Proposed Plan for Threat Intelligence Fusion Center

Summary of Threat Actors and Threats

APTs

APTs (Advanced Persistent Threats) are “Adversaries are typically well-funded, experienced teams of cybercriminals that target high-value organizations. They’ve spent significant time and resources researching and identifying vulnerabilities within the organization.” [1] Examples of these threats that can Target NVIDIA include nation-states (China) or even well-organized and funded cybercriminal gangs.

Cybercriminal Organizations

Cybercriminal Organizations are organizations that make a profit by committing cybercrimes. These organizations can be RaaS (Ransomware-as-as-Service), or even organizations that target certain companies. Some examples include the Conti Ransomware Group, Lazarus Gang, and the MageCart Syndicate. [2]

Insider Threats

Insider threats are typically threats that originate from the inside and can include any employees who work within an organization. This threat can both be accidental, or intentional. Examples include Disgruntled employees who purposely leak information, or even unintentional incidents such as falling for a social engineering attack.

Emerging Threats

Emerging threats are any new threats or tactics that have not been properly documented or explored yet. These threats can include zero-day exploits. They can even be on a broader level, such as AI or Quantum Attacks.

Hacktivists

Hacktivists are typically groups that oppose certain business practices or even partnerships. Examples of hacktivists include: The Anonymous group and LuLzSec. [3]

IRs AND PIRs

IR 1: Identify Threats to NVIDIA

PIR 1: Monitor unusual patterns of employees that indicate insider threats

PIR 2: Identify TTPs of potential external threat actors

IR 2: Identify APT’s that would target NVIDIA

PIR 3: Identify APT groups that are actively targeting semiconductor organization.

PIR 4: Identify APT TTP’s

IR 3: Identify threats to the NVIDIA supply chain

PIR 5: Identify potential disruptions in supply chain due to geopolitical incidents

PIR 6: Identify attacks that have recently impacted third party suppliers.

Data Sources

Data sources will include:

Internal:

- Logs from SIEM
- Access control logs
- User Behavior Analytics

External:

- Information Sharing and Analysis (ISAC’s, Information Sharing and Analysis Center)
- Government Agencies (an example: CISA)
- Dark Web Monitoring Services
- Vulnerability Databases

Threat Analysis Workflows

1. **Insider threat detection:** Track employee activity in the network to identify potential insider threats like unauthorized access to critical data and take appropriate action to prevent and mitigate an attack by escalating different degrees of breaches to the concerned departments.
2. **Identification of common TTPs used by a specific threat actor:** Gather data from various OSINT platforms for common TTPs used by threat actors. Once a TTP relevant to the industry is found, assess it to find the level of risk it poses to the company and take preventative measures accordingly.
3. **Identify and Track APTs:** Look for well-known APTs, assess their capabilities and TTPs, and proactively secure NVIDIA’s systems against these APTs.
4. **Monitoring for vulnerabilities present within the system:** Monitoring internal systems and external sources against a list of known CVEs that may affect NVIDIA’s tech stack. Patching vulnerabilities if found.
5. **Detection and response to Malware in the system:** Identify and respond to malware found in the system. Look for suspicious activity within the system and use end-point detection and threat intelligence tools to find malware if present. Roll-back to malware-free state if malware detected.

Strategic Analysis Workflows

1. **Identify and respond to threats from competitors:** Analyze the actions of competitors and be aware of their strategic moves and mode of operation. Use this information to predict potential attacks and their likelihood and take measures to defend and protect against them.
2. **Risk Assessment of Supply Chain:** Monitor for threat actor groups in areas of unrest near the supply chain facilities. Assess their capabilities and likelihood of attack.
3. **Identify the emerging threats and technologies:** Use different sources like the dark web, social media platforms, OSINT platforms, ISACs etc to find the general emerging trend in terms of TTPs and targets. Report this information to the C-suite to allow them to take necessary actions against it.
4. **Assess and forecast threats posed by Geopolitics:** Understand and track activities of nation-state hackers and come up with motives of why they would want to target NVIDIA keeping in mind the current political climate. Make plans to defend and mitigate prospective attacks accordingly.
5. **Assess Risks to Brand and Reputation:** Identify potential threats that could jeopardize NVIDIAs brand and reputation like being targeted by hacktivists for social and political reasons, threats to leaks of internal data and communication etc. Suggest strategies to mitigate the impact of these on public image and brand value.

