Aug 2024 - Sep 2024

Cyber Intelligence Sharing and Collaboration

TechGuard Inc., a major cybersecurity solutions provider with a diverse client base spanning financial services, healthcare, and critical infrastructure sectors, has recently been hit by a sophisticated and multi-faceted cyber attack. The attack appears to be part of a large-scale, coordinated campaign orchestrated by a well-resourced advanced persistent threat (APT) group known as "Specter."

Task 1

Identify and Assess Relevant Information Sharing Platforms:

The following platforms could assist in gathering additional intelligence on the "Specter" APT group and similar threats.

- **Government-Led Initiatives:**

  1. **National Computer Emergency Response Team (NCERT):** Pakistan's national cyber emergency response team, coordinating cyber security activities and sharing information.
  2. **Cybersecurity and Infrastructure Security Agency (CISA):** A U.S. government agency that facilitates information sharing and collaboration among government, industry, and academia.
  3. **National Cyber Security Centre (NCSC):** The UK's national authority for cybersecurity, offering various threat intelligence services and sharing platforms.
  4. **CERT-In:** India's national cyber emergency response team, providing threat intelligence and incident response services.

- **Industry-Led Initiatives:**

  1. **Financial Services Information Sharing and Analysis Center (FS-ISAC):** A nonprofit organization focused on sharing threat intelligence and best practices within the financial services industry.
  2. **Healthcare Information Sharing and Analysis Center (H-ISAC):** A nonprofit organization dedicated to protecting the healthcare sector from cyber threats.
  3. **Critical Infrastructure Information Sharing and Analysis Center (CI-ISAC):** A nonprofit organization that facilitates information sharing among critical infrastructure sectors.
  4. **Cloud Security Alliance (CSA):** A nonprofit organization promoting the adoption of secure cloud computing technologies and practices.

5. **ThreatConnect:** A cloud-based threat intelligence platform that provides access to a global network of threat intelligence sources.
6. **Anomali:** A threat intelligence platform that offers advanced threat detection and response capabilities.
7. **CrowdStrike Falcon Platform:** A cloud-native endpoint protection platform that includes threat intelligence and hunting capabilities.

Task 2

Develop a Collaboration Plan:

1. **Establish a Central Point of Contact:** Designate a dedicated team within TechGuard Inc. to manage information-sharing activities and coordinate with external partners.
2. **Prioritize Information Sharing:** Identify the most critical types of threat intelligence to be shared, such as indicators of compromise (IOCs), tactics, techniques, and procedures, and threat actor profiles.
3. **Develop Protocols for Sharing Sensitive Information:** Establish secure channels and protocols for sharing sensitive data, ensuring compliance with relevant regulations and privacy laws.
4. **Participate Actively in Information Sharing Communities:** Engage with relevant platforms and communities, contributing valuable insights and leveraging their resources to enhance threat detection and response capabilities.
5. **Leverage Threat Intelligence to Enhance Security Posture:** Integrate shared intelligence into existing security tools and processes, enabling proactive threat hunting and incident response.
6. **Conduct Regular Threat Assessments:** Analyze shared intelligence to identify emerging threats and vulnerabilities that could impact TechGuard Inc. and its clients.
7. **Foster Collaborative Relationships:** Build strong relationships with other organizations involved in information sharing, fostering trust and cooperation.

By actively participating in information-sharing communities and leveraging shared intelligence, TechGuard Inc. can significantly improve its ability to detect, mitigate, and respond to advanced cyber threats like the ”Specter” APT group.