AethelGuard Solutions

Risk Assessment

1. Objectives & Scope

This top-level risk assessment aims to define and categorize all the information security risks that could occur for AethelGuard Solutions, a company that provides a custom-built and modifiable software for protecting endpoint computers within enterprise companies. This risk assessment also proposes a mitigation plan to address the potential threats the company could face.

2. Key Assets

The key assets covered by AethelGuard Solutions, critical for its operations and client protection, are categorized as follows:

- **Information Assets:**
  - **Intellectual Property (IP):** Source code of AethelGuard's endpoint protection software, proprietary algorithms, threat intelligence databases, product documentation, and development roadmaps.
  - **Internal Access & Operational Data:** Employee access credentials and privileges (e.g., for badge access to server rooms, system permissions), operational data defining who within AethelGuard has access to client telemetry logs, and who is authorized to make modifications to AethelGuard's software or client configurations.
  - **Client Information (Non-telemetry):** Client contact details, service agreements, confidential deployment specifics (e.g., client network topology data, specific endpoint versions on their networks). This information, if compromised, directly impacts client security.
  - **Client Endpoint Telemetry Data:** Logs and real-time data collected from client endpoints by AethelGuard's software, crucial for threat detection and analysis.
  - **Internal Confidential Data:** Employee PII (e.g., HR records), financial records, strategic business plans, and internal communication.
- **Software Assets:**
  - **AethelGuard Product Software:** The deployed endpoint protection software (including current and historical versions, updates, and associated threat definitions).
  - **Development & Testing Environments:** CI/CD pipelines, code repositories (e.g., Git), build servers, testing VMs, and associated toolchains.
  - **Internal Business Applications:** CRM, ERP, HR management systems used by AethelGuard.
- **Hardware Assets:**
  - **AethelGuard's Internal Infrastructure:** Servers (on-premise or cloud-based) hosting AethelGuard's products, development, and internal operations; network devices (firewalls, routers, switches); and AethelGuard's employee workstations/laptops.
  - **Cloud Infrastructure:** Cloud accounts and services (IaaS, PaaS, SaaS) subscribed to and managed by AethelGuard for its own operations and for hosting its services.
  - **Note on Client Endpoints:** While client endpoints are owned by clients, AethelGuard's software operates on them, and AethelGuard holds vital information about them (e.g., their security status, network

configuration data). This information, when processed or stored by AethelGuard, becomes a critical asset for which AethelGuard holds a responsibility to protect.

- **Human Assets:**
    - AethelGuard's Employees: Their skills, knowledge, and integrity; especially developers, security engineers, and support staff with access to critical systems and data (both internal and client-related).

3. Threats

AethelGuard Solutions faces various internal and external threats, including:

- New Cyber Emerging Threats: Rapid evolution of malware, zero-day exploits, and sophisticated attack techniques targeting endpoint protection.
- Targeted Attacks on IP: Adversaries attempting to steal proprietary source code, algorithms, or threat intelligence data for competitive advantage or malicious use.
- Supply Chain Attacks: Compromise of AethelGuard's software development and distribution channels, potentially injecting malicious code into product updates delivered to clients.
- Ransomware & Advanced Malware: Campaigns targeting AethelGuard's internal infrastructure, disrupting operations, encrypting data, or impacting service delivery.
- Phishing & Social Engineering: Attacks targeting AethelGuard employees to gain unauthorized access to internal systems or sensitive customer data.
- Data Breaches: Unauthorized access to customer configurations, telemetry logs, client PII, or AethelGuard's internal confidential data.
- Denial of Service (DoS/DDoS) Attacks: Aimed at AethelGuard's product infrastructure, impacting service availability and client trust.
- Insider Threats: Malicious or negligent actions by current or former employees (e.g., data exfiltration, unauthorized access).
- Regulatory Non-Compliance: Failure to adapt to changing data protection laws (e.g., GDPR, CCPA) potentially leading to fines and reputational damage.
- Third-Party & Vendor Compromise: Security incidents affecting AethelGuard's vendors or suppliers, impacting service delivery or data security.

