**PROSIT – 3**

**KEYWORDS** a

* Cyberattack - an attempt by hackers to damage or destroy a computer network or system.
* Cybersecurity - Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
* SOC analyst – the person who is responsible to monitor a company's information system in the broad sense in order to detect all suspicious or malicious activities
* security administrator - employees who test, protect, and ensure the hardware, software, and the data within the computer networks, is secure. They are typically responsible for the entire system and ensure that it is defended as a whole.
* Firewalls - A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.
* VPN - an arrangement whereby a secure, apparently private network is achieved using encryption over a public network, typically the internet.
* VLANs - A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group.
* SIEM - Security information and event management, or SIEM, is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations.
* IDS - a network security tool that monitors network traffic and devices for known malicious activity.
* IPS - a technology that keeps an eye on a network for any malicious activities attempting to exploit a known vulnerability.
* Threats - acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems.
* System logs - System logs can include various types of information such as system errors, security events, application usage data, and network traffic details. Logs are often categorized into different types such as access logs, error logs, transaction logs, and security logs, each serving unique purposes.
* Risk analysis - The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact
* Anomalies - Anomalies in network behaviour deviate from what is normal, standard, or expected
* Security flaw - A flaw is unintended functionality. This may either be a result of poor design or through mistakes made during implementation. Flaws may go undetected for a significant period of time.
* Vulnerability - a weakness in an IT system that can be exploited by an attacker to deliver a successful attack. They can occur through flaws, features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal.
* Penetrate - Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system.

**CONTEXT** a

TechNova faces a critical cyberattack, and cybersecurity expert Lucas swiftly mitigates the threat, identifies vulnerabilities, and recommends corrective actions to safeguard sensitive data.

**PROBLEM STATEMENT** a

What can TechNova implement and improve to fix the breach in the it department while preventing future incidents to insure data and user safety?

**DELIVERABLES** a

* Make a report
* Identify potential threats
* Identify security methodologies and tools

**CONSTRAINTS** a

* Time
* Already existing infrastructure

**ACTION PLAN** a

1. Study different cyber security attacks
2. Security measures and polices
3. Study Soc (teams, roles)
4. Study CIA triad
5. Study IEM, IDS, IPS