LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

Level 7 – Threat Intelligence Life Cycle

(Electro Plus Company)

Assessment Type

60% Individual Coursework

Semester

2025 Summer

Credit: 20 Semester Long Module

Student Name: Abhiyan Shrestha

London Met ID: 24059497

College ID: np01ms7s250025

Assignment Due Date: Tuesday, July 8, 2025

Assignment Submission Date: Wednesday, August 20, 2025

Submitted To: Basudev Raut

Word Count (Where Required): 3,947

I confirm that I understand my coursework needs to be submitted online via MySecondTeacher classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

np01ms7s250025 Abhiyan Shrestha - Copy.docx

Islington College,Nepal

Document Details

Submission ID
trn:oid:::3618:108527675

Submission Date
Aug 16, 2025, 11:43 AM GMT+5:45

Download Date
Aug 16, 2025, 11:44 AM GMT+5:45

File Name
np01ms7s250025 Abhiyan Shrestha - Copy.docx

File Size
27.0 KB

18 Pages

3,947 Words

23,265 Characters

3% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

- 11 Not Cited or Quoted 3%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

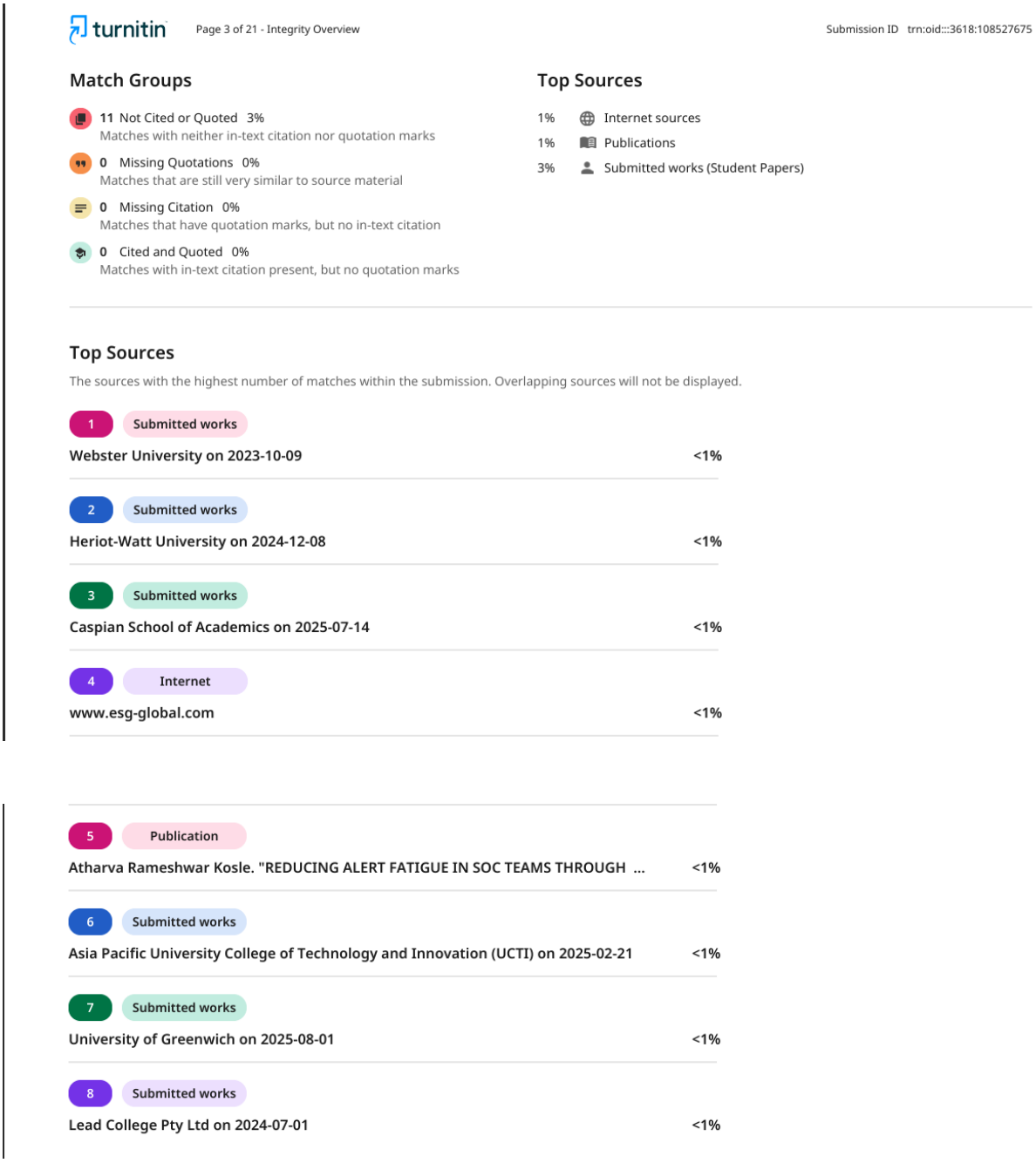
1% Internet sources
1% Publications
3% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.



