Project Objective: To create a state-of-the-art cyber security team at Nomura that can protect the company’s data and systems from cyberattacks.

Project Scope:

- Team Composition: The project team will be composed of experienced cyber security professionals with a wide range of skills and expertise.
    - Cybersecurity Manager/Team Lead: An experienced professional who oversees the entire cybersecurity team, sets the strategy, manages resources, and liaises with upper management.
    - Security Analysts: They are responsible for monitoring the company's network and systems for security incidents, analyzing threats, and responding to security alerts.
    - Incident Response Team: These individuals are trained to handle security incidents in real-time, mitigating the impact of cyberattacks, and ensuring a swift response to breaches.
    - Threat Intelligence Specialists: They gather and analyze information on emerging cyber threats and vulnerabilities, providing the team with proactive insights to strengthen defenses.
    - Penetration Testers/Ethical Hackers: Responsible for conducting simulated cyberattacks to identify weaknesses in the company's infrastructure and applications.
    - Network Security Engineers: They design, implement, and maintain the organization's network security infrastructure.
    - Application Security Experts: Specialized in ensuring that software applications developed and used within the organization are secure.
    - Data Security Specialists: Focused on protecting sensitive data through encryption, access controls, and data loss prevention measures.
    - Compliance and Governance Experts: Ensure the team adheres to relevant regulations and industry standards while maintaining a robust cybersecurity posture.
    - Security Operations Center (SOC) Analysts: Monitor security events and incidents in real-time, conduct initial analysis, and escalate issues to the incident response team.
    - Security Awareness Trainers: Responsible for educating employees about cybersecurity best practices and raising awareness about potential risks.
    - Forensic Analysts: If a cyber incident occurs, these experts help investigate the incident, gather evidence, and support post-incident analysis.
    - Vendor/Third-party Risk Specialists: Assess the cybersecurity posture of third-party vendors and manage associated risks.
    - Cloud Security Specialists: As more organizations move to the cloud, these experts focus on securing cloud-based assets and services.
    - Legal and Compliance Advisors: Provide legal expertise and ensure the team's actions align with legal requirements.

  - Communication and Public Relations: In the event of a cybersecurity incident, these professionals handle communication with stakeholders, the media, and the public.

- Team Training: What training would you provide to the team?
  - Cybersecurity Fundamentals
    - Introduction to cybersecurity and its importance in the financial industry.
    - Common cybersecurity terminologies, such as threat, vulnerability, and risk.
    - Overview of various cybersecurity domains, including network security, application security, and data security.
  - Latest Threat Landscape
    - Understanding recent cyber threats, attack trends, and attack vectors targeting the financial sector.
    - Analysis of real-world cyber incidents and case studies to learn from past experiences.
    - Monitoring and utilizing threat intelligence feeds and industry reports.
  - Penetration Testing and Ethical Hacking
    - Hands-on training on conducting penetration tests and vulnerability assessments.
    - Techniques for identifying and exploiting vulnerabilities in applications, networks, and systems.
    - Best practices for reporting and remediating discovered vulnerabilities.
  - Incident Response and Handling
    - Incident response planning, roles, and responsibilities during an incident.
    - Incident classification and escalation procedures.
    - Hands-on simulations of various incident scenarios and their resolution.
  - Threat Intelligence Analysis
    - Understanding different types of threat intelligence and their sources.
    - Analyzing threat data to identify potential risks and patterns.
    - Integrating threat intelligence into the organization's security infrastructure.
  - Secure Coding Practices
    - Secure coding principles and best practices (e.g., OWASP Top 10) for web and software developers.
    - Secure development frameworks and tools.
    - Conducting secure code reviews and code analysis.
  - Network Security
    - Designing and implementing secure network architectures.
    - Firewall management and rule configuration best practices.
    - Intrusion Detection/Prevention Systems (IDS/IPS) configuration and monitoring.
  - Data Protection and Encryption
    - Data classification and handling of sensitive information.

