Threat Modelling

AstroDev

1. What are we building – A system that allows grounds communications and computers on spacecrafts to operate with minimal disruption

2. What can go wrong – Signals and messages between the ground stations and the spacecraft can be intercepted by unwanted parties

3. What are we going to do about it – Ensure security within the communications, keeping information and confidential information private

4. Did we do a good job –

Risk Treatment Plan

Risk ID	Risk Description	Risk Treatment	Likelihood	Impact	Impact	Status
1						
2						
3						

Defence Ventures

1. What are we building – ShieldX: A secure defence software that benefits both military and civilian sectors, where it acts as a solution of providing barriers of security for defence organisations' systems.

2. What can go wrong – Unknown threats that aren't registered with ShieldX can slip through and cause problems with organisations' systems.

3. What are we going to do about it – Regularly record newfound threats to provide solutions and prevent attacks on systems

4. Did we do a good job -

Risk Treatment Plan

Risk ID	Risk Description	Risk Treatment	Likelihood	Impact	Impact	Status
1						
2						
3						

Secure Software Development (CMP020X306)

Generated Case Study

Company name

AstroDev

Company profile

AstroDev is a cutting-edge start-up specializing in innovative space technology solutions. Founded by a team of visionaries with expertise in aerospace engineering and computer science, AstroDev aims to revolutionize the industry through its pioneering approach to software development for space exploration. By combining state-of-the-art network connectivity and robust software design, AstroDev's products ensure seamless communication between spacecraft systems, enhancing mission efficiency and safety.

Product

GalacticLink

Users

GalacticLink Users

Astronomers

• **Seamless Data Transmission**: GalacticLink facilitates the secure transfer of large astronomical datasets between spacecraft, ground stations, and research centers. This accelerates data analysis and enables scientists to make groundbreaking discoveries sooner.

Space Agencies

• **Enhanced Mission Control**: By integrating GalacticLink into their systems, space agencies can monitor mission progress in real-time, receive critical alerts, and respond promptly to system anomalies. This ensures the success of complex space missions.

System architecture

GalacticLink Architecture

1. **Spacecraft System**: GalacticLink is integrated into spacecraft systems, enabling secure communication between onboard computers and ground stations.
2. **Ground Station Network**: A decentralized network of ground stations connects to the spacecraft system via satellite or terrestrial links, ensuring global coverage and redundancy.

3. **Cloud-Based Data Center**: The cloud data center processes and stores astronomical data from space missions, providing secure access for researchers and scientists worldwide.

Data

GalacticLink Data Storage

1. **Astronomical Data**: GalacticLink stores large datasets from space missions, including images, spectrograms, and other scientific observations.
2. **Spacecraft Telemetry**: The system records telemetry data from spacecraft systems, such as temperature, pressure, and power consumption.
3. **Mission Control Communications**: GalacticLink logs communication records between mission control centers and spacecraft, ensuring audit trails for critical decisions.

GalacticLink does not store personal data of customers or staff. All user information is handled securely through separate, compliant systems to maintain the highest level of data privacy.

Cyber risk appetite

AstroDev has a high cyber security risk appetite. The company is willing to take on significant cyber risks in pursuit of innovation and market leadership. This approach enables AstroDev to push the boundaries of space technology and drive growth, but also increases the potential for costly cyber breaches and reputational damage.

Employee awareness of cyber security

AstroDev employees have limited awareness of cyber security best practices. The company's focus on innovation and rapid development has led to a prioritization of technical skills over cyber security training. Many employees are not aware of common cyber threats, safe coding practices, or secure communication protocols, increasing the risk of human error contributing to potential breaches.

Secure Software Development (CMP020X306)

Generated Case Study

Company name

DefenceVentures (DVF)

Company profile

DefenceVentures (DVF) is an early-stage venture capital firm specializing in defence technology innovation. We invest in and support cutting-edge companies developing secure software solutions for defence applications, ensuring both military and civilian sectors benefit from advanced technological advancements. DVF's mission is to foster a vibrant ecosystem of next-generation defence technology, collaborating with entrepreneurs, industry partners, and governments to address the most pressing security challenges.

Product

ShieldX: DefenceVentures' advanced, secure defence software solution. Empowering innovation with uncompromised protection.

Users

ShieldX is designed for organizations in the defence sector, including military forces and civilian security agencies, who require robust and secure software solutions to protect sensitive information and maintain operational readiness. By implementing ShieldX, these organizations can mitigate cyber threats, safeguard intellectual property, and ensure the highest levels of data privacy and network security. Additionally, ShieldX's innovative approach helps defense teams focus on their mission-critical tasks without constant concerns about potential vulnerabilities in their software infrastructure.

System architecture

ShieldX's architecture includes a centralized Management Console for configuration and monitoring, connected to a distributed network of secure Agents deployed across the organization's IT infrastructure. These Agents continuously analyze network traffic and application activity for signs of threats, using advanced machine learning algorithms and intrusion detection systems.

The software employs multi-layered security, such as firewalls, antivirus solutions, and encryption, to protect against various cyber threats. ShieldX also integrates with external threat intelligence feeds and vulnerability databases for real-time risk assessments and automated responses. Network connectivity is essential for the software to receive updates, communicate with the management console, and share threat information between Agents, ensuring the organization remains protected from evolving security threats.

Data

ShieldX primarily focuses on storing and processing data related to network traffic and application activity within an organization's IT infrastructure for security analysis purposes. This includes metadata such as IP addresses, ports, packet sizes, timestamps, and application event logs. No personal data of customers or staff is intentionally stored by the software, but it may incidentally capture and process certain data if it passes through the network or applications under protection. In such cases, ShieldX complies with applicable privacy laws and regulations, ensuring that all handled data remains confidential, secure, and anonymized.

Cyber risk appetite

DefenceVentures and its software solution, ShieldX, have a moderate cybersecurity risk appetite. This means that the organization aims to strike a balance between accepting an acceptable level of risk and implementing sufficient measures to mitigate potential threats. They are not willing to take on excessive risks that could significantly impact their operations or reputation but are also open to making strategic decisions that involve some calculated risk for the benefit of their business and clients.

Employee awareness of cyber security

The level of cybersecurity knowledge among DefenceVentures' employees is considered modest. This lack of awareness may increase the organization's susceptibility to potential cyber threats, as employees might inadvertently create vulnerabilities through actions such as opening malicious emails, using weak passwords, or falling for phishing scams.

To mitigate this risk and improve the overall cybersecurity posture, DefenceVentures should invest in regular training programs that educate employees about best practices related to password management, email security, social engineering tactics, and safe browsing habits. Enhancing employee awareness will not only help prevent incidents but also foster a culture of security within the organization, making it more resilient against cyber threats.