Threat Indicators and Cyber Intelligence Sharing in Financial Sector

GUEST LECTURE

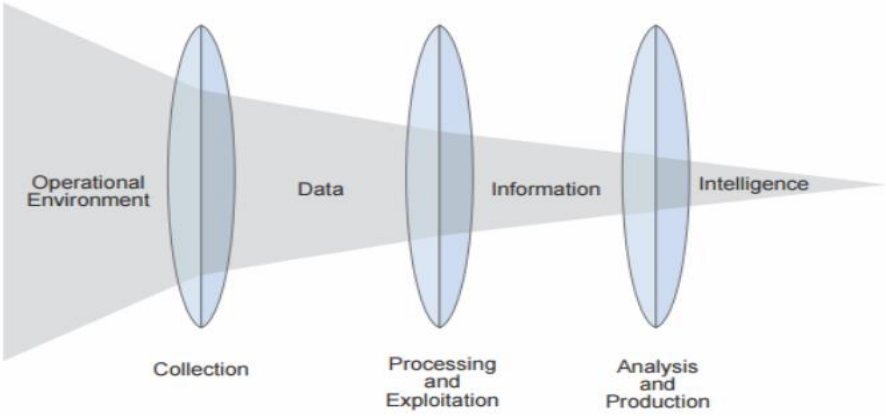
Blaz Ivanc
CISO

Agenda

- Warm Up
- Threat Convergence
- Insider Threat and Cyber Attacks
- Indicator of Compromise
- Threat Intelligence Sharing
- Private – Government Sharing
- Information Sharing and Analysis Center
- Information Sharing Restrictions

Warm Up

- **Cyber bank heist**
  - Attack anatomy: Bangladesh bank heist
  - Scale and sophistication: evolving attack techniques
  - Let's talk about insider threat
  - How many organized hacking groups were present in Bangladesh bank's network?
  - Casinos, AML and country-specific anti-money laundering laws
- **Convergence** of **cyber** attacks, **fraud** and money **laundering**
- **Knowledge** of current and **emerging technologies**
- **Intelligence** sharing is **crucial**



Source: US DoD JP 2-0

Threat Convergence

- **Criminal** ecosystem **will** always **adapt**
- **Cyber** information **sharing** community is less mature than fraud community
- Cyber **security** has their own threat **intelligence**, analytics and detection methods
- **Organized** cyber criminal **groups** are trying to find **weak** points in the **international** financial **system** as well as **emerging** FINTECH services

Threat Convergence

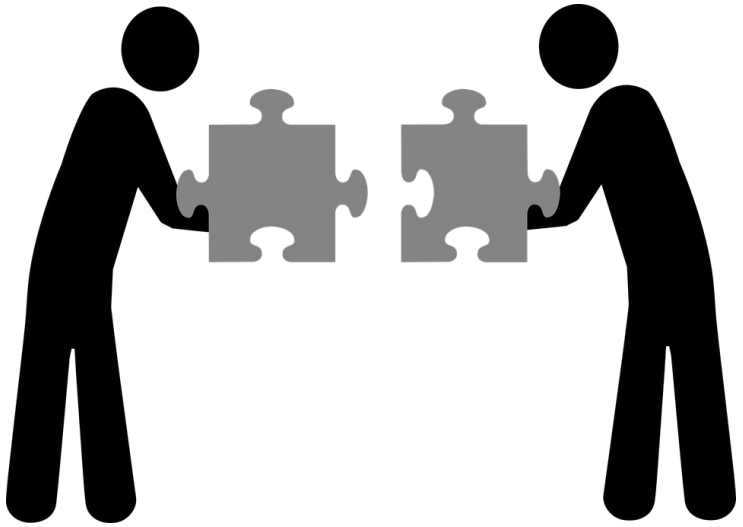
- **Cyber** and **financial** crime**:**
  - *Frequently related*
  - *Speak the same language*

- **Emerging** technologies → new **channels** for criminals
  - Individual end-point entity performs multiple transactions across multiple channels
  - Financial institutions – separate departments (cyber / fraud / compliance)