    - Understanding encryption algorithms and their applications.
    - Implementing data encryption at rest and in transit.
  - Cloud Security
    - Securing cloud services (IaaS, PaaS, SaaS) and understanding shared responsibility models.
    - Identity and access management in the cloud.
    - Monitoring and auditing cloud environments for security.
  - Security Tools and Technologies
    - Familiarization with SIEM tools for centralized event logging and correlation.
    - Antivirus, anti-malware, and endpoint protection solutions.
    - Intrusion Detection/Prevention Systems (IDS/IPS) configuration and use.
  - Compliance and Regulatory Training
    - Understanding relevant regulations such as GDPR, CCPA, and industry-specific compliance frameworks.
    - Ensuring data privacy and compliance with financial regulations (e.g., PCI-DSS).
  - Security Awareness and Training for Employees
    - Developing engaging cybersecurity awareness programs for employees.
    - Educating employees about phishing, social engineering, and other common attack vectors.
    - Regularly conducting simulated phishing exercises to measure awareness.
  - Threat Hunting
    - Techniques for proactive threat hunting and anomaly detection.
    - Using threat intelligence to hunt for potential threats and indicators of compromise.
  - Forensics and Incident Analysis
    - Understanding digital forensics methodologies and tools.
    - Conducting forensic analysis on compromised systems to determine the scope and impact of incidents.
  - Collaboration and Communication
    - Improving communication skills to effectively convey technical information to non-technical stakeholders.
    - Collaborating with other departments and teams for a coordinated security approach.
  - Red Team/Blue Team Exercises
    - Conducting simulated cyber warfare exercises with red team representing attackers and blue team representing defenders.
    - Analyzing the results to improve incident response and defense strategies.

- Team Tools: What are the latest cyber security tools and technologies we should use?
    - Endpoint Protection Platforms (EPP): EPP solutions protect individual devices, such as laptops and desktops, from malware, ransomware, and other threats. They often include features like antivirus, anti-malware, and behavioral analysis.
    - Next-Generation Firewalls (NGFW): NGFWs offer advanced firewall capabilities, including deep packet inspection, intrusion prevention, and application-aware filtering to better protect networks from sophisticated threats.
    - Security Information and Event Management (SIEM): SIEM tools collect and analyze log data from various sources across an organization's network, helping to detect and respond to security incidents.
    - Intrusion Detection and Prevention Systems (IDS/IPS): These systems monitor network traffic for suspicious activities and can either alert administrators (IDS) or automatically block malicious traffic (IPS).
    - Secure Email Gateways (SEG): SEGs help protect organizations from email-based threats such as phishing, spam, and malware by analyzing incoming and outgoing email traffic.
    - Data Loss Prevention (DLP): DLP solutions prevent sensitive data from being leaked or misused by monitoring and controlling data in use, in motion, and at rest.
    - Identity and Access Management (IAM): IAM tools ensure that the right individuals have access to the right resources at the right time, reducing the risk of unauthorized access.
    - Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring users to provide multiple forms of authentication before accessing sensitive data or systems.
    - Encryption Tools: Encryption solutions protect data from unauthorized access by converting it into unreadable code, which can only be decrypted with the appropriate keys.
    - Vulnerability Scanning and Management: These tools scan networks, systems, and applications to identify potential vulnerabilities, allowing organizations to remediate them before attackers can exploit them.
    - Web Application Firewalls (WAF): WAFs protect web applications from common cyber threats, such as SQL injection and cross-site scripting (XSS) attacks.
    - Threat Intelligence Platforms (TIP): TIPs collect, analyze, and disseminate threat intelligence to help organizations understand and respond to emerging threats.
    - Deception Technologies: Deception tools create decoy assets and traps to mislead and detect attackers within the network.
    - Security Orchestration, Automation, and Response (SOAR): SOAR platforms streamline incident response by automating repetitive tasks and facilitating collaboration among security teams.
    - Cloud Security Solutions: Tools specific to securing cloud environments, including cloud access security brokers (CASBs) and cloud workload protection platforms (CWPPs).

