Journal of Network and Information Security
10 (1) 2022, 29-36
http://www.publishingindia.com/jnis

Fill the Gap to Connect Dot, the Cyber Intelligence

Vinit Thakur
SME - Information & Cyber Security, Barclays Investment Bank, United States of America.
Email: vcthakur@gmail.com

Abstract: As we all are aware of from the recent headlines, hackers routinely steal intellectual property, privileged information, financial data, social security numbers, email addresses - which they sell on the black market for obscene profits and not the last but least costly ransomware attack. In 2020, more than 550 security breaches were reported to the U.S. Privacy Rights Clearinghouse, and 1.1 billion individual records were compromised or stolen since 2005 [1]. Regardless of their industry vertical or scale most organizations are vulnerable to cyber attacks, and yet continue to gamble with their reputations because they aren't taking cyber security seriously. It's just a matter of time before they join the countless other firms who've suffered embarrassing and costly privacy & security breaches due to weak process or lack of visibility. Because cyber threats and vulnerabilities constantly evolve; many organizations may not be as effective at managing the associated risk as they might be in managing risk in other areas of the business. Cyber threats are on the rise and growing exponentially in complexity; at the same time, the economy is forcing organizations to drive down their operational costs while still maintaining an aggressive, productive and agile business model.

Keywords: Cyber security, DDOS attack, Incident response, Security awareness, Threat management.

I. Executive Summary

Many InfoSec research says "Cyber Security Technologies" are very good at detecting known threats so that security professionals can react. However, an evolving concept, known as "Cyber Intelligent", involves using a combination of "People, Process and Technologies" to detect both known and unknown threats, helping security professionals become more proactive.

Cyber Intelligent harnesses the power of big data; analytics; security information event management, or SIEM; and other tools to more quickly identify anomalies that could be early signs of bad behavior or immediate threats.

II. Filling Gaps

Cyber Intelligent targets to close a gap by improving real-time visibility into network security threats. Many of SMB's security officers says, we've become good at catching spam, viruses, malware, worms and botnet and there's been an explosion of technology used in firewalls, proxy, spam filter, IDS/IPS, etc. And they are good at catching attacks on a network, cloud and virtual network. However, all those things put together only get us 95 percent there. The bad guys are getting in [by taking advantage of] the other 5 percent.

How to fill rest 5 percent gap; need to understand these threats work and identifying their patterns is important to mitigate them. That requires the use of people, process and technologies that help detect malware and hacking based less on signature and more on anomalies and behavior of the attackers.

"We're all trying to be smarter, "There is more layering of cyber security and more layers for discovery."

But more layers of technology don't always mean better security. "We can layer different security, but the problem is that each layer doesn't talk to the others, "That's where big data analytics help."

SMB's security officers integrating or layering a variety of technologies to look for anomalies in data from multiple sources that help connect the dots to identify security threats, however they are struggling to fill the 5 percent gap.

Organization research team should work closely with their partner Technology Company to fill the 5 percent gap using technology that record the network big data, analyze them on fly, make it visible, alert on behavioral anomalies and available for forensics.

III. Information and Cyber Security and Business Need to Work Together!

The Cyber Intelligence group needs to understand business process, procedure and IT requirement, to identify known and

unknown threat. This can be achieved, when organization have proper "People, Process and Technology" to understand business needs and cyber security tripod "CIA", Organization should have well defined process to identify business information and have proper labeling of the data and should have proper NVA (Network Vulnerability Assessment) program in place. Information Labeling and/or NVA provide business and IT details to organization SOC team to configure the monitoring device for anomaly detection as well eliminate false positive alert.

Organization SOC engineers should get periodically training and strict to follow defined process to catch all threats and anomaly behavior in network and same time to avoid sending false positive alert to business or IT team.

Organization can utilize industry standard technology to detect known as well unknown threat. However, before organization can reach to this level, organization should follow following steps [2].

1. Holistic Information and Cyber Security Risk Assessment

Information & Cyber Security Risk Assessment service should be designed to:

- Identify and prioritize cyber security risks based on legal, compliance, and regulatory requirements,
- Specify reasonable and appropriate managerial, operational, and technical security controls,
- Plan methods for implementing, managing, and tracking the efficacy of security controls, and
- Establish tracking and reporting on the actions taken to eliminate or reduce security risk.

