# HOW TO PREPARE A THREAT INTELLIGENCE REPORT WITH EXAMPLE (BANKING & HEALTH)

BY IZZMIER IZZUDDIN

## 1. Define Objectives and Scope

- **Set Objectives:** Determine what you aim to achieve with the threat intelligence report (e.g., identifying vulnerabilities, detecting threats, improving defences).
- **Define Scope:** Establish the boundaries of your investigation, such as focusing on specific types of data (e.g., expired certificates, dark web mentions) and specific threats (e.g., phishing, ransomware).

## 2. Data Collection

- **Internal Sources:**
  - **Collect SSL Certificate Data:** Use tools like Qualys SSL Labs or internal monitoring systems to identify expired or soon-to-expire certificates.
  - **Gather Log Data:** Collect logs from firewalls, IDS/IPS, SIEM systems, and endpoint protection solutions.
- **External Sources:**
  - **Dark Web Monitoring:** Use dark web monitoring tools or services such as Recorded Future, DarkOwl, or Digital Shadows to search for mentions of your organization.
  - **Threat Intelligence Feeds:** Subscribe to threat intelligence feeds from providers like AlienVault OTX, VirusTotal, or Cisco Talos.
  - **OSINT Tools:** Utilize open-source intelligence tools like Shodan, Maltego, or OpenVAS for additional data collection.

## 3. Data Processing

- **Normalization:** Standardize the collected data into a consistent format for easier analysis.
- **Enrichment:** Add context to raw data. For example, associate IP addresses with known threat actors or geographical locations.
- **De-duplication:** Remove duplicate entries to ensure clean datasets.

## 4. Analysis

- **Expired Certificates:**
  - **Identify Expired Certificates:** Use your certificate monitoring tools to list expired or soon-to-expire certificates.
  - **Assess Impact:** Evaluate the potential impact of these expired certificates on your organization’s security.
- **Dark Web Mentions:**
  - **Search for Mentions:** Use your dark web monitoring tools to find mentions of your organization or related keywords.
  - **Analyse Data:** Determine the type of data being sold or discussed (e.g., user’s records, credentials).
- **Phishing Campaigns:**
  - **Identify Campaigns:** Use email security solutions to detect phishing emails targeting your staff or users.

    - **Analyse Tactics:** Understand the methods used by attackers, such as spoofed email addresses or fake login pages.
- **Ransomware Activity:**
    - **Detect Infections:** Use endpoint protection and SIEM systems to identify ransomware infections.
    - **Analyse Patterns:** Investigate how the ransomware was delivered (e.g., malicious email attachments, compromised RDP).
- **Vulnerabilities:**
    - **Identify Vulnerabilities:** Use vulnerability management tools to detect new vulnerabilities relevant to your software and systems.
    - **Assess Severity:** Evaluate the criticality of these vulnerabilities and their potential impact on your systems.

**5. Production**

- **Create Reports:** Compile your findings into a detailed report, including sections on expired certificates, dark web mentions, phishing campaigns, ransomware activity, and new vulnerabilities.
    - **Use Templates:** Employ a standardized template to ensure consistency and comprehensiveness.
    - **Tailor for Audience:** Prepare executive summaries for management and detailed technical sections for IT/security teams.

**6. Dissemination**

- **Internal Distribution:**
    - **Share Reports:** Distribute the report to relevant stakeholders within the organization.
    - **Conduct Briefings:** Hold briefings or meetings to discuss the findings and necessary actions.
- **External Sharing:**
    - **Collaboration:** Share relevant findings with industry peers, ISACs, and other organizations if appropriate.

**7. Response and Mitigation**

- **Incident Response:**
    - **Phishing and Ransomware:** Use threat intelligence to enhance your incident response processes. For phishing, implement better email filtering and educate users. For ransomware, ensure backups and incident response plans are robust.
- **Expired Certificates:**
    - **Renew Certificates:** Immediately renew any expired SSL certificates.
    - **Implement Management System:** Use a certificate management system to prevent future expirations.
- **Dark Web Monitoring:**
    - **Notify Affected Parties:** Inform users or staff whose data has been compromised.
    - **Enhance Security Measures:** Increase monitoring and implement stronger access controls.

- **Vulnerability Management:**
  - **Patch Management:** Apply patches for critical vulnerabilities as soon as they are available.
  - **Configuration Reviews:** Regularly review and update system configurations to follow best security practices.

**8. Feedback and Improvement**

- **Evaluate Effectiveness:**
  - **Gather Feedback:** Collect feedback from stakeholders on the usefulness of the report and the effectiveness of the implemented measures.
  - **Measure Impact:** Evaluate how well the threat intelligence has mitigated risks and improved security posture.
- **Iterate and Improve:**
  - **Refine Processes:** Continuously improve your threat intelligence processes based on feedback and evolving threats.
  - **Update Tools:** Keep your tools and methodologies up to date with the latest developments in threat intelligence.