turnitin Page 3 of 21 - Integrity Overview Submission ID trn:oid:::3618:108527675

Match Groups

- **11** Not Cited or Quoted 3%
  Matches with neither in-text citation nor quotation marks
- **0** Missing Quotations 0%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

1% Internet sources
1% Publications
3% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1 Submitted works
Webster University on 2023-10-09 <1%

2 Submitted works
Heriot-Watt University on 2024-12-08 <1%

3 Submitted works
Caspian School of Academics on 2025-07-14 <1%

4 Internet
www.esg-global.com <1%

5 Publication
Atharva Rameshwar Kosle. "REDUCING ALERT FATIGUE IN SOC TEAMS THROUGH ... <1%

6 Submitted works
Asia Pacific University College of Technology and Innovation (UCTI) on 2025-02-21 <1%

7 Submitted works
University of Greenwich on 2025-08-01 <1%

8 Submitted works
Lead College Pty Ltd on 2024-07-01 <1%

Abstraction

Threat Intelligence Program (TIP) for Electro Plus Company is a comprehensive, strategic program for defeating phishing assaults on corporate mobile phones. It aims to transform the company's security posture from reactive, ad-hoc to proactive, data-informed defence.

Program development begins with the gap analysis to identify gaps in current security, followed by specifying well-articulated objectives focusing on the reduction of risk and enhanced incident response. It constitutes a cross-functional team and establishes an orderly process of gathering intelligence from open-source, commercial, and internal sources. The intelligence is ranked, analysed, and incorporated seamlessly into every stage of the incident response playbook. An integral component is continuous, targeted security training for employees, supplemented by metrics (KPIs) to measure the efficacy of the program as well as maintain it in constant refinement. The TIP is, ultimately, warranted as an essential investment to mitigate significant financial and reputational costs.

Table of Contents

Introduction

The Electro Plus Company Threat Intelligence Program (TIP) is a strategic initiative to advance the cybersecurity posture of the enterprise via the proactive identification, examination, and neutralization of threats, including phishing attacks targeting corporate mobile phones, tablets, and laptops (networks, n.d.). These are primary compromise vectors in today's online ecosystem, and a mature, dedicated threat intelligence capability is essential. This whitepaper outlines the building blocks, operational processes, and strategic objectives of the TIP, ensuring a systematic and continuous approach to security that transitions from reactive incident response to proactive, predictive defense (networks, n.d.).

The program structure is guided by industry's best practices and the intelligence life cycle, rendering it a living, breathing entity that stays in line with the changing face of cyber threats (networks, n.d.). With clear objectives, roles, and procedures, the TIP will enable Electro Plus to make data-driven security decisions, anticipate adversary behavior, and harden its defenses against the most relevant and viable threats (networks, n.d.). The following sections trace the development of the program, from the preliminary gap analysis to ongoing improvement, to develop a step-by-step roadmap for success (networks, n.d.).

Fig: Electro Plus Company Logo

1. Gap Analysis

1.1. Current State vs. Desired State

A thorough gap analysis is the necessary starting point for building a strong TIP. It involves a review of the existing security position of Electro Plus Company and an identification of gaps between existing capability and the desired state a mature, proactive, and data-driven security program that is compliant with industry's best practices and organizational needs.