4. Vulnerabilities

Internal weaknesses and system flaws that could be exploited by threats include:

- Inconsistent Security Processes & Documentation: Security procedures are informal, ad-hoc, and inadequately documented, hindering consistent application.
- Lack of Internal Audits: Absence of regular internal security audits means weaknesses are not systematically identified and addressed.
- Low Security Awareness: Staff lack sufficient understanding of information security risks and best practices, making them susceptible to social engineering.
- Staff Complacency: Over-reliance on technical tools without proper human oversight or process adherence, leading to a false sense of security.
- Limited Understanding of ISO 27001 & Data Laws: Insufficient knowledge of key security standards and data protection regulations within relevant teams.

- Resource Constraints: Lack of dedicated security personnel or budget to implement and maintain robust security controls.
- Inconsistent Approach Across Departments/Sites: Different security practices across various teams or geographical locations, creating security gaps.
- Software & Development Vulnerabilities: Potential bugs or design flaws in AethelGuard's own software, or vulnerabilities within the development pipeline (e.g., insecure code repositories, misconfigured CI/CD).
- Cloud Misconfigurations: Insecure default configurations or oversight in the deployment of cloud services (AWS, Azure, GCP).
- Inadequate Patch Management: Internal systems and infrastructure are not consistently or timely patched against known vulnerabilities.
- Insufficient Logging & Monitoring: Lack of comprehensive logs or real-time security monitoring (SIEM) makes detecting and responding to incidents difficult.
- Weak Access Controls: Overly permissive access rights, inadequate Multi-Factor Authentication (MFA) on critical systems, or poor management of privileged accounts.
- Outsourced IT Concerns: Over-reliance on an outsourced IT provider that may not be proactive or sufficiently security-aware.

5. Likelihood & Impact (Qualitative)

To effectively evaluate risks, AethelGuard Solutions defines qualitative scales for Likelihood (the probability of a threat exploiting a vulnerability) and Impact (the severity of the damage should the risk materialize).

- Likelihood Scale:
  - High: Highly probable to occur within one year (e.g., >80% chance).
  - Medium: Likely to occur within one to three years (e.g., 50-80% chance).
  - Low: Unlikely to occur within three years (e.g., <50% chance).
- Impact Scale:
  - Critical: Severe financial loss, significant reputational damage, major legal/regulatory penalties (e.g., large GDPR fines), total loss of IP or core operations.
  - High: Significant financial loss, substantial reputational damage, moderate legal/regulatory penalties, partial loss of IP or disruption of core operations.
  - Medium: Moderate financial loss, minor reputational damage, minimal legal/regulatory issues, minor disruption to operations.
  - Low: Minimal financial loss, negligible reputational damage, no legal/regulatory impact, minimal operational disruption.

6. Existing Controls & Gaps

AethelGuard Solutions currently has some foundational security controls in place, but also recognizes existing gaps based on identified vulnerabilities.

- Current Controls:
  - Perimeter Security: Basic firewalls and network segmentation in critical production environments.
  - Access Management: Password policies enforced for internal systems.
  - Endpoint Protection: AethelGuard's own software deployed on internal endpoints.
  - Backup & Recovery: Routine data backups for critical internal systems.

    - Cloud Security: Basic security configurations applied to cloud accounts.
    - Development Security: Basic code review processes.
- Identified Gaps (Linked to Vulnerabilities):
    - Patch Management: Inconsistent and untimely patching cadence for internal infrastructure and third-party software.
    - Multi-Factor Authentication (MFA): Not uniformly implemented across all critical systems, especially for administrative access to cloud services or internal applications.
    - Security Awareness Training: Infrequent and insufficient training for employees, leading to susceptibility to social engineering.
    - Logging & Monitoring: Lack of comprehensive SIEM (Security Information and Event Management) for centralized logging and real-time threat detection across all environments.
    - Internal Audit Program: Absence of a formal, periodic internal audit process to independently assess control effectiveness.
    - Privileged Access Management (PAM): Insufficient controls for managing and monitoring privileged user accounts.
    - Third-Party Risk Management: Limited assessment and oversight of security practices of external vendors and outsourced IT.
    - Policy Enforcement: Existing security policies are often informal and lack consistent enforcement mechanisms.

7. Risk Evaluation & Prioritization

This section combines identified threats and vulnerabilities, assesses their likelihood and impact, and determines the overall risk level for AethelGuard Solutions. Risks are then prioritized to guide mitigation efforts.

