and other DLLs) and associated malicious registry keys from the compromised assets.

5. System administrators discovered that the compromised web server was missing a patch. Without this patch, the server was susceptible to users executing arbitrary code. The system administrators also determined that the web server and the database server had the same username and password for their local administrator accounts. This is how the adversary gained privileged access to the database server.

6. System administrators forced the change of all passwords for all local accounts on the web server and database server to prevent future reuse of any credentials that were compromised.

7. When the hunter finished hunting on the database server, the hunt sensor was removed from the server in accordance with the company's on-demand deployment strategy.

Hunt Reporting

The hunter documented the findings and results for the hunt on an ongoing basis, issuing a separate report for each major compromise investigated through hunting. His report for the database server compromise includes the following information:

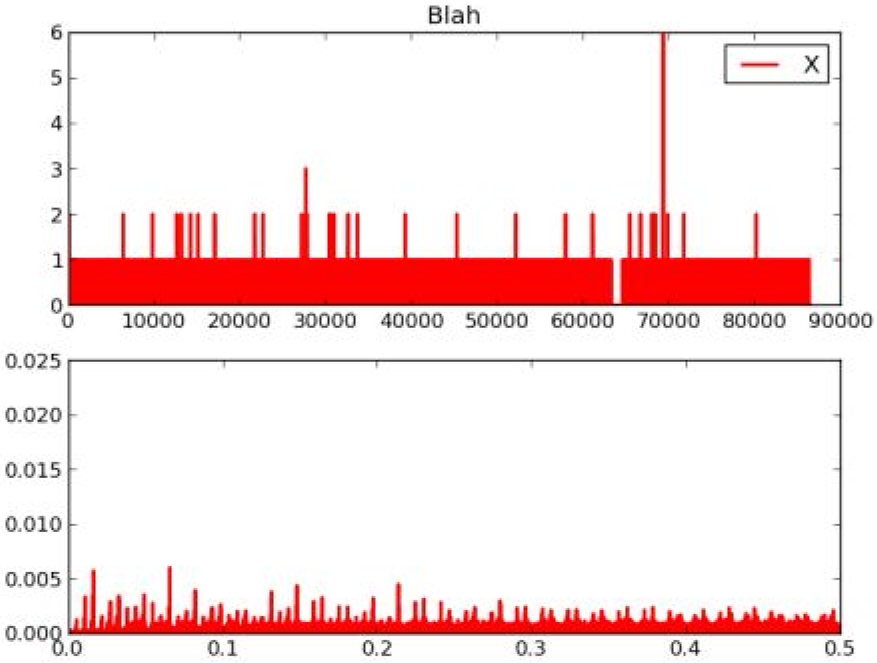
- An executive summary that reiterates the most important points from the report
- The scope of the compromise, such as which business processes, IT assets, users, data sets, etc. were affected, in what ways they were affected, and how long they were affected
- The identity of the adversary, if known
- A timeline of the activities involving the compromise and the hunt investigation into that compromise
- A narrative corresponding to the timeline, indicating what the findings were at each step in the hunt process, which tools or techniques were used for each step, who received information from the hunters and when, what challenges or other issues were encountered and how they were resolved (or why they aren't yet resolved), etc.
- The root cause or causes of the compromise

- Recommendations for improving the company's security and for making future hunts more effective, and the consequences to the company if these recommendations are not followed

Malware Beaconing: How To Hunt

One of the most common malware's behavior is "beacon", which implies that infected hosts communicate to Command and Control servers at **regular intervals** that have relatively **small time variations**. To be more specific, there are two key points about malware beaconing:

1. **It has to beacon (duh).** Meaning that it is regular (every N seconds/minutes/hours/days from any given infected machine). This also means that it is *not* the once-off type.
2. **It does not look like normal traffic.** If you have done web application profiling before, you would have some idea of what normal traffic is like. Most/all of a page's resources are requested for within the first few seconds when the browser loads the page. Anything else is either "AJAX"-type requests (legit), or the suspicious domains that we're looking for. This also helps in avoiding legit domains that enter our radar simply because they generate a lot of requests (the top N domains method).



But how to hunt Malware Beaconing?!

Here is a simple instruction (including 6 steps) to detect malware beaconing.

1. Retrieve proxy events containing a non-null URL;
2. Sort them by time;
3. For every 2 consecutive events matching the same source host and URL,
    1. calculate the time difference between those events, in seconds;
4. Once that difference is calculated for all events, append to every row/event (per source host and URL):
    1. the number of events matched;
    2. the standard deviation of the time differences between consecutive events;
5. Filter in only those rows where the standard deviation is below 5 and with count greater than 100 (thresholds may be adjusted);

6. Finally, group every relevant attribute/field by URL, including the count of unique source hosts and start checking the output.