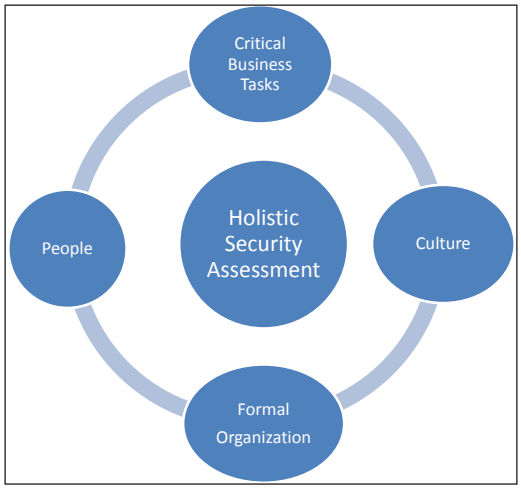

Fig. 1

Value: Results in a flexible information & cyber security program that can be used to gain visibility into the current security posture of an organization. The output from the assessment can be used to assist senior leadership/executives to facilitate informed decisions on how best to protect organizational data in the least disruptive manner. Serves as: Proof of "Due Diligence" for auditors, and can be leveraged as a roadmap for selecting cost effective security controls at are aligned to the strategy and culture of the organization [3].

2. Network Vulnerability Assessment (NVA) [4]

- Organization NVA should be designed to provide a comprehensive identification, analysis, and corrective action planning of networks, servers, and operating systems. The NVA should identify security flaws, missing patches, and poor configuration.
- Organization should perform the NVA from both an external and internal perspective. Security engineers or specialized consultant should leverage well-respected vulnerability data sources for network vulnerability assessment. The classification of vulnerabilities should be based on the Common Vulnerability and Exposure (CVE) database which is used today as an international standard for vulnerability numbering and identification.
- Organization should use research and analytic methods to normalize organizational threats with the identified vulnerability in order to communicate the actual organizational risk of the findings. NVA produces should be granular and comprehensive (meaningful) report that documents the security posture of devices connected to the network. It should be performed by certified ethical hacker, so they can verify and validate the identified vulnerabilities using various manually methodologies and technical toolsets. Vulnerability/Risk assessment modules should include:
  - Social Engineering,
  - Wireless security assessment, and
  - Web application (OWASP) top 10 Assessment.

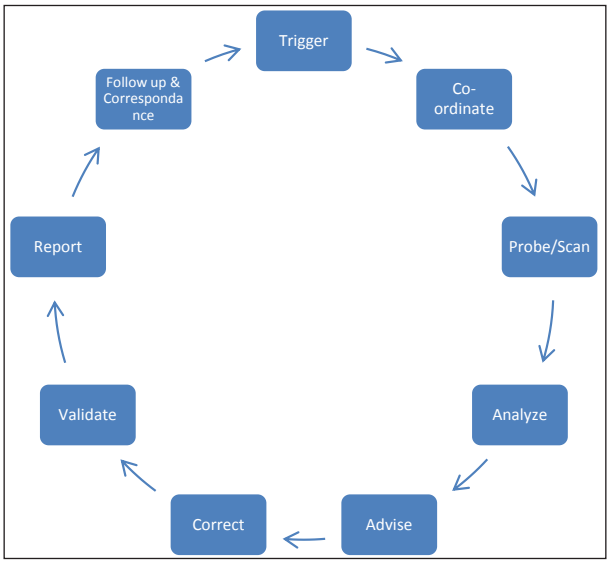

Fig. 2

Value: Performing an NVA is a proactive approach towards security that allows an organization to examine the current status of system security. A comprehensive review and analysis can be valuable because it enables the organization to identify and address security issues before a hacker has a chance to wreak havoc on the organization's digital assets [5].