**9. Compliance and Legal Considerations**

- **Ensure Compliance:**
  - **Regulations:** Ensure that all threat intelligence activities comply with relevant laws and regulations (e.g., GDPR, HIPAA).
  - **Documentation:** Keep thorough records of your threat intelligence activities for compliance and auditing purposes.
- **Legal Consultation:**
  - **Consult Experts:** Work with legal experts to navigate any legal implications, especially when dealing with data from external sources or the dark web.

**Example 1: Banking Sector**

**Threat Intelligence Report for Izzmier Banking Berhad**

**Date:** 30 June 2024
**Prepared by:** Izzmier Banking Berhad Threat Intelligence Team

**Executive Summary**

This report provides an analysis of the current threat landscape impacting Izzmier Banking Berhad. Key findings include:

- Multiple expired SSL certificates exposing critical services to potential Man-in-the-Middle (MitM) attacks.
- Several mentions of Izzmier Banking Berhad and associated customer data on dark web forums.
- Indicators of phishing campaigns targeting Izzmier Banking Berhad customers.
- Observations of increased malware activity and new vulnerabilities relevant to the banking sector.

**1. Expired Certificates**

**Details:**

- **Domain:** secure.izzmierbank.com
- **Expiration Date:** 15 June 2024
- **Risk:** High
- **Impact:** Potential exposure to MitM attacks, loss of customer trust.

**Recommended Actions:**

- Immediate renewal of the expired SSL certificate.
- Implementation of a certificate management system to prevent future expirations.
- Regular audits of all certificates in use.

**2. Dark Web Monitoring**

**Findings:**

- **Forum:** AlphaBay (Dark Web)
- **Mentions of Izzmier Banking Berhad:** 15 instances
- **Customer Data Found:** Yes
    - **Data Types:** Credit card numbers, account login credentials, personal identification information.
    - **Volume:** Approximately 200 records.

**Sample Excerpt from Dark Web:**

***Selling verified Izzmier Banking Berhad credit card details. Price: $50 per card. Contact for bulk deals.***

**Risk Assessment:**

- **Risk Level:** Critical
- **Potential Impact:** Financial loss, reputational damage, regulatory penalties.

**Recommended Actions:**

- Notify affected customers immediately.
- Enhance monitoring of account activities for suspicious transactions.
- Collaborate with law enforcement to track and mitigate the source of the data breach.
- Strengthen security measures, such as multi-factor authentication (MFA).

**3. Phishing Campaigns**

**Details:**

- **Campaign Start Date:** June 1, 2024
- **Targeted Customers:** Approximately 5,000
- **Phishing Emails Detected:** 200
- **Common Subject Lines:**
    - "Urgent: Update Your Izzmier Banking Berhad Account Information"
    - "Security Alert: Unusual Activity Detected"

**Observed Tactics:**

- Spoofed email addresses mimicking Izzmier Banking Berhad’s official communications.
- Fake login pages designed to harvest user credentials.

**Recommended Actions:**

- Alert customers to the ongoing phishing campaign through official channels.
- Implement email filtering solutions to detect and block phishing emails.
- Educate customers on recognizing and reporting phishing attempts.

**4. Malware Activity**

**Details:**

- **Malware Family:** Emotet
- **Detected on:** Internal network, customer systems.
- **Method of Delivery:** Malicious email attachments, infected websites.

**Risk Assessment:**

- **Risk Level:** High

- **Potential Impact:** Data exfiltration, financial fraud, operational disruption.

**Recommended Actions:**

- Deploy anti-malware solutions across all endpoints.
- Conduct a thorough network scan to identify and isolate infected systems.
- Provide training to employees on avoiding malware infection.

**5. New Vulnerabilities**

**Vulnerability:**

- **CVE-ID:** CVE-2024-12345
- **Description:** Remote Code Execution in Izzmier Banking Berhad Software Version 2.3
- **Severity:** Critical

**Impact:**

- Exploitation could lead to unauthorized access and control over banking systems.

**Recommended Actions:**

- Apply the patch released by the software vendor immediately.
- Review and update all system configurations to ensure security best practices.

**Conclusion**

Izzmier Banking Berhad faces a dynamic threat landscape with several critical issues that require immediate attention. By addressing expired certificates, monitoring and mitigating dark web threats, enhancing defences against phishing and malware, and patching known vulnerabilities, Izzmier Banking Berhad can significantly improve its security posture.

**Recommendations Summary:**

- Renew and manage SSL certificates.
- Monitor dark web for data leaks and collaborate with law enforcement.
- Enhance phishing defences and customer awareness.
- Deploy robust anti-malware solutions and patch critical vulnerabilities.