Let's review the instruction again:

1. Retrieve proxy events containing a non-null URL;
2. Sort them by time (epoch);
3. For every 2 consecutive events matching the same source host and URL,
    - calculate the time difference between those events, in seconds;
4. Once that difference is calculated for all events, append to every row/event (per source host and URL):
    - the number of events matched (count);
    - the standard deviation of the time differences between consecutive events;
5. Filter in only those rows where the standard deviation is below 5 and with count greater than 100 (thresholds may be adjusted);
6. Finally, group every relevant attribute/field by URL, including the count of unique source hosts and start checking the output.

Required Data Sources:

Proxy Logs, Firewall Logs (optional)

Splunk Query:

```
index=proxy sourcetype=whatever url=*

| eval current_time=_time

| sort 0 + current_time

| streamstats global=f window=2 current=f last(current_time) AS
previous_time by src, url

| eval diff_time=current_time-previous_time
| eventstats count, stdev(diff_time) AS std by src, url

| where std<5 AND count>100


| stats count AS conn_count, dc(src) AS unique_sources,
values(http_method) AS methods, values(http_user_agent) AS agents,
values(std) AS diff_deviation, values(category) AS category by url
```

Chapter 8 MSSP outsourcing

By David Nathans

Most organizations think about outsourcing cybersecurity due to its high costs and lack of resources. Unless you are in the business of cybersecurity building your own SOC many not have a high return on investment. Larger organizations see cybersecurity as a cost avoidance (Saving money they would have to spend if they were breached) whereas smaller businesses see it as a cost of doing business (money they need to spend to stay in business) if they invest anything in cyber to begin with. Very different perspectives but the results are the same. Not everyone can have their own Security Operations Center (SOC).

Before you can really think about MSSP outsourcing you need to understand what an MSSP is and how different organizations use the acronym to describe themselves. Having a good understanding of how organizations are different, yet call themselves the same thing will help in getting closer to what you ultimately want in an outsourcing relationship.

In this chapter we are going to discuss and answer these questions:

- What is an MSSP?
- What is a Pure MSSP?
- What is an MSP?
- What to look for in an outsourcing relationship?
- Key questions not to ask?
- Setting expectations?
- Being a good partner?

What is an MSSP?

As defined by Gartner[1], a Managed Security Service Provider (MSSP) provides outsourced monitoring and management of security devices and systems. This definition goes on to say, “Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and antiviral services.”

This definition does not go far enough and could be considered outdated as there are many more types of services and cross-over offerings available today. Here is an attempt to provide a sample of examples opposed to an exhaustive list:

- Data loss prevention (DLP)
- Distributed Denial of Service prevention (DDOS)
- Managed Detection and Response (MDR)
- Endpoint Detection and Response (EDR)
- Managed Domain Name Service (DNS)
- Managed Security Incident and Event Management (SIEM)
- Threat Intelligence
- Managed Compliance

The key to any organization calling themselves an MSSP would be that their focus is providing services that the name squarely states. They are a provider who Manages Security, as a service. Long gone are the days where MSSP’s just provided managed firewall and Intrusion Detection (IDS). Today, a key differentiator of an MSSP is that they offer a wide range of security services backed by a 24/7 Security Operations Center.

Examples of MSSP’s are (Alphabetic order):

- AT&T - https://www.business.att.com/portfolios/cybersecurity.html
- Capgemini - https://www.capgemini.com/service/cybersecurity-services/
- IBM - https://www.ibm.com/security/services/managed-security-services
- Secureworks - https://www.secureworks.com/
- Symantec - https://www.symantec.com/services/cyber-security-services/managed-security-services

- Verizon - https://enterprise.verizon.com/resources/articles/managed-security-services/

Typically, MSSP's have been large businesses that provide a long list of services but have a Managed Security Service (MSS) offering as either part of their extended internal operations or as a separate business unit. This can be the lifeblood of large enterprise organizations who need outsourcing due to the size and volume of needs. Large organizations need to outsource to other large if not larger organizations to ensure that the provider can handle their workload and have the resources to be successful for long periods of time.

What is a Pure MSSP?

Over the last few years, a new breed of MSSP has begun to grow and address a much different market. The pure-play MSSP is an entire company whose primary and only focus is on offering security services. These new types of MSSP's also bring with them a new crop of service offerings that are boutique, focused, and address specialty markets. Entire security companies can be dedicated to the protection and security of the evolving landscape of Internet of Things (IoT), Internet of Medical Things (IoMT), or specialize in industries such as oil and gas to include Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. These organizations also bring with it, expertise in protecting small businesses, Government, cloud and more.

