An Excerpt From (**Why is NIST SP 800-61r2 relevant in Security Operations Center).**

Dr. Yawo Kondo

Incident response significantly decreases the likelihood of hackers and intruders penetrating an organization's data system and causing damage by stealing or corrupting the data. Essentially, an incident response ability rapidly helps in incident detection, cushioning against loss and destruction, restoring information technology services, and redressing the weaknesses exploited. The NIST Special Publication 800-61 Revision 2 covers systematic and structured processes that organizations must adhere to when identifying and effectively dealing with incident response. In particular, this framework emphasizes the need for organizations to establish a computer-security incident response capability and ways to handle an incident.

Cyberattack happens in various forms and typologies, including phishing emails. Enhancing the internal incident response capability requires a deeper understanding of the numerous types of phishing emails and the red alerts to keep tabs on at all times. Therefore, the organization must incorporate security operations center analysts whose roles entail detecting and evading incidents in their jurisdiction. The reality in the cyber world is that criminals continuously lure internet users with numerous social engineering tactics. For example, employees may innocently open emails and email attachments disguised as legitimate, etc. Readiness in incident response capability would imply knowledge of methods for detecting and analyzing the underlying security threats.

When it comes to incident response, the primary consideration for the organization is detecting and analyzing given security incidents. Based on this fact, the organization has to explore two methods for detecting and evaluating security incidents, including statics and dynamics analysis. The analysis approach would differ based on the nature of the attacks. For example, when faced with phishing attacks from email, fake websites, link manipulation, CEO Fraud, session Hijacking, content injection, and malware, the static analysis would be the ideal approach to apply when detecting the incident. This signature-based analysis approach is significant because it allows the respondent to scrutinize the code while avoiding executing them to determine if the code is malicious without any noise. The analysis style utilizes many tools and techniques, among them Virus total, Hybrid Analysis, Jotti virus scanner, Any Run, IPvoid, Bright Cloud, or Abused IP for file fingerprinting. The main advantage of this analysis approach is its ability to detect a unique malware program in a hash.

The dynamic analysis approach differs from the static analysis because it adopts the behavior-based analysis. As we all know, executing malware is dangerous, especially if the execution takes place within the network. Instead, such analysis is preferable if done in a closely monitored environment such as sandbox. With this awareness in mind, the dynamic analysis style proves effective as it facilitates a designated environment or a controlled environment that is not only isolated and safe but also observable. The analyst investigates different resources within the environment, such as registry keys, IP addresses, domain name, etc. During incident analysis, the analyst applies numerous tools, including Netsat, T-shark, Netcat, Nmap, Splunk, Wireshark etc..for files integrity check, behavior or open ports.

Given the critical essence of policy in incident response, it is advisable that its structuring and wording encompass the commitment statement by the organization’s management. The management's willpower to tackle cyber incidences sets the tone for the rest of the individuals in the organization on matters cybersecurity. In other words, the extent to which the management expresses commitment to tackling cyber incidents implores the rest of the workforce to equally commit to tackling the menace. Apart from the management's willpower, the policy statement must enumerate the objectives and aims of the incident response plan, clarify the scope, and define the security incidents. The policy statement must also describe the responsibilities and roles in the organization, identify priority areas concerning incident response, indicate the performance standards and reporting mechanism for the entire team…