3. Cyber Security Policy Development

- Review and identify gaps in existing policy, and develop the necessary documentation to address those gaps in a manner that meets regulatory, compliance and business obligations.
- Develop security policy, standards, and guidelines addressing the following specific cyber security domain areas:
  - Security Policy (Policy on Policy)
  - Information Security Management Program
  - Access Control
  - Human Resource Security
  - Risk Management
  - Compliance
  - Asset Management
  - Physical and Environmental Security
  - Communications and Operations Management
  - Information Systems Acquisition, Development and Maintenance
  - Cyber Security Incident Management and Response
  - Business Continuity Management

Information & cyber security policy shall address the operational, managerial, and technical security controls necessary to preserve the Confidentiality, Availability and Integrity of the organization information assets. These controls are further defined below:

- *Operational Security Controls:* Focuses on controls that are implemented and executed by people. These controls are put into place to improve security of a particular system. They often require specialized or technical expertise and rely on management and technical controls.
- *Managerial Security Controls:* Focuses on the management of the computer security program and the management of risk within the Sands.
- *Technical Security Controls:* Focuses on security controls that the computer system executes. The implementation of technical security controls requires operational consideration. They shall be consistent with the management of security throughout the Sands.

Value: Cyber security policy is the foundation to and organization's Cyber Security Governance program. Establishing a sound policy framework and ensuring it is maintained and communicated across the organization fulfils many purposes. Formal written policies are:

- The foundation for protecting people, IT assets, and information, and
- Setting the rules for expected behavior by users, system administrators, management, and security personnel. They authorize security personnel to monitor, probe, investigate, define and authorize consequence of violation. Security policies are essential to defining management's baseline stance on security; minimize cyber risk, and tracking compliance with regulations and legislation.

4. Security Awareness Training and Education (SATE)

Organization should have internal talent or through partnerships, organization should provide various types of Cyber Security Awareness Training and Education to all the employees. Development of security awareness programs should be customized to the organization needs. The awareness program should include security practitioner training, employee ad workforce's awareness, and focused security training for IT professionals. These training sessions should conduct via classroom setting, workshops, posters and flyers, and/or Software as a Service via customer web portals.

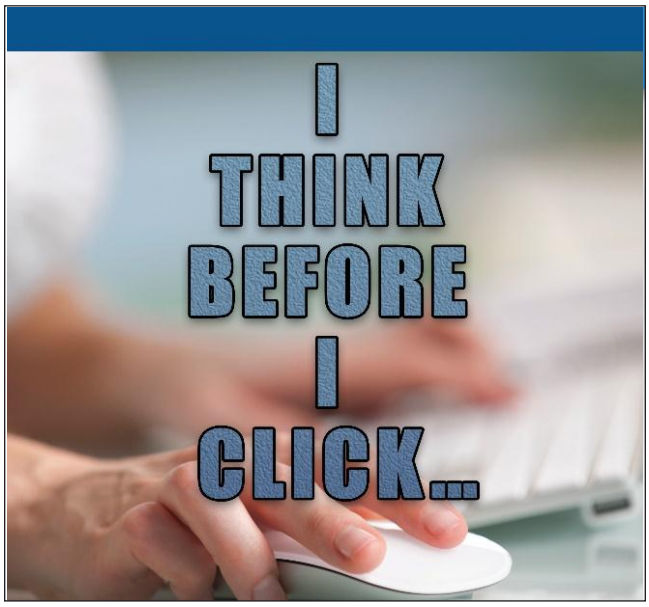

Fig. 3

Fig. 4

Value: Regardless of what type of security controls organizations put into place they can potential be circumvented by what has been referred to as the "weakest link" – people. In fact; one of the first steps for cybercriminal is to exploit people via social engineering techniques designed to gather information that allow them to escalate their attack and bypass other controls.

All employees should understand he underlying significance of security and the specific security requirements expected of them. With a sound cyber security awareness training and education program organizations can empower employees through knowledge; this helps to prevent the end user from making unintentional mistakes and being fooled by cybercriminals with mal-intent ultimately awareness results in reducing the likelihood of an organization experiencing a breach of corporate & client data.