Risk ID	Asset Category	Threat Descrption	Vulnerability Descrption	Current Control(s)	Likelihood	Impact	Current Risk	Priority
RA-01	IP (Source Code)	Targeted attack to steal proprietary source code	Insecure code repository access; weak MFA; insufficient logging	Basic access control on Git (role-based)	High	Critical	Critical	P1 (Urgent)
RA-02	Client Data (PII)	Data Breach (Phishing) affecting client PII	Low security awareness; lack of MFA on internal email/systems	Password policy; basic email filter	High	Critical	Critical	P1 (Urgent)
RA-03	Development Env.	Supply Chain Attack via CI/CD pipeline	Vulnerable CI/CD; insufficient security testing in dev process	Basic code review	Medium	Critical	High	P2
RA-04	Internal	Insider	Overly	Password	Medium	High	High	P2

	Access Data	Threat (malicious/ negligent) leading to privilege escalation	permissive access rights; no PAM; inconsistent access reviews	policy				
RA-05	Cloud Infrastructure	Cloud Misconfiguration leading to data exposure	Lack of cloud security posture management (CSPM); inadequate review of cloud configs	Basic cloud account config	Medium	High	High	P2
RA-06	Endpoint Telemetry	Denial of Service (DoS) attack on product infrastructure	Insufficient DDoS protection; lack of scalability in infrastructure	Basic load balancing	Low	High	Medium	P3

Prioritization Key:

- **P1 (Urgent):** Immediate action required; critical impact with high likelihood.
- **P2 (High):** Action required within short-term; significant impact or high likelihood.
- **P3 (Medium):** Action within medium-term; moderate impact or moderate likelihood.

8. Risk Treatment Options

AethelGuard Solutions adopts the following strategies for treating identified risks:

- Mitigate: Implementing controls to reduce the likelihood or impact of a risk. This is the primary strategy for all Critical and High risks.
- Transfer: Shifting the risk to a third party (e.g., through cyber insurance).
- Accept: Acknowledging the risk and its potential impact without implementing further controls, typically for Low risks where mitigation cost outweighs benefit.
- Avoid: Eliminating the risk by discontinuing the activity that gives rise to it.

The focus of the 90-day Mitigation Roadmap (Section 9) is on implementing mitigation controls for the highest priority risks.

9. 90-day Mitigation Roadmap

This roadmap outlines key actions to address the highest priority risks identified.

- **30 days:**
  - Improve patch management for critical internal systems and third-party applications.
  - Finalize asset inventory for all key IT infrastructure and software assets.
  - Enforce Multi-Factor Authentication (MFA) for all administrative accounts and access to critical systems.
- **60 days:**
  - Implement network segmentation for development, production, and corporate environments.
  - Initiate regular access reviews for privileged user accounts and critical system access.
  - Harden critical endpoints with advanced security configurations and endpoint detection & response (EDR) solutions.
- **90 days:**
  - Establish basic incident response procedures and develop incident playbooks.
  - Create dashboards and baseline reporting for key security metrics (e.g., patching compliance, MFA adoption, security awareness scores).
  - Enforce Multi-Factor Authentication (MFA) for all administrative accounts and access to critical systems. *(Addresses RA-02, RA-04)*

10. Roles & Accountability

Information security is a shared responsibility within AethelGuard Solutions. The following roles are primarily accountable for driving and overseeing risk management and mitigation efforts:

- **Security Lead:** Overall owner of the risk assessment process, policy enforcement, and security strategy.
- **IT Operations:** Responsible for implementing technical controls, patch management, and infrastructure security.
- **Risk Manager (or designated person):** Oversees risk identification, analysis, and reporting.
- **Compliance:** Ensures adherence to legal and regulatory obligations (e.g., GDPR, ISO 27001).
- **HR (onboarding/offboarding policy):** Manages user access lifecycle and security awareness training for employees.

11. Appendices

References:

- NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments
- ISO 31000: Risk Management – Guidelines
- ISO/IEC 27005: Information Security Risk Management
- MITRE ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge

Disclaimer:
This document is a simulated project developed for portfolio purposes.
The company AethelGuard Solutions is entirely fictitious, and any resemblance
to existing companies, products, or services is purely coincidental.
This project does not represent any real-world assessment or operational advice.