1.2. Current State

The existing security posture of Electro Plus Company is, to a great extent, reactive and lacks an organized, formal threat intelligence capability. While minimal security controls, such as endpoint protection and email filtering, have been implemented, they are operating in a disconnected and siloed manner. The company's focus is primarily reacting to incidents post-facto, e.g., when a user complained about suspicious email or when a device was compromised.

- Inadequate Proactive Threat Detection: There is no established process for gathering intelligence on emerging phishing attacks, techniques, or indicators of compromise (IoCs) for the company's sector or mobile platforms. The company relies on public disclosures and vendor notifications that are generic and not specific to its own unique threat environment.

- Limited Threat Data Sources: Threat information is primarily limited to internal logs and alerts from security tools. The company lacks commercial threat feeds, and it does not join regular industry-specific information-sharing groups (ISACs/ISAOs) to gain broader visibility into shared threats.

- Ad-Hoc Analysis: Ad-hoc threat analysis is handled by the IT support staff without any training in threat intelligence. There is no official data enrichment process, internal activity correlation with external threat data, or the generation of products of actionable intelligence.

- Poor Incident Response: The incident response is reactive. Once a phishing attack is found, the team scrambles to respond to the immediate threat without pre-existing intelligence. This leads to a longer mean time to detect (MTTD) and mean time to respond (MTTR) since the team must examine each new incident from scratch.

- No Central Knowledge Base: There is no central place to keep and share threat information. Experience learned from previous attacks is lost or not adequately shared, leading to repeated vulnerabilities and inability to develop institutional knowledge.

- Untrained User Base: End-user security awareness training is generic and ad-hoc. They lack domain-specific training on how to identify sophisticated phishing attempts, particularly on smartphones where the user interface might be less intuitive in identifying malicious links or spoofed sender domains.

1.3. Desired State

The desired state for Electro Plus Company is a fully mature TIP that will transform the organization from a reactive to a proactive security posture. The program will be an integral component of the overall cybersecurity strategy, providing timely, pertinent, and actionable intelligence to all stakeholders.

- Active Threat Hunting: The program will venture out and collect, analyze, and enhance threat data to predict and prepare attacks beforehand. This includes the prediction of phishing trends, identifying evolving TTPs (Tactics, Techniques, and Procedures), and defining customized IoCs relevant to mobile and laptop systems.

- Multifaceted and Customized Information Sources: The TIP will draw on a wide range of sources of intelligence, such as open-source intelligence (OSINT), commercial feeds, and industry-specific sharing groups to compile a holistic understanding of the threat environment.

- Structured Prioritization and Analysis: A designated team will perform structured analysis using frameworks like the Diamond Model or the Cyber Kill Chain to develop bespoke intelligence products. The threats will be prioritized on the basis of a clear and consistent set of criteria meaningful for the company's business operations and assets.

- Seamless Integrated Incident Response: Threat intelligence shall be natively integrated into every phase of the incident response playbook. This will enable faster detection, improved containment, and a more effective recovery process.

- Centralized Threat Knowledge Management: Centralized management of and sharing of threat intelligence by one platform shall enable all teams to have access to the same, up-to-date information.

- Targeted Training and Sensitization: The program will feature continuous, targeted security awareness training with simulated phishing attempts specifically for mobile and laptop users.

The difference between wished-for state and existing state is significant, which mirrors the need for a massive TIP that addresses critical gaps in threat anticipation, threat analysis, and response to incidents. The program is an addition and not an upgrade but a full turnkey shift in the cybersecurity program of the organization.

2. Development of the TIP Program

2.1. Define Objective and Scope

The main goal of Electro Plus Company TIP is to safeguard its corporate devices laptops, tablets, and mobile phones from phishing attacks that seek unauthorized control. The scope of the program is established by the following strategic and tactical objectives:

- Strategic Objectives:
  - Proactive Risk Reduction: To decrease the overall risk of a successful phishing attack on corporate devices by at least 50% in the first year of the program's existence.
  - Enhanced Incident Response: To minimize the average mean time to detect (MTTD) and mean time to respond (MTTR) for phishing attacks by 40% through the delivery of timely actionable intelligence.
  - Enhanced Security Posture: To transition the organization's security posture from reactive to proactive, wherein the security team would be able to anticipate and prepare for future threats rather than simply reacting to them.
- Tactical Objectives:
  - Collect and Analyze Phishing Data: To gather and in a structured manner analyze the threat data, e.g., IoCs (malicious URLs, domain names, sender IPs), TTPs, and current social engineering lures used in phishing campaigns.
  - Produce Actionable Intelligence: To create and disseminate timely and relevant intelligence products to the security operations center (SOC), IT, and management.
  - Raise User Awareness: Implement a continuous training and awareness program that significantly improves employees' ability to identify and report phishing incidents.