5. Network Security Profiling [6]

A network profile should be the first activity conducted by organization information & cyber security team. The network profile activity can last for as long as 4-6 weeks depending on the size of the network segment(s). The main idea behind the network profile should be to establish a baseline of what is considered to be normal traffic flow for the environment. SOC team analyst cannot determine what "abnormal" or "unknown activity" on the network segment until they understand what should be considered to be "Normal" traffic. A network profile is an inventory of all the assets on the network segment and their associated purpose including the traffic flows associated with those devices.

The profile consists of analysis of traffic over ports, protocols, and other network flow data available at the perimeter gateways. This can be a very interactive process between SOC and the organization various business team and can be considered to be a discovery process, at the end of the exercise SOC team should produce a baseline for what is considered to be Normal traffic that includes identified outliers.

The Network Profile steps include:

- Gather available network information,
- Selection of an initial data set,
- Identification of the active address space,
- Catalog of common services,
- Catalog of other services,
- Catalog of leftover assets, and
- Documentation and report of findings.

Value: Visibility and understanding of one's own network environment is paramount in performing predicative analysis; as well as, the identification and timely response to security events of interest and incidents. The insight gained can be used to assist them in making informed decisions about how to address actual anomalous activities currently occurring on their network.

6. Network Security Monitoring (NSM) [7]

Organization Network Security Monitoring should occur around the clock and augments all the existing intrusion detection/ prevention capabilities the organization may already have in place. NSM should consist of products, people, and process necessary to provide indicators, alerts, and warning of security events of interest occurring on the organization's network in near real time. The NSM department should be designed to utilize the baseline network profile to perform both predictive and after- the- fact identification of cyber attacks. Organization can use the various technology tools or appliance are available in market, as well as certified and experience security analyst to provide this service.

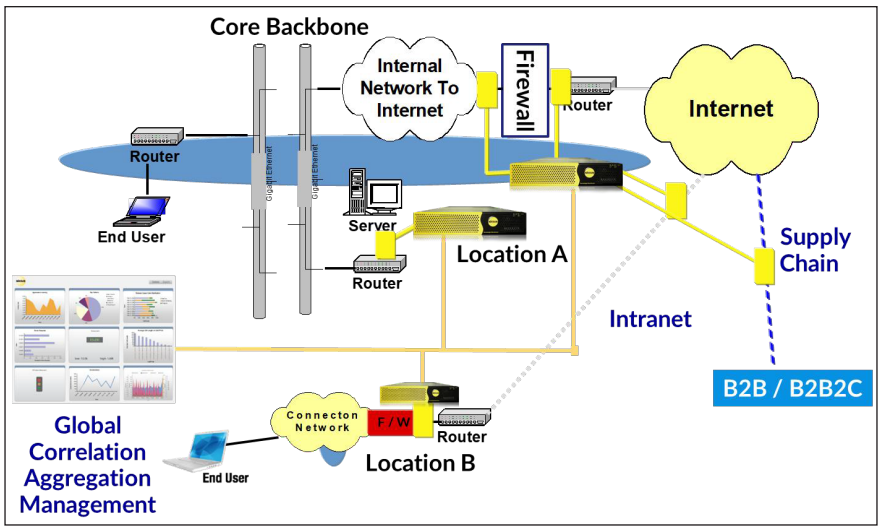

Fig. 5 [10]

Value: Organized cybercrime and insider threats are changing the security threat landscape across all industries. Proactive security monitoring provides a logical offensive and defensive approach. When an organization becomes aware and better understands the strengths and weaknesses of their own network; they are in a better position to prepare, defend and respond to an attack. Cyber attackers will constantly change their tactics. Knowing what to address based on impact to critical assets also helps an organization to make better spending decisions; as well as, realize better return on investment (ROI) on future security spending.

7. Cyber Security Incident Management and Response Planning [8]

Defending against cyber threat requires extensive planning and sustainable processes, and skilled individuals. Organization Cyber Security Incident Management and Response Planning team should focus on working with the business's key stakeholders to develop and document a formal incident response planning document. The document will include roles, responsibilities, and activities necessary to prevent, detect, and respond to a cyber security incident. The customized security incident plan will consist of the following sections:

- Preparation,
- Detection and Analysis,
- Containment, Eradication,
- Recovery, and
- Post Incident Activities.

