INFO 7374 - Cybersecurity Audit and Compliance
Week 12 - Assignment 11

Krisha Lakhani – 002334794

Part 1: Continuous Monitoring

1. Identify and explain three key continuous monitoring controls that INFO-7374 Cloud Services should implement to detect security threats proactively.

a) Intrusion Detection and Prevention System (IDPS):
An IDPS is a fundamental measure that inspects network traffic and identifies malicious behavior such as port-scanning, brute-force attempts, and malware signatures.

- Intrusion Detection System (IDS) identifies and alerts on threat indicators via traffic analysis.
- Intrusion Prevention System (IPS) detects malicious events and manipulates the traffic in real-time to stop them (dropped or quarantined).

IDPS is implemented in cloud providers like INFO-7374 to provide a proactive defensive measure against attacks from both the inside and outside of the environment, but especially for the protection of Customer data in sensitive sectors like healthcare and finance.

b) Security Information and Event Management (SIEM):
SIEM tools allow logs and events to be centralized across the IT environment, the entire stack (application configuration, endpoint, firewall, server, etc.) is possible.

- SIEM provides: Correlates the data for complex threat detection, such as APTs (Advanced Persistent Threats).
- Alerts the security team in real-time.
- Dashboards and reports that ensure continuous visibility and oversight.

SIEM provides INFO-7374 with real-time visibility into its security posture and incident investigation for compliance reports.

c) Continuous Vulnerability Scanning & Patch Management:

This control calls for:

- Automated regular scans for known vulnerabilities across software, OS, and network configurations.
- Integration of any patch management decision with automated remediation mechanics of vulnerability.

By continuously scanning and remediating, INFO-7374 reduces the risk of exploitation from known CVEs (Common Vulnerabilities and Exposures), thus maintaining a hardened cloud environment.

INFO 7374 - Cybersecurity Audit and Compliance
Week 12 - Assignment 11

Krisha Lakhani – 002334794

2. What challenges might INFO-7374 Cloud Services face in implementing a robust continuous monitoring strategy? Provide two examples.

a) Data Volume and Alert Fatigue:

A system of continuous monitoring will produce a large amount of data. Without filtering or prioritization, this creates alert fatigue, where we will miss a critical alert due to a large volume of much less valuable false positives or low-severity alerts.

b) Integration Across Multi-Cloud Environments:

INFO-7374 operates in multiple regions and is most likely hybrid/multi-cloud environments. Integrating different monitoring tools/platforms (AWS, Azure, on-prem, etc.) while maintaining similar security policies and visibility is an immense workload.

3. Describe how continuous monitoring can help INFO-7374 Cloud Services detect insider threats. What specific indicators should be monitored?

Ongoing monitoring is a critical component of initiating detections of insider threats as they typically occur unnoticed by using valid access.

Monitoring should include the following types of indicators:

- Abnormal Login Behavior: Access outside of normal hours or geolocations.
- Abnormal File Access: Abrupt access to an unusually large number of sensitive files or confidential records unrelated to the user's position.
- Use of Unauthorized Devices: Copying files to USB drives or uploading files to personal cloud storage.
- Privilege Abuse: Users increasing privileges without authorization or accessing computar systems or personal data without permission.
- Changes in Activities: Changes to the frequency and timing or type of activity to internal systems can lead to unsafe behavior.

By correlating user behavior, logs, and behavioral changes in internal systems, the monitoring tools can flag potential insider threats early.

INFO 7374 - Cybersecurity Audit and Compliance
Week 12 - Assignment 11

Krisha Lakhani – 002334794

4. INFO-7374 Cloud Services experiences an attempted data breach. How should their continuous monitoring system **detect and respond to this incident in real-time?**

Detection:

- SIEM identifies abnormal outbound data traffic or unauthorized access attempts.
- NTA detects unusual data flows to suspicious external IP addresses.
- EDR alerts on processes or scripts running that match malicious behavior profiles.

Response:

- Automated workflows isolate compromised systems from the network.
- Revocation of affected credentials and tokens.
- Alerts are escalated to the incident response team.
- Logging systems preserve evidence for forensic analysis.
- Customers and regulatory bodies are notified if required (per IR plan and GDPR/C5).

The faster this system detects and contains the threat, the lesser the business impact.

5. Explain how continuous monitoring integrates with incident response planning. Provide an example of how real-time alerts can reduce incident impact.

Continuous monitoring feeds directly into the incident response lifecycle—specifically the detection, analysis, and containment stages.