Examples of Pure MSSP's are (Alphabetic order):

- Dragos - https://dragos.com/
- MedSec – https://medsec.com/
- Red Canary - https://redcanary.com
- Rapid7 - https://www.rapid7.com
- SOCSoter – https://www.socsoter.com
- FireEye – https://www.fireeye.com

There has been no better time than now to find a company that specializes in security services who is as unique as the organizations with whom they are protecting. Not only can you now find Pure MSSP's who specialize in your industry but also bring with them products and services unique to business size and offer price points that make sense. MSSP's are also bringing new capabilities to market such as Managed Detection and Response (MDR). This is service that is typically provided by pure MSSPs and has a strong focus on threat intelligence, threat hunting, security monitoring, incident analysis, log analysis, and incident response through a SIEM or even a managed SIEM infrastructure. Using advanced security analytics on the network and endpoints to track user behavior, application behavior and mis-usage. MDR provides deeper detection by combining security analytics with machine learning and augmented or artificial intelligence compared to traditional MSSPs, who mostly rely on static rules and signatures. Endpoint Detection and Response (EDR) is another emerging yet game changing technology pure MSSPs have been leveraging. Threats are constantly changing, and anti-virus software is only able to stop some of the problems some of the time. New EDR offerings by MSSPs include the capability to perform searches of all endpoints in an organization or across all devices an MSSP manages leveraging threat intelligence to find known and unknown threats, isolate compromised devices and stop malicious activity instantly.

While relatively new in the way of MSSP offerings, MDR and EDR is proving to be valuable for organizations looking to increase their cyber defenses. If your organization is looking to improve its incident response and threat detection programs with a pro-active, hands on approach to cyberdefense, an MSSP offering MDR and EDR could be a great way to achieve these goals.

What is an MSP?

Over the last few years there has also been other changes in the technology business. Value Added Resellers (VAR) of technology products and services, technology resellers and IT break/fix companies, which traditionally operates on a transactional and short-term basis, have all struggled as computing platforms move to the cloud and end users become more technically proficient and self-supportive. The emergence of the Managed Service Provider (MSP) has evolved to become the entrusted lifeblood of businesses who rely on technology but cannot afford full time in-house staff to support the varied needs, or they can supplement full time in-house staff that are overwhelmed with their responsibilities. The MSP partners with their customers over annual, or multi-year periods. They can handle a number of technical and administrative duties such as help desk support, network and application management and ensuring that the systems are working seamlessly with as little (ideally NO!) downtime as possible.

These services typically have consisted of general IT administration, management, support and maintenance and patching of clients, servers, infrastructure and now of course, Cloud. As technology has evolved and hackers develop new methods of threat and intrusion, so has the breadth of what MSP's have to, and are expected to provide by their customers. This has caused a morphing and blending of traditional outsourced IT services into new areas of what would ordinarily come from a MSSP. Many MSSP's have partner and reseller programs that MSP's can subscribe to in order to leverage expertise in all areas of cybersecurity without having to have their own 24/7 SOC and internal expert staff. MSP's need to ensure their customers are safe and secure and depending upon the industry – adhering to strict compliance guidelines set by regulating bodies.

What to look for in an outsourcing relationship

The first thing you need to do before you begin outsourcing is to look in a mirror. You have a lot of choices out there and you can either shop for the best fit for your needs or be swayed by slick marketing and stories of how great one company over another. The best relationships are built on a firm ground of understanding what the business needs and what it is getting from the outsourced relationship. If those two things are not well understood, then the relationship is not going to work even with the best of intentions. A good outsourcing relationship is not about getting an advantageous contract or getting more for your money, but rather gaining a partnership that extends, enhances, and augments a business' ability to grow and benefit from that relationship. The MSSP partner you choose should be willing to protect your business as if it's their own and you should also be willing to make them a key member of your team.

How to test the relationship? The difference between selling and recommending is trust. If you trust your outsourcing partner and they make recommendations, then you do trust them.

If all you hear is them trying to sell you, then maybe you don't trust them nor have a good relationship.

Another thing you should look for in an MSSP relationship is innovation and enhancements and if those come free or at a charge. Did the MSSP build proprietary technology and do all their own inhouse development or are they just reselling other companies' products and services? In the case of a pure MSSP, cybersecurity is all they do. They live and breathe for cyber and should always be improving their capabilities. Of course, MSSP's need to make money but they should have clear pricing models and set clear expectations on what you get versus what is an extra charge.

Additionally, you need to see if the MSSP is going to be aligned with your needs not just from an offering perspective but also from a compliance perspective. If there are country requirements that don't allow you to outsource outside your own country, if data backups are going overseas. These and many more questions should be asked of an MSSP as you begin to build a relationship with them.

Key questions not to ask

The list of questions you can ask an MSSP are endless and there are many sites out there that have an exhaustive list of things that you can ask. Instead it is more fun and beneficial to explore questions that maybe you should not ask when looking for a new MSSP partner.

