INCIDENT RESPONSE FRAMEWORK IMPORTANCE :

An incident response framework is essential because it gives organizations access to better response strategies. Large firms with extensive research and security experience frequently create these frameworks. Two of the most well-known examples of incident response frameworks developed by system administrators and the National Institute of Standards and Technology (NIST) These frequently consist of audit, network, and security organizations (SANS). Organizations need incident response frameworks because they offer a standardized, dependable, and systematic method of responding to and managing security incidents. The whole incident response process, from the initial identification of an incident to the post-incident evaluation and analysis, is thoroughly outlined in incident response frameworks. They also act as a reference manual for incident response teams, assisting them in making quick decisions regarding the appropriate course of action to take in certain scenarios. In order to ensure that everyone is taking the same actions and pursuing the same objectives, the frameworks also assist businesses in developing a shared understanding of how to respond to crises. Last but not least, incident response frameworks assist businesses in ensuring that all security issues are properly addressed and that any possible repercussions are minimized.

NIST INCIDENT RESPONSE FRAMEWORK :

The incident response cycle is defined by the NIST framework as a four-step process, not a linear one that begins with the detection of an incident. When eradication and recovery are involved, this is over. In contrast, incident response is a constant process of learning and improvement to figure out how to better protect the organization from these cyberattacks.

The cycle involves 4 steps :

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-incident activity

PREPARATION :

The NIST Framework's preparation stage is intended to lay the framework for organizations to participate in the next stages. This stage focuses on creating a cybersecurity strategy, conducting a risk analysis, and getting the organization ready to put the strategies into practice. In order to establish a comprehension of the current environment, the preparation stage entails obtaining information on the organization's current structure, resources, and risk profile. It also entails the creation of a risk assessment plan that details the procedures to follow in order to identify and evaluate risks as well as the methods to mitigate them.

DETECTION AND ANALYSIS :

An essential component of the whole security procedure is the NIST Framework's detection and analysis stage. Finding possible security events and evaluating them are the main goals of this stage in order to comprehend the context and source of the threat. Various technologies and techniques are used at this step to detect, gather, analyze, and relate the data in order to spot any harmful behavior. It is crucial to remember that this step should be repeated regularly to ensure the optimum security posture. Additionally, this level helps firms to quickly and effectively detect, comprehend, and respond to risks.

Containment, Eradication, and Recovery:

The NIST Cybersecurity Framework stages of containment, eradication, and recovery give businesses a process to react to a cybersecurity issue. To stop more damage and/or data exfiltration, the compromised systems and networks must be identified and isolated during the containment stage. Organizations must find the incident's underlying cause and get rid of the threat actors during the eradication stage. Organizations must restore systems and services to regular functioning and record any lessons learned during the recovery stage. The NIST Cybersecurity Framework gives businesses the direction they need to stop, find, contain, and handle cybersecurity issues.

Post-incident activity:

The NIST Framework's Post Incident Activity stage is the last level of implementation. In this phase, the emphasis is on drawing lessons from the experience that can be used to avoid repeating the same mistakes. It entails processes like incident reporting and evaluation, root cause analysis, and corrective planning. To guarantee that future events are kept to a minimum, this stage also involves creating metrics for gauging incident response and putting in place a plan for ongoing improvement. This phase also includes developing communication strategies to make sure that all parties are informed and kept up to speed on the incident and its solution.

SANS INCIDENT RESPONSE FRAMEWORK:

An open-source front-end framework called Sans Framework was created in CSS, HTML, and JavaScript. It was developed to cut down on the time and quantity of code needed to create a contemporary web application. Sans Framework gives programmers access to a collection of

pre-made elements, styles, and layouts that can be combined to produce a unified user experience. Responsive design is also supported by the Sans Framework, enabling developers to create apps that look fantastic on any device. The SANS framework consists of :

1. PREPARATION
2. IDENTIFICATION
3. CONTAINMENT
4. RECOVERY
5. LESSONS LEARNED

Preparation:

The SANS Framework's preparation phase is a crucial step in the security review process. The security assessor will define the scope of the evaluation at this point, design a threat model, and establish an assessment schedule. The security assessor will also create a thorough outline of the assessment's goals and prerequisites. Additionally, at this phase, pertinent data about the system, including configuration parameters, hardware and software characteristics, and user data, must be gathered.