Fusion Center Job Roles and Responsibilities

Since NVIDIA does not currently have a threat intelligence capability, we recommend 6 key job roles and their responsibilities that are essential to starting this Fusion Center.

1. **Threat Intelligence Analyst:** This person would be responsible for extracting data from different sources and generating intelligence about the threat landscape, the projected risks, the industry risks, competitor risks, and how geopolitics affect NVIDIA.
2. **Incident Responder:** This person is responsible for mitigating and recovering from an attack
3. **Vulnerability Analyst:** This person reviews the current systems and practices to find any vulnerabilities in the current systems and monitors for insider and external threats.
4. **SOC Analyst:** This person monitors and audits the company's systems and looks for indications of compromise within system. If present they work with the incident responder to mitigate threats.

5. **Fusion Center Manager:** This person is responsible for the smooth operation of activities in the fusion center. They are responsible for facilitating communication between different departments and ensuring that the activities of the fusion center align with their strategic goals.

Tools

Depending on the data sources used to gather information, we recommend using some or all of the following tools:

- **Elastisearch, Kibana & Logstash (ELK):** This is one of the most robust, feature-rich, and intuitive open-source SIEM tools that would make monitoring and logging easy. It is used by the US Department of Defense in their tech stack so it is reliable.
- **Splunk:** This SIEM Tool offers free and paid services that can be tailored to the needs of NVIDIA. This can also be used to get User Behaviour Analytics
- **Duo Security:** This is an access control tool that offers multi-factor authentication, passwordless authentication, and adaptive access policies and would allow NVIDIA to keep track of access permission given to different employees and monitor their login activity.
- **Teramind:** This is a user behavior analytics tool that can turn employee activity patterns into intelligence and help identify anomalous user behavior.
- **MS-ISAC Toolkit:** This provides a list of emerging trends and cybersecurity threats.
- **SpyCloud:** This is a cybercrime analytics tool that draws on data recaptured from the dark web to protect businesses from cyber attacks.
- **FireEye:** This is a vulnerability management tool that assists companies in responding to cyber threats.
- **Suricata:** This is an open-source IDS.
- **Argus:** This tool can be used for network analysis.

Monitoring Activities / Indicators to Track

1. Constant access control and network monitoring. Indicators of threat to look out for include:
    - Unusual time of login to certain systems (ex. MES system, usually no one will log in to manufacturing-related systems during weekends)
    - Unusual number of login or access attempts monitored
    - Suspicious origin IP and destination
2. Constant virus and malware tactics detection. Indicators of threat to look out for include:

   - The type of virus or malware detected. It might give clues about who is attempting the attack.
   - The complexity of viruses or malware.
   - The origin of the virus or malware. It provides clues of what could have been compromised within the IT infrastructure.
3. Regular monitoring of dark web activities through SpyCloud. Activities detected through the tool could provide indicators such as:
   - The information was compromised. NVIDIA could later implement mitigating controls on where the information originates.
   - The suspected cyber-criminal.
4. Alerts and Threat Indicators Gathering. AIS gathered from ISACs should provide indicators of potential threats.
5. Regular monitoring of vulnerabilities.

Collaboration Partners

Suppliers and OEMs
NVIDIA outsources the manufacturing of its products to several original equipment manufacturers (OEM), including Taiwan Semiconductor Manufacturing Company (TSMC) and Foxconn. NVIDIA also builds its internal IT infrastructures, such as servers, cables, cloud services, and computers, with many third-party suppliers. To ensure no supply chain attacks would occur within NVIDIA's supply chain, NVIDIA should have service level agreements (SLAs)and collaborate with its OEMs and suppliers.

