Oksana Syvun

Insider Threat Intelligence Strategy:

1. Define Insider Threats:

Insider Categories:

Identify and classify different types of insider threats, such as negligent employees, malicious insiders, and compromised accounts.

2. Risk Assessment:

Data Sensitivity Analysis:

Assess the sensitivity of different types of data within the organization.

Access Permissions:

Review and manage employee access permissions based on their roles.

3. Insider Threat Detection:

Behavioral Analysis:

Implement tools and processes for monitoring and analyzing user behavior to detect anomalies.

Endpoint Monitoring:

Employ endpoint monitoring solutions to detect unusual activities on employee devices.

User Activity Logging:

Ensure comprehensive logging of user activities across critical systems and applications.

4. Incident Response Planning:

Insider Threat Incident Response Plan:

Develop a specific incident response plan for insider threats, outlining steps for identification, containment, eradication, recovery, and lessons learned.

Communication Protocols:

Establish communication procedures for notifying relevant stakeholders during an insider threat incident.

5. User Education and Awareness:

Training Programs:

Conduct regular training sessions for employees to increase awareness about insider threats, security best practices, and the consequences of violating security policies.

Reporting Mechanisms:

Provide clear channels for employees to report suspicious activities without fear of reprisal.

6. Access Controls:

Least Privilege Principle:

Implement the principle of least privilege to restrict access based on the minimum level necessary for job functions.

Regular Access Reviews:

Conduct regular reviews of employee access privileges to ensure they align with their roles and responsibilities.

7. Monitoring and Analysis Tools:

Insider Threat Intelligence Tools:

Invest in tools that specialize in detecting and analyzing insider threats, including user and entity behavior analytics (UEBA) solutions.

8. Data Loss Prevention (DLP):

DLP Policies:
Implement DLP solutions and policies to monitor, detect, and prevent unauthorized data exfiltration.

9. Insider Threat Intelligence Sharing:

Information Sharing Platforms:

Participate in industry-specific information sharing platforms to stay informed about insider threat trends and tactics.

Collaborate with External Partners:

Establish partnerships with external organizations and government agencies to share threat intelligence related to insider threats.

10. Legal and Compliance Considerations:

Legal Framework:

Ensure that the insider threat intelligence strategy complies with relevant laws and regulations.

Privacy Protection:

Implement measures to protect employee privacy while monitoring for insider threats.

11. Continuous Improvement:

Incident Post-Mortems:

Conduct thorough post-incident reviews to identify areas for improvement and update the insider threat intelligence strategy accordingly.

Feedback Loops:

Establish feedback loops to incorporate insights from incidents and investigations into the overall security posture.