- Scope: The TIP will only address threats to corporate devices: laptops, tablets, and cell phones. The initial threat focus is phishing attacks. The program will cover all stages of the intelligence lifecycle, from planning to collection to dissemination and feedback, and will be integrated with the security tools and processes already established within the company.

2.2. Establish a Cross-Functional Team – RACI Matrix

Well-coordinated and defined roles and collaboration are essential for effective TIP. A cross-functional team with participation from IT, cybersecurity, legal, and business groups is also vital. Below is an RACI matrix that defines the responsibilities for key activities for TIP.

Table 1: Threat Intelligence Program RACI Matrix

Activity	Threat Intelligence Analyst	SOC Analyst	IT Administration	Legal & HR	CISO/Management
Gap Analysis & Planning	C	I	I	I	R, A
Define Objectives & Scope	C	C	I	C	R, A
Threat Data Collection	R, A	I	I		
Threat Data Analysis	R, A	C	I		
Incident Response Integration	R, A	R, A	C		C
Disseminate Intelligence	R, A	I	I	I	C
Threat Awareness Training	R, A	C	C	C	C

Program Evaluation & Reporting	C	I	I	I	R, A

R: Responsible (performs the task), A: Accountable (is ultimately answerable for the correct completion), C: Consulted (provides input), I: Informed (is kept up-to-date on progress).

2.3. Identify Information Sources

The effectiveness of the TIP has to do with the variety and quality of its threat data sources. Adopting the lead of phishing of laptop and mobile devices, a multi-layered collection strategy is required.

Open-Source Intelligence (OSINT):

- Reason: OSINT is an affordable but powerful starting point. It provides an overall view of the threat landscape and is a fundamental skill learned in the majority of cybersecurity labs.

- Sources: Threat intelligence blogs (e.g., KrebsOnSecurity), security news websites, open-source IoC repositories (e.g., AlienVault OTX), and public lists of phishing domains.

- Lab-based Tools: Utilities like Virus Total, likely used within a lab setting, are excellent at analyzing the reputation of URLs and files associated with phishing emails. whois is also a command-line tool that can be used to extract domain registration data for checking suspicious domains.

Commercial Threat Intelligence Feeds:

- Justification: Commercial feeds provide pre-analyzed, high-quality, and automated IoCs. They are more comprehensive and timely than OSINT can be, which is critical in real-time blocking of rapidly moving phishing campaigns.

- Sources: Vendors' feeds like CrowdStrike, Mandiant, or Anomali who specialize in phishing intelligence and provide targeted IoCs suitable for mobile platforms.

Industry Information Sharing & Analysis Centers (ISACs):

- Rationale: ISACs facilitate information peer-to-peer sharing within one's line of business. It is sharing information with other companies facing the same threats that provides a specific and highly relevant source of intelligence. For Electro Plus, an ISAC in either retail or finance would be quite helpful as both industries are common targets for phishing.

Internal Data:

- Justification: The most pertinent source is internal data, which captures threats actively targeting the firm. Examination of internal logs gives a baseline and puts external intelligence into context.

- Sources: Corporate laptops and mobile devices' EDR logs, email gateway logs, and phishing emails reported by users.

2.4. Collect and Process Threat Data

Automated and manual collection of data will be provided to assure extensive coverage.

- Collection:
    - Automated: Bury commercial threat feeds directly into the SIEM (Security Information and Event Management) or other security tools. Use automated scripts to gather data from OSINT repositories. Automate the email gateway to forward suspicious emails automatically to a sandbox for analysis.
    - Manual: The Threat Intelligence Analyst will proactively scan OSINT sources, participate in ISAC forums, and scan user-submitted phishing emails for fresh IoCs.
- Processing:
    - Normalization: Normalize collected data into a format that can be tool-compatible (e.g., STIX/TAXII).
    - De-duplication & Enrichment: De-duplicate duplicate IoCs and provide additional context to the remaining data, e.g., whois data for suspicious domains or geolocational data for IP addresses.

