SECURING MONITORING AND EVALUATING DATA

GROUP 5

LEVEL: HND 2

DEPARTMENT: CYBER SECURITY TECHNOLOGY

COURSE: CRYPTOGRAPHIC APPLICATION

GROUP 5

1. ILUORE DAVID OSHOKE
2. EJIYI EMMANUEL
3. OKOJIE EBEAGBOR KENNETH
4. MUSAH IBRAHIM
5. ALIYU SADIA
6. ABDULLAH MUHAMMED SEGIRU
7. OSARIEMEN RAYMOND ODION
8. TIJANI FATIMA
9. OLALERE FAVOUR AKIN
10. OBEASO-IGECHI IKHADE STEVEN
11. AWHINAWHI PRAISE EJIRO
12. IFEDAYO TOLUWALOPE MOYINOLUWA
13. OSAYOMWANBOR OSADEBAMWEN DESMOND
14. ODIOR EMMANUEL OGHENAOGWE
15. OMONZEJELE TRUST OMONIGHO
16. ENOMWENGHO DESTINY OSAZUWA
17. OMORUYI BENJAMIN OSALUMESE
18. JOEL ELIZABETH
19. JAMGBADI SUNDAY ARUMALA
20. SUFUYANU TOUHIRAH
21. ABBAS HASSAN

INTRODUCTION

In an era where data is often described as "the new oil," the ability to protect and refine it is what separates successful organizations from those facing litigation and collapse. Securing, monitoring, and evaluating data are not three separate tasks; they are a **continuous loop** of digital hygiene.

Today, we will dive into how we lock the doors (Secure), how we watch the hallways (Monitor), and how we measure the value of what’s inside (Evaluate).

SECURING DATA: THE PERIMETER AND THE CORE

Securing data is the proactive defense against unauthorized access, corruption, or theft. It is the "Shield."

- **Encryption at Rest and in Transit:** Data must be unreadable to unauthorized eyes whether it is sitting on a hard drive or traveling across the internet.
- **Identity and Access Management (IAM):** The principle of "Least Privilege." Users should only have access to the data necessary for their specific role.
- **Data Masking and Anonymization:** For testing or research, sensitive identifiers are removed so that even if the data is seen, it cannot be linked back to an individual.
- **Physical Security:** Often overlooked, this involves the actual protection of servers and data centers against environmental hazards and physical intrusions.

MONITORING DATA: THE EYES ON THE SYSTEM

Monitoring is the "Watchtower." It is the real-time observation of data usage, flow, and system health to detect anomalies before they become disasters.

- **Real-time Alerts:** Using **SIEM (Security Information and Event Management)** tools to flag unusual activities, such as a bulk download of sensitive files at 3:00 AM.
- **Audit Trails:** Maintaining a chronological record of who accessed what data and when. This is vital for forensic investigations after a breach.
- **Data Integrity Monitoring:** Ensuring that data hasn't been altered by unauthorized parties. If a file's "checksum" or digital signature changes unexpectedly, the system triggers an alarm.
- **Network Traffic Analysis:** Identifying "bottlenecks" or suspicious data "exfiltration" points where data might be leaking out of the organization.

EVALUATING DATA: THE STRATEGY OF VALUE

Evaluation is the "Brain." It is the process of assessing whether the data we are securing and monitoring is accurate, useful, and compliant with regulations.

- **Data Quality Assessment (DQA):** Is the data clean? Evaluating for accuracy, completeness, and consistency. Decisions made on "garbage data" lead to "garbage results."
- **Compliance Evaluation:** Ensuring data practices align with laws like **GDPR**, **CCPA**, or **HIPAA**. This involves regular audits to avoid massive legal fines.
- **Data ROI (Return on Investment):** Determining if the cost of storing and securing specific data outweighs its business value. Not all data is worth keeping forever.
- **Performance Metrics:** Evaluating how well the security and monitoring systems are actually performing. If the "Mean Time to Detect" (MTTD) a breach is too high, the strategy needs an overhaul.

THE SYNERGY: HOW THEY WORK TOGETHER

These three pillars form a virtuous cycle:

- **Secure** it to prevent loss.
- **Monitor** it to ensure the security holds and to see how it’s used.
- **Evaluate** the usage patterns and quality to improve your security protocols.

Key Takeaway: You cannot evaluate what you haven't monitored, and you cannot monitor what you haven't secured.

CONCLUSION

Securing, monitoring, and evaluating data is not a "one-and-done" project. It is a mindset. As threats evolve and data volumes grow, our methods must become more sophisticated. By mastering this triad, we don't just protect bytes and bits—we protect the reputation and the future of our institutions.