**Example 2: Health Sector**

**Threat Intelligence Report for Bruno Fernandes Healthcare**

**Date:** 30 June 2024
**Prepared by:** Bruno Fernandes Healthcare Threat Intelligence Team

**Executive Summary**

This report provides an analysis of the current threat landscape impacting Bruno Fernandes Healthcare. Key findings include:

- Multiple expired SSL certificates exposing critical services to potential Man-in-the-Middle (MitM) attacks.
- Mentions of Bruno Fernandes Healthcare and associated patient data on dark web forums.
- Indicators of phishing campaigns targeting Bruno Fernandes Healthcare staff and patients.
- Observations of increased ransomware activity and new vulnerabilities relevant to the healthcare sector.

**1. Expired Certificates**

**Details:**

- **Domain:** portal.brunofernandeshealthcare.com
- **Expiration Date:** 15 June 2024
- **Risk:** High
- **Impact:** Potential exposure to MitM attacks, compromise of patient data.

**Recommended Actions:**

- Immediate renewal of the expired SSL certificate.
- Implementation of a certificate management system to prevent future expirations.
- Regular audits of all certificates in use.

**2. Dark Web Monitoring**

**Findings:**

- **Forum:** Hydra (Dark Web)
- **Mentions of Bruno Fernandes Healthcare:** 12 instances
- **Patient Data Found:** Yes
    - **Data Types:** Personal health information (PHI), social security numbers, insurance details.
    - **Volume:** Approximately 500 records.

**Sample Excerpt from Dark Web:**

***Selling verified Bruno Fernandes Healthcare patient records. Price: $100 per record. Contact for bulk deals.***

**Risk Assessment:**

- **Risk Level:** Critical
- **Potential Impact:** Identity theft, fraud, regulatory penalties, reputational damage.

**Recommended Actions:**

- Notify affected patients immediately.
- Enhance monitoring of patient account activities for suspicious transactions.
- Collaborate with law enforcement to track and mitigate the source of the data breach.
- Strengthen security measures, such as enhanced encryption and access controls.

**3. Phishing Campaigns**

**Details:**

- **Campaign Start Date:** June 1, 2024
- **Targeted Individuals:** Approximately 2,000 (staff and patients)
- **Phishing Emails Detected:** 150
- **Common Subject Lines:**
  - "Urgent: Update Your Bruno Fernandes Healthcare Account Information"
  - "Security Alert: Unusual Activity Detected in Your Health Records"

**Observed Tactics:**

- Spoofed email addresses mimicking Bruno Fernandes Healthcare’s official communications.
- Fake login pages designed to harvest user credentials.

**Recommended Actions:**

- Alert staff and patients to the ongoing phishing campaign through official channels.
- Implement email filtering solutions to detect and block phishing emails.
- Educate staff and patients on recognizing and reporting phishing attempts.

**4. Ransomware Activity**

**Details:**

- **Ransomware Family:** Ryuk
- **Detected on:** Hospital network, staff workstations.

- **Method of Delivery:** Malicious email attachments, compromised remote desktop protocol (RDP).

**Risk Assessment:**

- **Risk Level:** High
- **Potential Impact:** Data encryption, operational disruption, financial loss.

**Recommended Actions:**

- Ensure all systems have updated anti-malware solutions.
- Conduct regular backups and ensure they are stored securely offline.
- Perform a thorough network scan to identify and isolate infected systems.
- Provide training to staff on avoiding ransomware infection.

**5. New Vulnerabilities**

**Vulnerability:**

- **CVE-ID:** CVE-2024-54321
- **Description:** Remote Code Execution in Bruno Fernandes Healthcare Management Software Version 1.8
- **Severity:** Critical

**Impact:**

- Exploitation could lead to unauthorized access and control over health management systems.

**Recommended Actions:**

- Apply the patch released by the software vendor immediately.
- Review and update all system configurations to ensure security best practices.
- Conduct a vulnerability assessment to identify and mitigate other potential weaknesses.

**Conclusion**

Bruno Fernandes Healthcare faces a dynamic threat landscape with several critical issues that require immediate attention. By addressing expired certificates, monitoring and mitigating dark web threats, enhancing defences against phishing and ransomware, and patching known vulnerabilities, Bruno Fernandes Healthcare can significantly improve its security posture.

**Recommendations Summary:**

- Renew and manage SSL certificates.
- Monitor dark web for data leaks and collaborate with law enforcement.
- Enhance phishing defences and increase staff and patient awareness.

- Deploy robust anti-malware solutions and ensure regular backups.
- Patch critical vulnerabilities and conduct regular vulnerability assessments.