NIST Continuous Monitoring

1. **Benefits**
    a. **Enhanced security posture**:
        i. Continuous monitoring provides a dynamic view of an organization's security state. This then helps the organization immediately identify potential problems early on, before they escalate into major issues, enabling timely intervention and mitigation strategies. This also shifts an organization's security mindset from being reactive to proactive when dealing with information security. Lastly, periodic checks of systems and networks can miss patterns and trends that then impair strategic decision-making.
    b. **Informed decision-making**:
        i. Real-time data on security risks enable better decision-making regarding resource allocation and security controls. This is important because organizations can focus their resources where they are most needed. Continuous monitoring provides a comprehensive view of operations, enabling data-backed decision-making rather than relying on intuition. Lastly, this can be helpful to increase response times to evolving threats that emerge.
    c. **Compliance and accountability**:
        i. ISCM helps organizations meet regulatory requirements and maintain accountability with documented evidence of security activities. Many continuous monitoring tools can generate reports that specifically map to

regulatory requirements. Therefore, this makes it easier to demonstrate compliance to relevant authorities. Lastly, continuous monitoring allows organizations to stay updated on evolving threats and adjust their security controls accordingly, ensuring ongoing compliance with dynamic regulatory landscapes.

2. **Challenges**
    a. **Complexity of systems**:
        i. IT environments often consist of diverse and sometimes incompatible systems. Ensuring a uniform integration and coordination of continuous monitoring tools with these existing IT infrastructure and risk management practices is crucial for continuous monitoring. Not only is it a crucial step for continuous monitoring, but it can also create a major challenge for IT teams. This is because effectively analyzing and responding to alerts often demands specialized skills in data analysis, security practices, and understanding of the monitored systems.
    b. **Data overload**:
        i. The vast amount of data that is generated by continuous monitoring can be overwhelming and difficult to analyze effectively. This is because large datasets make identifying relevant patterns or anomalies challenging. Therefore, this often leads to missed critical insights due to the sheer amount of information that is being produced. It can also lead to decision fatigue by analysts as trying to interpret too much data at once can lead to

analysis paralysis, where decision-makers become overwhelmed and struggle to make informed choices.

c. **Privacy concerns**:

   i. It is challenging to balance security needs with privacy expectations. Continuous monitoring can create data privacy issues. This is because it involves constantly collecting and analyzing large amounts of personal data that is collected and analyzed. Therefore, this can lead to concerns about over-surveillance, unauthorized access, and the potential for misuse of sensitive information. Additionally, if users are not adequately informed about how their data is being collected, analyzed, and used, it can lead to privacy concerns and a lack of trust in the organization.

3. **Mitigation Strategies**

   a. **Complexity of systems:**

      i. Some mitigation strategies to address the complexity of continuous monitoring is to select monitoring solutions that are well-suited to your specific IT infrastructure. Additionally, resources should be allocated for training IT staff to enhance their knowledge of monitoring tools and data analysis techniques.

   b. **Data overload**

      i. Some mitigation strategies to address the concern of data overload is to use data filtering and prioritization. This means utilizing advanced analytics and machine learning to identify relevant data and prioritize critical alerts. Additionally, the organization can implement data

aggregation which means that they use tools that can consolidate and summarize data into meaningful insights to reduce information overload on its analysts.

c. Privacy concerns

i. Some mitigation strategies to address data privacy is to implement data minimization policy to only collect data necessary for its intended purpose. Additionally, the organization can obtain user consent prior to collecting and utilizing sensitive personal data. Lastly, the organization can clearly communicate its data collection practices, usages, and retention policies to users to address these concerns.

References

- CrowdStrike. (2022). What is continuous monitoring? Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/continuous-monitoring/
- Marcum LLP. (2023). Best practices for cybersecurity compliance monitoring. Retrieved from https://www.marcumllp.com/insights/best-practices-for-cybersecurity-compliance-monitoring
- National Center for Biotechnology Information. (2017). Privacy issues in big data monitoring. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC5478039/
- PurpleSec. (2024). Why continuous security monitoring is a requirement in 2024. Retrieved from https://purplesec.us/learn/continuous-security-monitoring/
- Secureframe. (2024). Monitoring & how automation can maximize impact. Retrieved from https://secureframe.com/blog/continuous-monitoring-cybersecurity