Integration Example:

- A real-time SIEM alert about multiple failed login attempts from a single IP helps identify a brute-force attack.
- Automated rules within the incident response plan kick in: the IP is blacklisted, and affected accounts are temporarily disabled.
- The security team is notified to investigate further, preventing account compromise and potential data breaches.

This integration reduces impact by:

- Minimizing response time
- Containing threats before damage occurs
- Providing context for informed decisions

INFO 7374 - Cybersecurity Audit and Compliance
Week 12 - Assignment 11

Krisha Lakhani – 002334794

Part 2: German C5 2020 Standard

6. Describe two unique requirements of the C5 2020 standard that differentiate it from frameworks like SOC 2. If different from the ones discussed in class that is preferred.

a) Transparency Obligations (C5 "C" Criterion):
C5 requires cloud providers to explicitly disclose the scope of the audited services, data processing locations, and roles of subcontractors. Unlike SOC 2, which provides a general trust report, C5 demands detailed transparency in audit documentation to help customers assess compliance with EU data protection laws.

b) Alignment with German and EU Law:
C5 directly incorporates legal requirements from the German Federal Office for Information Security (BSI) and EU directives such as the GDPR. For example, it emphasizes data processing principles, lawful transfer outside the EU, and client responsibilities in shared service models—something not explicitly covered in SOC 2.

7. INFO-7374 Cloud Services must ensure compliance with C5's continuous monitoring requirements. Provide an example of a C5-specific control that mandates ongoing security oversight.

A specific C5 control from the "Operational Security" (OS) domain is:

"The cloud provider must implement mechanisms for continuous logging and monitoring of system activities to identify security-relevant events."

This includes:

- Real-time log aggregation.
- Defined thresholds for alerting and escalation.
- Regular log reviews and anomaly analysis.
- Ensuring logs are protected from unauthorized access and retained for a minimum period.

Such requirements ensure **continuous oversight**, traceability of incidents, and proactive threat detection.

INFO 7374 - Cybersecurity Audit and Compliance
Week 12 - Assignment 11

Krisha Lakhani – 002334794

8. How does the C5 2020 standard address incident response? What specific requirements does it impose on cloud service providers in terms of handling security incidents?

C5 stipulates organized and codified expectations of CSPs regarding incident response, including:

- **Incident Response Plan (IRP) Documentation:** The written IRP should identify roles and responsibilities, communication channels, and escalation paths.
- **Customer Notification Responsibility:** If incidents are data breaches with low to moderate impact on the organization, service providers must notify impacted customers as soon as possible, if the breaches involve personal, sensitive data or a data breach.
- **Evidence Retention:** CSPs must maintain logs and other artifacts of the incident for possible forensic investigation, and for audit purposes.
- **Testing and Training:** CSPs must routinely test their IRP in simulations. CSPs must train relevant personnel in response to incidents, and related document review and information collection.

All of this supports reasonable, timely, transparent, and effective incident responses, minimizing the risk of regulatory repercussions or loss of sensitive data.

9. INFO-7374 Cloud Services is planning to expand its operations within the EU. How does achieving C5 certification benefit the company's market position and regulatory standing?

a) Increased Market Confidence:
C5 certification indicates that INFO-7374 meets or exceeds stringent cybersecurity standards in Germany and the EU, thereby establishing itself as a credible vendor for regulated industries like healthcare or finance.

b) Competitive Advantage in the EU:
C5 certification provides evidence of compliance with GDPR, as well as other arrangements in the region, and can provide the company with a competitive advantage when bidding on contracts in Germany or the EU.

c) Regulatory Confidence:
The independent audit against the C5 standard is an indication to the regulators that the company is taking relatively proactive measures to meet data protection and cloud security obligations, which may lead to reduced audits or inquiries.

INFO 7374 - Cybersecurity Audit and Compliance
Week 12 - Assignment 11

Krisha Lakhani – 002334794

10. INFO-7374 Cloud Services fails to comply with certain C5 requirements. What potential consequences could they face from regulatory bodies and clients?

a) Regulatory Consequences and Investigations:
Failure to comply may trigger audits by German authorities (BSI) and GDPR-regulated data protection authorities. It is possible this could result in a financial penalty, sanctions imposed upon the organization, or being prohibited from continuing to operate in the EU.

b) Loss of Client Confidence and Contracts:
Clients, especially those in regulated industries - may terminate their contracts due to non-compliance with the agreed-upon terms of service. This could lead to the loss of revenue and damage to the organization's reputation.

c) Legal Responsibility and Lawsuits:
If an organization experiences a breach related to non-compliance, affected clients may be inclined to take legal action against them. This potentially includes seeking damages as the result of service outages, breaches of data security, or failure to fulfill contractual service level agreements.