2.5. Analysis and Prioritize Threats

Threats will be analyzed and ranked with a good and transparent framework to focus limited resources on the most important threats.

Criteria for Threat Prioritization:

- Relevance: Is the threat specifically attacking our assets (laptops, mobile phones, tablets)? Is it a phishing attack?
- Impact: If successful, what would be the impact of the business (operational, reputational, financial)? We will use a score of 1 (Low) to 5 (Critical).
- Probability: Based on external intelligence and internal data, how likely is it that this threat will successfully breach a device? (1=Low, 5=Very Likely).
- Defend ability: Is there definable, concrete action we can take to defend against this threat?
- Timeliness: Is this an active, new, or highly virulent campaign which requires urgent attention?

Example Prioritization

A new phishing attack targeting the employees of a big electronic store chain (e.g., Electro Plus) with a very credible phony internal memo lure would be given top priority. It scores high in Relevance, Likelihood (since it is extremely convincing), and Impact (potential data compromise).

2.6. Threat Intelligence Sharing

Sharing intelligence is important for both internal defense and external collaboration.

- Internal Sharing:
    - Platform: Use a central platform (e.g., a particular channel in the company's chat tool or a secure wiki) to post intelligence reports, IoCs, and threat notifications.
    - Audience: The SOC team receives real-time IoCs, IT admin receives config recommendations, and management receives high-level executive briefs.
- External Sharing:
    - ISACs: Participate in sector-specific ISACs in order to exchange threat data de-identified and receive intelligence from peers. This is a collective defense.
    - Law Enforcement: Report critical incidents and threat information to relevant law enforcement agencies in the case of a crime having been committed.

2.7. Incident Response Integration

Threat intelligence is not a standalone function; it is an incident response force multiplier. TIP will be integrated into all facets of the Incident Response Playbook to accelerate detection, containment, and recovery.

Table 2: Threat Intelligence Integration with Incident Response Playbook

IR Phase	Threat Intelligence Contribution	Examples of Phishing Attacks
Preparation	Provides intelligence to inform and harden security controls. Develops threat profiles and trains the team on common TTPs.	Intelligence identifies that a new phishing kit is using. xyz domains. The team proactively adds a block rule for this TLD at the email gateway.
Detection & Analysis	Provides IoCs to enable rapid detection. Helps analysts enrich alerts by providing context (e.g., threat actor information).	An email alert is triggered. Threat intelligence instantly provides context: this malicious URL is linked to a known actor group using the same TTPs that were previously reported by an ISAC.
Containment	Provides specific mitigation steps and recommended actions based on threat actor TTPs.	Intelligence reports that the phishing lure uses a specific URL structure. The team can quickly contain the threat by blocking all URLs matching that pattern, not just the one in the initial alert.

Eradication	Provides intelligence on how the threat was delivered and the actor's post-exploitation goals. Help the team understand the full scope of the compromise.	The intelligence report on the phishing kit reveals that it drops a specific type of malware. The team uses this information to scan all devices for the specific malware signature to ensure all traces are removed.
Recovery	Provides data on the attacker's TTPs and the initial access vector to help validate that all vulnerabilities have been patched and the system is clean.	The intelligence team confirms that the phishing actor is no longer active in the company's network and that the initial phishing URL is no longer functional. This helps the team validate that the recovery is successful.
Post-Incident Activities	Contributes to the post-incident review by analyzing the intelligence that was missing or what could have been collected to prevent the attack.	The team analyzes the phishing email and determines that a new, more sophisticated lure was used. This new information is fed back into the TIP to update the threat profile and train employees on the new threat.

2.8. Continuous Monitoring and Feedback

Threat intelligence isn't a process for one-time effort but rather a continuous cycle. A TIP will include a feedback loop to ensure that its content stays relevant and active.

- IR Feedback: They will give feedback on the quality, relevance, and timeliness of the intelligence passed to the security team during an incident.

- Source Assessment: The threat intelligence sources will be constantly assessed for their relevance and worth.