Contracting with a big-name player may be great. If you are a small fish then will you get the attention you deserve? Let's be real, you get what you pay for with the big guys. There is no doubt that they will do everything they can to service your contract and provide you the best, and you can be very happy with them. But let's be honest, if your only spend $1,000 and another company's spends $10 million, who is going to get more attention? Do you really need to ask this question?

Growth questions always seem to come up and never seem to make real sense at the time. Asking questions like "what's your staff growth rate?" is a waste of time for everyone unless you are specifically looking for a job. Growth of a company is a distractor to servicing a customer's account. An MSSP should do all they can to ensure that any growth does not upset their customer base. Besides, having a ton of employees and an impressive office means they have big bills and need you to help pay for them.

Asking why they think their technology is the best. Is this a game? MSSP marketing departments can drown you in whitepapers, marketing materials, social media and more. If you want to ask technical questions then go for it. Don't just ask questions to show off your technical wizardry or play "stump the chump." Make the questions meaningful because you are interested in how they address a real problem. You want to know how they are going to protect you, not how they are going to keep you entertained on twitter.

There are many more other questions you should probably not ask. Next time you get a blank stare, bewilderment or long pause, stop and ask yourself it that was a good question and if the answer really matters to establishing a good relationship with your MSSP.

Setting expectations

Previously we discussed looking in the mirror and understanding your needs before going out to look for an MSSP. That is never truer than when looking to set expectations. If you are not sure of what you want, then it will be impossible for any MSSP to make you happy. This does not mean you need to be the most technical person in the room, but you should know what is important to your company and what your company needs to protect. You should also clearly understand your challenges in providing cybersecurity services yourself. You need to know if it is cost issues, internal knowledge, resource or time problems that prevent you from doing it yourself. You not only need to know what is important from a cyber protection perspective but also understand and be able to communicate what they expected outcomes are. If you do not have the capability to run a full incident response and containment of a breach, then you need to ensure that your MSSP or even multiple MSSP's can and will offer it to you if you need it.

Setting expectations goes both ways. An MSSP should be willing to share with you their development roadmap. Knowing what you want out of your MSSP is great but if you are able to strengthen your cybersecurity along with the growth and development of new features and capabilities of your MSSP then it will be easier to plan, budget and ultimately meet company business objectives.

Lastly, every business is different and as such there are times when something custom will be needed. Knowing what services, you are going to be contracted for, it would be worthwhile to understand if there are any capabilities that could be customized. Not only can they be custom but also if there is a charge for any customization.

You need to understand where the MSSP services begin and end and your responsibilities begin and end.

Being a good partner?

The best relationships for MSSP and customers alike are ones where the customers are engaged and the MSSP is responsive. The customer needs to be responsive and willing to work collaboratively in cybersecurity efforts alongside the MSSP. This does not mean you have to have a dedicated resource but at least someone who has ultimate responsibility to be available to the MSSP when needed. It is always best to assign a dedicated resource to work with the MSSP that is not the CEO. It is not that the CEO is a bad person, but they have other stuff to do and may not be able to respond to issues or requests from the MSSP. Obviously, you will need to decide in your own organization who is the best for this role but don't skip assigning it, it could mean the difference between an incident and a breach.

Understanding what are the depth of services and capabilities that the MSSP has is critical for you to understand what they can do for you especially when it matters most. If all you get is a notification of a potential incident without the ability to question, engage or invoke full incident response services, then are you in an outsourced relationship or did you just buy a product. MSSP's and customers should have regular meetings and touchpoints to ensure that everything is working smoothly. This should be a time that is set aside regularly to review reports, plan new projects, discuss issues and provide feedback. Feedback is a critical component to being a good partner. If you are happy or not, letting your MSSP know will help them either continue doing what they are doing or make course changes to help resolve issues.

Summary

While there are certainly similarities and difference between an MSP, MSSP, and pure-play MSSP. It essentially boils down to the fact that MSP's do not offer their own security in their portfolio of services outside of infrastructure, Firewall, Patch, and anti-virus management unless they partner with an MSSP or a cybersecurity vendor. MSSP's offer focused cybersecurity offerings as part of a larger organization, and pure-play MSSP's only deal in cybersecurity and even sometimes provide specialized cyber services in specific focus areas.

Regardless of who you choose and why, in the end, you need to focus your decision and outsourcing efforts in achieving a few simple objectives. Find a partner that cares about you and is skilled in your size and type company. Minimize costs by leveraging security experts working for you at a fraction of the cost of having your own in-house team. Increase efficiency by allowing your outsourcer to apply proven procedures and policies into the management of your infrastructure that ultimately helps reduce false positives and improve responsiveness to detect and contain cyber-attacks. And lastly, your MSSP needs to enable you to focus on your business while they focus on protecting it.

References:

[1] Gartner https://www.gartner.com/it-glossary/mssp-managed-security-service-provider