Identification:

The SANS framework's Identification stage is a crucial element in the security management process. The assets, weaknesses, threats, and remedies that will be employed to safeguard the system must be identified. It involves creating a security policy that defines the system's security requirements. In this phase, the users who will have access to the network are also identified, along with their functions and duties. The evaluation of the system's present security stance and

the detection of prospective threats and vulnerabilities are also included in the identification stage. The identification step also involves developing a strategy for putting security measures in place and keeping track of them.

3. Containment:

The SANS Framework's containment stage is the key to minimizing and avoiding cyber security problems. This important phase aims to confine the event and lessen the damage it causes to the organization's data and systems. The organization will determine the attack's origin at this phase, look into the occurrence, make efforts to isolate the origin, and implement the proper countermeasures.

4. Recovery:

The SANS Framework's Recovery stage is intended to aid businesses in recovering from security incidents as soon and effectively as feasible. This stage's objectives are to fix the organization's systems and procedures and stop similar incidents from happening in the future. Finding the incident's primary cause and creating an incident response plan are the first steps in the recovery stage. This strategy should include actions that will lessen the impact of the incident on the firm, like reinstating data backups and networks and putting new security measures in place.

5. Lessons Learned:

Security experts and companies can evaluate their security posture with the help of the SANS framework. It offers a thorough framework for assessing and enhancing an organization's security posture. Businesses may find and fix security posture weaknesses by using the lessons

learned from the SANS framework. The framework is useful for identifying possible threats, setting priorities for actions and expenditures, and recommending security best practices.

Determine which framework you recommend the most and why.

The demands of any organization ultimately determine which of the SANS and NIST frameworks is the best. For enterprises that require a framework that is more concentrated on cyber security, SANS is a solid option, whereas NIST is a better option for those that require a broader, more comprehensive framework. Organizations with more sophisticated security infrastructure frequently use SANS since it has a more complete set of rules and best practices for cyber security. On the other hand, NIST is more appropriate for companies that must prioritize adherence and have a basic security architecture. In the end, enterprises must evaluate their unique security requirements and choose the framework that best satisfies them.

The SANS security framework is preferred by organizations above the NIST framework because it provides the most thorough and in-depth method for managing information security. The SANS framework is made up of a collection of security procedures and controls that may be modified and customized to meet the particular security needs of any organization. Along with a variety of security tools, the SANS framework also provides audit and risk and compliance training, and incident response planning. The SANS framework includes more instructions on how to establish security controls and procedures and is intended to be more thorough than the NIST framework. The SANS framework is additionally more adaptable and adjustable, enabling enterprises to better adapt their security standards to their particular circumstances.

Discuss which metrics are most important to collect/dashboard and why.

Any security framework, such as the SANS Framework, must have metrics. This is so that businesses may evaluate their security posture, gauge the efficiency of their security controls, and monitor the advancement of their security efforts. Metrics are useful for giving organizations a way to develop goals and objectives that are based on numerical data.

Organizations can utilize a number of metrics from the SANS Framework to assess the efficacy of their security posture. The following metrics are among them:

Security Maturity Level: Regarding the security controls put in place and the level of risk accepted, this metric assesses the organization's level of security maturity.

• Security Effectiveness: This indicator assesses how well security procedures, processes, and controls work to stop, identify, and address security issues.

• Security Compliance: This indicator assesses how well the organization adheres to security rules and guidelines.

• Security Performance: This indicator assesses how well security operations and procedures are performing.

• Security Risk: Based on the firm's security posture and prospective threats, this metric assesses the risk level of the organization.

• Security Awareness: The success of the organization's security awareness training initiatives is measured by this indicator.

REFERENCES:

Understanding Incident Response Frameworks - NIST & SANS

https://www.stickmancyber.com/cybersecurity-blog/incident-response-frameworks-nist-sans#:~:text=The%20purpose%20of%20an%20Incident,of%20security%20expertise%20and%20experience.

Building an incident response framework for your enterprise

https://www.techtarget.com/searchsecurity/tip/Incident-response-frameworks-for-enterprise-security-teams