Technical Documentation

Overview
This document outlines technical information to the end-user, with respect of potential business implications associated with various types of cybersecurity vulnerabilities and breaches, technological terminology of operating systems, virtual machine and networking system, firewalls and prevention systems.

How you the end-user support the process of cyber-risk assessment

- What is the process of cyber risk assessment?
  Cyber risk assessment is a systematic process of identifying, analysing, and evaluating potential security threats to determine their likelihood and impact on business operations. It involves cataloguing assets, identifying vulnerabilities, determining threat probabilities, and evaluating potential business impacts.

- How is cyber risk assessment carried out?
  - Asset inventory and classification
  - Vulnerability identification using scanning tools like Nmap and OpenVAS
  - Threat analysis and correlation
  - Risk prioritisation based on potential impact
  - Development of mitigation strategies
  - Documentation and continuous monitoring

- What role and how can end-users play in the process of cyber-risk assessment?
  - Identifying unusual system behaviour or performance issues
  - Reporting suspicious emails or phishing attempts
  - Following security protocols and maintaining credential security
  - Participating in security awareness training
  - Providing business context about the sensitivity of data they handle
  - Supporting testing periods by providing feedback on system functionality

The business implications of cyber security breaches

- What are the business implications of the types of vulnerabilities and cyber security breaches you identified in your initial investigations?

  1) Content Theft or Fraud: Unauthorised replication or distribution of proprietary digital content or manipulation of digital assets for fraudulent gain
  Business Implications:
  - Direct financial impact due to lost sales or subscription income.
  - Erosion of customer trust and diminished brand equity.
  - Potential lawsuits and penalties from violated intellectual property rights or consumer protection laws.

  2) Unauthorised access: Gaining system or data access without proper authentication or authorisation, typically exploiting system misconfigurations or credential weaknesses.
  Business Implications:
  - Exposure of sensitive organisational or customer data.
  - Breach of regulatory obligations (e.g., GDPR, HIPAA), resulting in legal sanctions and compliance costs.

3) Payment fraud / Chargebacks: Illegitimate transactions carried out via compromised payment systems, often resulting in chargebacks or losses.
Business implications:
- Revenue loss from reversed transactions and penalties.
- Degraded relationships with payment processors or financial institutions due to high fraud rates.

4) Device Exploitation (BYOD): Exploitation of vulnerabilities in employee-owned devices used in the workplace, leading to malware propagation and security breaches.
Business implications:
- Lateral movement of malicious software between personal and enterprise environments.
- Downtime and increased IT overhead due to threat containment and remediation.

5) Weak credential practices: Use of insecure authentication mechanisms such as shared or weak passwords, increasing the risk of account compromise.
Business Implications:
- Unauthorised access to business systems or data through credential reuse or phishing.
- Compromised user segregation policies and elevated risk of internal data leakage.

6) Unsecured backups: Storage of backup data without adequate encryption or physical safeguards, increasing the risk of data theft or loss.
Business Implications:
- Irretrievable loss of business-critical information due to theft or destruction of backup media.
- Failure to meet data protection standards, leading to fines or enforcement actions.

- What are the implications to the user if they do not adopt or implement the solution?
  - The business is exposed to payment fraud and revenue loss
  - Unauthorised access to creator content bypassing the paywall
  - Content theft leading to creator distrust and they will leave the platform, for example if creators know content is uploaded to forums illegally, they will stop using that platform because of plummet income
  - Data breaches exposing sensitive information from the password spreadsheet
  - Man-in-the-middle attack to the organisation's network system and intercepts communication and steal data or even manipulate the data being exchanged

Operating systems (Windows or Linux)

- Give an overview of how the operating system used within the organisation is vulnerable to cybersecurity risks.
  - Unpatched systems exposing known security flaws
  - Default configurations with unnecessary services running
  - Weak access controls allowing unauthorised system modifications
  - Password storage and login details saved in a plain text spreadsheet
  - Lack of endpoint protection on mobile devices
  - Insufficient logging and monitoring for suspicious activities

- Describe two methods the user can implement to improve security when using the operating system identified.
  - Implement automated patch management and updates using scripted solutions

integrated with Metalog for auditing
- Deploy endpoint protection with centralised management to enforce security policies across all devices, regardless of location.

Virtualisation operation and structure

- Explain what virtualisation is and why the end-user needs to use it:
  Virtualisation creates isolated environments where multiple operating systems run on a single physical machine. The end-user, or the business needs it for secure testing of security configurations without risking production systems, or isolating network segments for different business functions, creating secure development and testing environments, running security tools like penetration testing without impacting business operations and facilitating disaster recovery with portable system images.

- Explain how they access the virtualisation:
  Virtual environments can be accessed through virtual machine management console on local workstations, or secure remote access tools when working offsite, or web-based administration portal for cloud-hosted virtual resources.

- Explain the structure of the virtualisation:
  Virtualisation structure includes host systems running hypervisor software, guest virtual machines for specific functions like development, testing or production, other components could be virtual networks connecting systems in isolated segments, shared storage resources with appropriate access controls, backup and recovery systems for virtual environments.