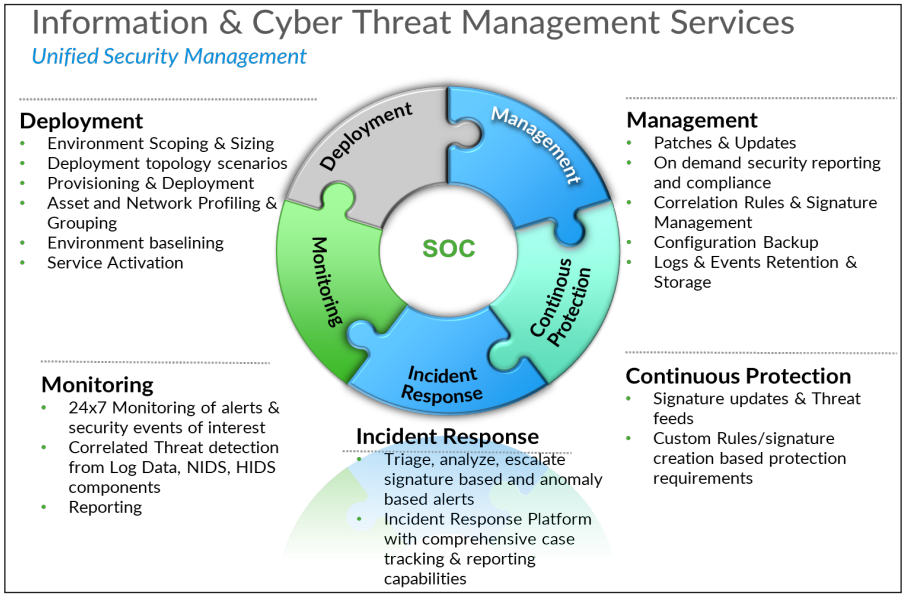

Fig. 6

TABLE I

Category	Description	Type
Unauthorized Access	Gains logical or physical access without permission to network, system, application, data, or other resource	Security Incident
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Security Incident
Malicious Code	Detection of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application.	Security Incident
Improper Usage	A person violates acceptable computing use policies.	Security Event
Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Security Event
Anomalies	Deviation from baselines.	Security Event

Value: Cyber attacks are a cost of doing business on the Internet. Organizations must put themselves in the position to reduce the impact that these attacks have on digital assets. By putting a well-structured cyber incident plan in place organizations can reduce the impact these attacks can have on confidentiality, availability, and integrity of the data entrusted to them. By reducing the time, it takes to detect and respond to incidents. Organizations are able reduce their risk of exposure. By developing and implementing a plan that has been thoroughly designed and tested organizations will be better prepared when the inevitable occurs.

Organization SOC engineers should follow the layered approach to figure out unknown threat using above outlined Policy, Procedure, People and Technology device and help business without false positive alert.

The Threat can be:

- DOS/DDOS (Denial-of-Service/Distributed Denial-of-Service)
- IP Address Spoofing
- Broadcast Amplification
- Host/Port Scan
- ARP, ICMP and unknown protocol, etc.

IV. To Know More About How? Here is One Test Cases

Distributed Denial-of-Service (DDoS) attacks are all too common reality in today's Internet landscape and are an escalating global problem. Whether a DDoS attack is motivated by criminal intent, like cyber extortion, or is executed as an extreme form of free expression, the resulting service interruptions can have wide-ranging effects.

A Denial-of-Service attack is a computer-based attack whose intention is to make the attacked resource unavailable. The SYN Flood Attack is an attack that falls into the Denial-of-Service category.

To gain a better understanding of the SYN Flood attack, we must first cover the basics of Transmission Control Protocol (TCP). TCP is a connection-oriented protocol that rides over IP. It's reliable in the fact that receiving host has to acknowledge the receipt of the sender's packet. If a packet is dropped in transit, then the receiver will not provide a receipt known as an Acknowledgment or "SYN-ACK" back to the sending or transmitting host and the sender will resend the dropped packet. This sending and acknowledgment mechanism is called the TCP 3-way handshake [9].

Below is an example of a typical initial TCP communication flow.