- Performance Metrics: The performance of the program will be tracked against its KPIs to determine areas for enhancement.

2.9. Reporting and Communication

Effective communication is key to the success of the TIP. There will be multiple reports for different audiences.

- Strategic Reports: CISO/Management Level, non-technical analysis of the most critical threats to the program, the effectiveness of the program, and recommendations for resource allocation.

- Tactical Reports (for SOC/IT): Detailed intelligence bulletins with IoCs, TTPs, and specific mitigation recommendations.

- Operational Reports (for the TIP Team): Detailed analysis of threat data, source performance, and progress toward objectives.

2.10. Continuous Improvement

The TIP will apply a "lessons learned" approach. The team will review the program's performance after each significant event or at a fixed time interval (e.g., quarterly). This includes:

- Evaluating the timeliness and correctness of intelligence.
- Assessing the effectiveness of the training program.
- Checking the collection sources and the prioritization factors for relevance.

2.11. Compliance and Legal Considerations

The program will be operated in full compliance with all relevant laws and regulations, including GDPR and any sectoral data privacy law.

- Data Privacy: The threat data accumulated will be kept in strict confidentiality adhering to stringent data privacy policies.

- Ethical Considerations: The system will be subject to a strict code of ethics, whereby intelligence-gathering operations will be within the law and will not infringe user privacy.

- Legal Counsel: Both Legal and HR departments will be consulted in all aspects of the program, particularly in handling user-reported phishing data that may contain personally identifiable information (PII).

2.12. Training and Awareness

A well-educated employee is the first line. The TIP will oversee an in-depth training and awareness program.

- Training Plan:
  - Preliminary Onboarding Training: Mandatory for all new employees on phishing attempt identification, with specific focus on the specific vulnerabilities of mobile devices.
  - Routine Phishing Simulations: Execute monthly, randomized phishing simulation campaigns to test user resistance. These simulations will be realistic and threat-sophisticated (e.g., imposter internal IT notices, package delivery reminders).
  - Gamified Learning: Implement a gamified platform to incentivize employees for effective identification and reporting of phishing emails.
  - Focused Micro-learning: Provide short, bite-sized video clips or articles (e.g., on an intranet) on focused, recently discovered phishing tactics.

- Awareness:
  - Communication: Use multiple channels (email, intranet, team chat) to share new threats and best practices.
  - Leadership Buy-in: Rally the support of the leadership to speak on behalf of the importance of security awareness, setting the example for the rest of the company.

Table 3: Training and Awareness Plan

Component	Description	Frequency	Audience
Initial Onboarding Training	Mandatory session covering phishing recognition, mobile device security, and company reporting procedures.	Once, during new employee onboarding.	All new hires.
Regular Phishing Simulations	Realistic, tailored email simulations designed to test and improve employee resilience against phishing.	Monthly	All employees with email access.
Gamified Learning	Interactive platform for identifying and reporting phishing attempts, with points and rewards.	Ongoing	All employees.
Targeted Micro-learning	Short video clips or articles on newly identified phishing techniques.	Ad-hoc, as new threats emerge.	All employees.
Communication	Multi-channel messaging (email, intranet, chat) on new threats and best practices.	Continuous, as needed.	All employees.
Leadership Buy-in	Senior leadership champions security awareness and participates in training and communication.	Continuous	All employees (through leadership example).

2.13. Program Evaluation and Metrics

The effectiveness of the TIP will be measured using key performance indicators (KPIs).

Table 4: Threat Intelligence Program KPIs

KPI	Description	Target
Phishing Click Rate	The percentage of employees who click on a malicious link in a simulated phishing email.	Less than 5%
User Reporting Rate	The percentage of employees who correctly report a simulated phishing email.	Greater than 90%
MTTD for Phishing Attacks	The average time from a phishing email's arrival to its detection by the security team.	Less than 10 minutes
MTTR for Phishing Attacks	The average time to fully contain and eradicate a phishing attack.	Less than 1 hour
Coverage of Threat Sources	The percentage of critical threat sources that are actively monitored.	100%
False Positive Rate	The percentage of legitimate emails incorrectly identified as phishing by the security tools.	Less than 0.1%

2.14. Final Justification for TIP

The implementation of an official Threat Intelligence Program is a necessity, not an extravagant, for Electro Plus Company. The current reactive security model puts the organization at great risk for phishing attacks, which are escalating in sophistication. The financial, reputation, and business costs of a single successful data breach because of a phishing attack loss of customer data, legal fines, and business interruption are much higher than the cost of this program.