- Team Processes: Come up with a set of rigorous cyber security processes and procedures based on general domains of Cybersecurity.
  - Incident Response Process:
    - Incident Identification: Establish procedures to detect and identify security incidents promptly.
    - Incident Categorization: Classify incidents based on severity and impact to prioritize response efforts.
    - Incident Containment: Isolate affected systems to prevent further damage or data loss.
    - Incident Eradication: Identify and remove the root cause of the incident from the environment.
    - Incident Recovery: Restore affected systems and data to normal operation.
    - Incident Analysis: Conduct a post-incident analysis to understand the cause and improve future responses.
    - Incident Reporting: Report incidents to relevant stakeholders, regulatory bodies, and law enforcement if necessary.
  - Patch Management Process:
    - Patch Identification: Regularly scan systems and applications for missing patches and updates.
    - Patch Prioritization: Assess the criticality of patches based on severity and potential impact on the organization.
    - Patch Testing: Test patches in a controlled environment before deploying them in the production environment.
    - Patch Deployment: Schedule and deploy patches in a timely manner to address vulnerabilities.
    - Patch Verification: Verify that patches have been successfully applied and did not cause any adverse effects.
  - Access Control Process:
    - User Access Provisioning: Define procedures for granting access privileges to users based on the principle of least privilege.
    - Access Reviews: Regularly review and audit user access rights to ensure they align with job responsibilities.
    - Privileged Access Management: Implement strict controls for privileged accounts and administrative access.
    - Account Deactivation: Establish a process for promptly removing access privileges when users change roles or leave the organization.
  - Data Protection Process:
    - Data Classification: Classify data based on its sensitivity and criticality.
    - Data Encryption: Define policies and procedures for encrypting sensitive data in transit and at rest.
    - Data Handling and Retention: Establish guidelines for handling and retaining data in compliance with legal and regulatory requirements.
  - Security Awareness and Training Process:

    - Employee Training: Conduct regular cybersecurity awareness training for all employees to educate them about common threats and best practices.
    - Phishing Simulation: Regularly perform simulated phishing exercises to gauge employee susceptibility to phishing attacks.
    - Training Metrics and Evaluation: Measure the effectiveness of training programs and adjust them based on feedback and results.
  - Vulnerability Management Process:
    - Vulnerability Scanning: Conduct periodic vulnerability scans of networks and systems to identify potential weaknesses.
    - Vulnerability Assessment: Assess the impact and risk of identified vulnerabilities to prioritize remediation efforts.
    - Vulnerability Remediation: Establish a process for promptly addressing and patching discovered vulnerabilities.
  - Network Security Process:
    - Network Segmentation: Segregate networks and implement firewalls to limit lateral movement for attackers.
    - Network Monitoring: Deploy intrusion detection/prevention systems (IDS/IPS) to monitor network traffic for signs of suspicious activity.
  - Secure Software Development Process:
    - Secure Coding Standards: Implement coding practices that prioritize security and adhere to industry standards (e.g., OWASP Top 10).
    - Code Review: Conduct thorough code reviews to identify and remediate security vulnerabilities in software applications.
  - Third-Party Risk Management Process:
    - Vendor Assessment: Assess the cybersecurity posture of third-party vendors before engaging in business relationships.
    - Ongoing Vendor Monitoring: Continuously monitor third-party vendors for security compliance during the partnership.
  - Disaster Recovery and Business Continuity Process:
    - Business Impact Analysis: Identify critical systems and processes to prioritize recovery efforts.
    - Disaster Recovery Planning: Develop detailed plans and procedures to recover systems and operations in case of a major incident.
  - Cloud Security Process:
    - Cloud Access Controls: Define policies for secure access to cloud services and data.
    - Cloud Configuration Management: Establish procedures for securely configuring cloud resources.