- Host A *sends* a TCP *SYN*chronize packet to Host B
- Host B receives Host A's *SYN*
- Host B *sends* a *SYN*chronize-*ACK*nowledgement
- Host A receives Host B's *SYN-ACK*
- Host A *sends ACK*nowledge
- Host B receives *ACK*.

Host-A --- *SYN*--->Host-B

Host-A <--- *SYN-ACK*--- Host-B

Host-A --- *ACK*---> Host-B

TCP socket connection is ESTABLISHED.

Firewalls, routers, servers, and other computer-based systems have a theoretical maximum number of connections or sessions they can handle. Each is different based on the make and model of the specific piece of hardware. Simply put a web-server may only be able to establish and maintain 100,000 concurrent sessions before it starts dropping traffic.

The SYN Flood attack is works by an attacker sending a continuous and rapid succession of *SYN* packets to the remote host. Following the TCP model, the host replies back with a *SYN-ACK* and waits for the returning *ACK*. To the receiving host this connection is open, so deduct 1 connection from the 100,000 connections it's capable of supporting. The attacker doesn't just send out one SYN packet, remember he sends a continuous and rapid succession of SYN packets. So, the attacker sends out as many SYN packets as fast as it can until the host can't accept anymore and the service, in this case a website, is rendered unavailable. Hence the term "Denial-of-Service".

You many often hear the term Distributed Denial-of-Service (DDoS). The DDoS version of the SYN Flood attack works the same way except the attack is initiated from a multitude of different systems that are focused on one target.

Denial-of-Service floods and reconnaissance activities are two examples of traffic that may not make it through the firewall, but that could provide an early warning of an impending attack or details for effectively responding to an attack.

V. How do You Know if an Attack is Happening?

Not all disruptions to service are the result of a Denial-of-Service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the following symptoms *could* indicate a DoS or DDoS attack:

- Unusually slow network performance (opening files or accessing websites).
- Unavailability of a particular website.
- Inability to access any website.
- Dramatic increase in the amount of spam you receive in your account.

VI. What do You do if You Think You are Experiencing an Attack?

Even if you do correctly identify a DoS or DDoS attack, it is unlikely that you will be able to determine the actual target or source of the attack. Contact the appropriate technical professionals for assistance.

- If you notice that you cannot access your own files or reach any external websites from your work computer, contact your network administrators. This may indicate that your computer or your organization's network is being attacked.
- If you are having a similar experience on your home computer, consider contacting your internet service provider (ISP). If there is a problem, the ISP might be able to advise you of an appropriate course of action.

VII. Conclusion

In effective solution, Organization can believe in "People, Process and Technology". DoS/DDoS attacks is reality of every business and same time your computer can be compromised to victim of the attack and behave as zombie. Today's attacks are sophisticated, it is critical for every business to monitor the network traffic patterns and behavior for baseline the anomaly configuration continuously. Every business needs to detect DoS attack before business or reputation damaged. That being said, attacks are continually getting better and smarter every day and so must the network administrators as well. The best defense to any attack is knowledge. So, network administrators must keep up with the latest technology and practices to help protect company's systems and their jobs.

References

[1] R. A. Clarke, *Cyber War: The Next Threat to the National Security*. ISBN: 978-0-06-196224-0. [Online]. Available: https://privacyrights.org/

[2] NISTIR 8286 - Enterprise Risk Management paper. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8286/final

[3] Transformation Cyber Security - Digital McKinsey and Global Risk Practice, Mar. 2019, p. 56. [Online]. Available: https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

[4] P. Foreman, *Vulnerability Management*. ISBN: 1439801509. pp. 103-125. [Online]. Available: https://csrc.nist.gov/glossary/term/vulnerability_management

[5] ISC2, Cyberedge Group - 2022 Cyberthreat Defense Report.

[6] C. McNab, *Network Security Assessment*, 3rd ed. ISBN: 9781491910955. O'Reilly Media, Inc., pp. 92-110.

[7] J. R. Vacca, *Network and Security System*. ISBN: 978-0-12-416689-9. Steven Elliot, pp. 21-73.

[8] https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide

[9] https://www.inetdaemon.com/tutorials/internet/tcp/3-way_handshake.shtml

[10] NIKSUN NetVCR & NetOmni datasheet.