- **Frequency** and diversity of **attacks**

Threat Convergence

- Cyber **Security** and Actionable **Intelligence**
  - **Timing** and **patterns** of cyber-related **events**:
    - Suspicious activities identification
    - Risk exposure understanding
- **Patterns** → indicators
- Cross-department collaboration
- **Know** your data **requirements** and **technology**



Insider Threat and Cyber Attacks

- **Insider** Threat & Cyber **Attacks**: source / motivation / targets / methods
- **Important factor**: analysis based on solid intelligence
- **Insider threat**:
  - Malicious insider
  - Accidental insider
  - External actors
- Pressure / Opportunity / Rationalization

Indicator of Compromise (IOC)

- **IOC** vs **observable** ← *important!*
- **Indicators** require context to be useful
- **Importance** of understanding **context**, **relevance** and **accuracy**
- **Sharing** can be **restricted** on legal grounds

HANDS-ON DEMONSTRATION

Threat Intelligence Sharing

- *"**Cyber** threat intelligence is the **process** and **product** resulting from the **interpretation** of raw data into information that meets a **requirement** as it relates to the **adversaries** that have the intent, opportunity and capability to do harm"* *R. M. Lee, 2016*
- **Automated sharing** → situational awareness / complex threat analysis / proactive defense
- Early **detection** and **prevention** (before exploitation phase)
- **Issues** with automatic threat **sharing**:
  - Shortage of available resources
  - Lack of security maturity
  - Insufficient internal processes or tools to consume threat information
- **Verifications** before consuming **intelligence**
  - Access point, source, sender, verification of message integrity …

Threat Intelligence Sharing

- **Standards** to **facilitate exchange** of threat **intelligence**:
  - **STIX** (Structured Threat Information eXpression) – **format**. *STIX is maintained by the OASIS CTI TC*
  - **TAXII** (Trusted Automated eXchange of Indicator Information) – **protocol**. *TAXII is designed to support the information exchange represented in STIX*
  - CybOX (Cyber Observable eXpression): CybOX has been integrated into **STIX 2.0** (CybOX objects → **STIX Cyber Observables**)
  - OpenIOC (Open Incident of Compromise); IODEF (Incident Object Description Exchange Format) …

Threat Intelligence Sharing

- **Threat Intelligence Platforms (TIPs)**: Open Source / Commercial / Community
- Threat **feeds** and information **sources**
- Some of the **advantages** of TIPs: Data refinement / Information sharing / Automation …
- **Users**: SOC & CTI analysts / Incident responders / Researchers / IT managers and executives …
- **Limitations** of TIPs

HANDS-ON DEMONSTRATION

Private – Government Sharing

- Cyber-**events** → various **reports**
  - Data driven techniques
  - Employee's initiative
  - Based on inputs from government sector entities
- **Government** sector entities: relatively little useful or timely **information**
- Barriers in **intelligence** sharing across **community**
- Information-sharing **partnerships**:
  - Cross-sectoral
  - Real-time
  - Iterative

Information Sharing and Analysis Centre

ISAC - Information Sharing and Analysis Centre

ISACs »… *organizations that **provide** a central **resource** for gathering **information** on cyber threats (in many cases to critical infrastructure) as well as allow **two-way** sharing of information **between** the **private** and the **public** sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.«* *ENISA, 2017*

- **Good practice**: SWIFT ISAC
  - IOCs
  - Machine-digestible information: CSV, OpenIOC XML, YARA rules*
  - Modus operandi analyses
  - General security information

Information Sharing Restrictions

- **Cyber** and **financial crime**
  - Legal barriers in intelligence sharing across community
  - Financial institutions need to develop operating models and establish information hubs
  - No regulations in place; only recommendations

- **Classified Information**
  - Restricted access by law/regulation
  - EU / NATO / State-based
  - Lack of solid intelligence (weak content) can be an issue

- **Traffic Light Protocol** (TLP)
  - Forum of Incident Response and Security Teams (FIRST) → CSIRTs, ISACs …
  - Sharing sensitive information with the appropriate audience
  - Four colors (white / green / amber / red) – sharing boundaries

„An investment in knowledge pays the best interest.“

B. Franklin