- Give instructions for each of the following as they related to your planned solution:

- Creating and configuring virtualised images
  - Select appropriate base image from the repository, or source download centre
  - Configuration of CPU, memory and HDD
  - Install required operating system updates and security patches: from Windows Updates for Windows OS, or command line from Terminal of Linux OS Distribution.
  - Apply security hardening templates specific to the virtual machine's purpose.
  - Install and configure required applications and security tools (NMap, PfSense, Wireshark)
  - Create system snapshot before deployment.

- Interconnecting virtual images
  - Define virtual network segments based on security zones
  - Configure virtual switches to isolate traffic between segments
  - Implement virtual firewalls between networks segments
  - Apply access controls between virtual machines
  - Monitor inter-VM traffic using virtual intrusion detection system (IDS) sensors

Using networking devices

- Explain what networking devices the end-user may need to interact with.
  - pfSense firewall for network protection
  - Network switches for connecting workstations and servers
  - Wireless access point with segregated networks
  - Network monitoring tools interfacing with Snort and Metalog
  - VPN concentrator for secure remote access

- Give instructions for using networking devices post-implementation of your planned solution. i.e. how to gain access, how to maintain access, how to control access, how to secure etc.
  - Access network management through secured admin portal requiring two-factor authentication
  - Maintain access by regularly updating credentials according to password policy
  - Control access through role-based permissions in the management interface
  - Secure devices by applying vendor security updates when available
  - Monitor device logs forwarded to sophisticated tools like Elasticsearch, Logstash and Kibana (ELK) Stack for anomaly detection

Configuring firewalls

- Explain how firewalls are to be used in the client workplace as identified in your planned solution.
  Firewalls are deployed as a multi-layer defence using pfSense
  - Perimeter protection blocking unauthorised external access
  - Network segmentation between content delivery and payment systems
  - Application-level layer filtering to prevent content extraction
  - Traffic monitoring with alerts for suspicious patterns
  - VPN enforcement for remote worker connections
- Give instructions for configuring or maintaining the firewall as it applies post-implementation of your planned solution
  - Access pfSense management interface via secure HTTPS connection
  - Review firewall logs daily through logging tools, like ELK Stack dashboard
  - Apply recommended rule updates when notified by security team
  - Test configuration changes in virtualised environment before deployment
  - Verify rule effectiveness using built-in packet capture tools
  - Schedule monthly security reviews to evaluate rule effectiveness

Implementing Intrusion Detection Systems (IDS)

- Identify and explain the purpose of the intrusion detection systems (IDS) implemented by your team. Include examples of the key features to support your answer.

  - *Real-time traffic analysis and packet logging*
  Purpose: Monitors network traffic in real-time and records detailed logs for forensic analysis
  Example: Detects unauthorised attempts to download copyright music files in bulk, helping to prevent content theft and enforce licensing terms.

  - *Pattern matching against known attack signatures*
  Purpose: Compares incoming traffic against a database of known malicious patterns (signatures).
  Example: Identifies SQL injection attempts targeting user login APIs, a common method to bypass authentication and hijack user accounts, a risk noted under weak credential practices.

  - *Protocol analysis to identify abnormal behaviours*
  Purpose: Evaluates network protocol behaviour to detect anomalies, misuses, or policy violations
  Example: Flags unusual use of HTTP methods or excessive POST requests to payment endpoints, indicating a potential payment fraud or bot attack exploiting the checkout system.

- *Anomaly detection to identify deviations from baseline traffic*
Purpose: Establishes normal network behaviour and flag deviations.
Example: Alerts when a personal device on BYOD policy starts scanning internal IP addresses signalling a compromised device used in lateral movement attempt.

- *Integration with ELK Stack for centralised monitoring*
Purpose: Aggregates and visualises logs and alerts in a unified dashboard for rapid incident response.
Example: Security analysts can correlate logs from the IDS, web servers, and payment systems to investigate and mitigate a multi-vector attack targeting both content and financial systems.

- *Custom rules tailored to protect digital content and payment systems*
Purpose: Allows the creation of specific detection rules relevant to unique business needs.
Example: Rules can be crafted to detect large volume streaming requests from a single IP, indicating potential API abuse or scraper bots aiming to mirror content unlawfully.

- Explain how your end-user can use the IDS to examine data for and respond to anomalies in line with your planned solution.
  - Access the IDS dashboard through the ELK Stack interface
  - Review daily summary reports highlighting detected anomalies
  - Investigate alerts using provided drill-down capabilities
  - Cross reference suspicious activity with business events
  - Escalate confirmed incidents according to response playbooks
  - Participate in regular reviews to refine detection rules

Implementing Intrusion Prevention Systems (IPS)

- Identify and explain the purpose of the intrusion prevention systems (IPS) implemented by your team.
  - Active threat blocking using Snort in prevention mode
  - Automated response to known attack patterns
  - Traffic normalisation to prevent evasion techniques
  - Rate limiting to mitigate denial of service attempts
  - Application protection focused on payment system integrity
- Explain how your end-user can use the IPS to monitor traffic and respond to anomalies in line with your planned solution.
  - Monitor IPS dashboard showing blocked threats
  - Review false positive reports to approve rule adjustments
  - Temporarily disable specific rules when needed for business functions
  - Analyse blocked traffic reports to identify persistent threats
  - Validate that legitimate business traffic is not being blocked
  - Participate in periodic rule tuning to balance security and functionality