The suggested TIP provides an institutionalized, proactive, and evidence-based defense. It will not merely enhance the company's ability to meet current threats but also build an institutional capacity to deal with evolving ones. By incorporating intelligence into every security consideration, ranging from educating the users to responding to incidents, the TIP will make the organization more secure and resilient.

3. Critical Analysis

3.1. Final Justification of the Proposed TIP Program

The Electro Plus Company Threat Intelligence Program recommended here is a highly valuable investment for several main reasons. To start, the program directly addresses the largest and most prevalent threat to the company: phishing. Phishing is a primary initial vector for most cyber incidents, and through addressing this threat, the program addresses the origin of most potential incidents. The exclusive focus on corporate laptops, tablets, and mobile devices is also critical, as these devices are less secure and more susceptible to social engineering and present a clear and present danger to the company's information.

Secondly, the TIP shifts the security mindset from reactive to proactive. Instead of waiting for the attack to happen and then responding, the program enables the security team to anticipate and prepare against threats. This is not a hypothetical benefit; it is translated into tangible benefits, such as a better likelihood of evading successful attacks and faster incident response time. The proposed program's integration of threat intelligence into every stage of the Incident Response Playbook ensures that the security team has the knowledge required to respond quickly and effectively when an incident occurs.

Finally, the program is structured on a cycle of continuous improvement and measurable outcomes. The set KPIs provides an evident way of measuring the effectiveness of the program as well as demonstrating its return on investment to management. Ongoing training, feedback loops, and cross-functional staff keep the program current, useful, and targeting the company's evolving requirements. The proposed TIP is a strategic and vital component of modern-day cybersecurity policy, protecting not just the company's information but also its reputation and financial health.

3.2. Suggestion and Recommendation to Fill the Gap

The proposed TIP is designed to address the gaps identified in the initial analysis. Each component of the program directly addresses a weakness in the firm's current, reactive approach.

- Gap: Lack of Proactive Threat Identification

  How the TIP Fills It: By systematic exploration and leveraging of diverse sources of information (OSINT, commercial feeds, ISACs), the program will move away from generic news announcements to proactive gathering of tailored intelligence. The intelligence will be analyzed to predict and prepare against deliberately targeted phishing attacks, rather than waiting for them to become known.

- Gap: Restricted Threat Data Sources

  How the TIP Closes It: The collection strategy of the program demands the use of a combination of sources, including commercial feeds and ISACs, previously unavailable. This will provide richer, more timely, and more pertinent data to analyze, providing the company with a 360-degree view of the phishing threat space.

- Gap: Ad-Hoc Analysis

  How the TIP Fills It: The TIP establishes a particular function (Threat Intelligence Analyst) and formal process for analysis. Criteria for prioritization established within the program will lead to analysis focused on the greatest threats, and the product will be actionable intelligence and not raw data.

- Gap: Ineffective Incident Response

  How the TIP Fills It: Through the addition of intelligence to the Incident Response Playbook, the TIP provides the IR team with critical context both before, during, and after an incident. Intelligence before an incident will prevent attacks from being made, and post-incident analysis will aid in refining the program.

- Gap: Untrained User Base

  How the TIP Plugs It: The comprehensive training and awareness program directly tackles this shortcoming. The initiative exceeds generic training to provide targeted, continuous, and game-style learning that is directed squarely at phishing, including vulnerabilities from mobile devices. Phishing simulations are practical measures to test employee strength in real life and identify areas where more training is necessary.

  In short, the Threat Intelligence Program proposed in this paper is a strategic one that addresses methodically every gap discovered. By shifting from reactive to proactive defense, the Electro Plus Company will not only be safer from phishing attacks but will also build a strong and intelligent security culture. The program provides a clear path towards a more advanced security posture, protecting the organization's assets, information, and reputation for the long term.

References

networks, p., n.d. *paloalto networks.* [Online]
Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-the-threat-intelligence-life-cycle