Information Technology Sector Coordinating Council and Cyber Information Sharing and Collaboration Program (CISCP) [4] [5]
According to CISA's definition of The Information Technology (IT) Sector, one of the critical infrastructure sectors in the US, NVIDIA could be classified as one of the organizations within the sector. NVIDIA should collaborate with the Information Technology Sector Coordinating Council or gain shared information about the industry from other organizations through CISA's CISCP program or IT-ISAC to come up with sector-specific strategies against cyber attacks.

The QIR Alliance [6]
The QIR Alliance is an organization NVIDIA is a part of that focuses on the development and standardization of quantum computing. NVIDIA should also collaborate with companies in the alliance to design quantum computing services with security integrated in the very beginning.

Plan for insider threats & protect employees from social engineering

Social Engineering Training Program

As a valuable target for cybercriminals, NVIDIA remains vulnerable to phishing emails either from big cyber gangs such as state-sponsored cyber units or from individuals such as disgruntled employees. The most effective way to protect the company from any form of social engineering tactics is through raising awareness of their employees through a thorough social engineering training program, helping them identify common social engineering methods and understand what to do if accidentally fall victim to an attack. NVIDIA should:

1. Require new employees to complete online training plus a quiz within 2 weeks of onboarding.
2. Require all employees to complete refresher training plus a quiz semi-annually.
3. Send occasional fake phishing emails on a quarterly basis. Those who fall for the fake emails are required to complete additional training within a week.
4. Hold occasional cyber awareness events, such as a lottery for employees completing a quiz, to not only raise awareness but also increase employees' interest.

Restricted Data Transfer and Ongoing Monitoring of Employee Activities

NVIDIA should implement several restrictions on data transfer to prevent confidential data leakage. For instance:

1. Employees are not allowed to install any social media apps on company laptops, and transferring data through external tools (ex. Gmail, Google Drive, Facebook) should be automatically banned by tools.
2. If confidential data transfer is needed (ex. to suppliers, to clients, to business partners etc.), employees should only use company permitted methods for transfer, such as using a monitored cloud environment.
3. Usage of USB should be restricted; employees should not be allowed to transfer data out to a USB.
4. All emails are monitored by the network administrator. If any email is suspected to be transferring confidential data to a suspicious IP, an alert should be immediately triggered and investigated.
5. Reports of phishing emails should be constantly monitored to further implement prevention controls.

Reporting

Vulnerability Reports

Vulnerability reports record discovered vulnerabilities in NVIDIA's IT infrastructure. The vulnerabilities could be discovered through regular vulnerability scanning, regular penetration testing, or published CVEs.

Report process:

Junior System Administrators (including database administrators) → Senior System Administrators (including senior database administrators) → Infrastructure Team Manager

Patch Status Reports
Patch status reports record how each vulnerability is patched. Patch status reports could be combined with vulnerability reports.
Report process:
Junior System Administrators (including database administrators) → Senior System Administrators (including senior database administrators) → Infrastructure Team Manager

Threat Analysis Reports
Threat analysis reports include threat actors and threat actor TTPs for each attempted cyber attack or incident identified through various tools, including firewall traffic logs, system logs, EDR alerts, and phishing email reports. The threat analysis report is a collaborative effort of different IT teams.
Report process:
Junior Network Administrators, System Administrators → Senior Network Administrators, System Administrators → Infrastructure Team Manager → Malware Analysts → Cyber Intelligence Manager → CIO and CISO

Future Threat Analysis Reports
Future threat analysis reports, similar to threat analysis reports, also include threat actors and threat actor TTPs. However, it focuses on anticipating who the future threat actors will be and how they will attack NVIDIA. The report information is collected through incidents from ISACs or news and analysis by systems security analysts.
Report process:
Junior Network Administrators, System Administrators → Senior Network Administrators, System Administrators → Infrastructure Team Manager → Malware Analysts → Cyber Intelligence Manager → CIO and CISO

Executive Reports
Executive reports are intended for the CIO and the CISO. The report contains a summary of the efforts done, risks identified and mitigated, and challenges yet to be solved about the cybersecurity domain of NVIDIA. The report should at least be reported quarterly to keep the CIO and CISO up to date.
Report process:
Infrastructure Team Manager → Software Development Team Manager → Cyber Intelligence Manager → CIO and CISO