A Nuclear Operator Approach to Identify Credible Cyber Insider Threats

Threat Intelligence – Threat Brief
September 2024

Luke Walker
Threat Defence and Cyber Security Operations
Threat Intelligence Manger

TLP White

Disclaimer

TLP – White

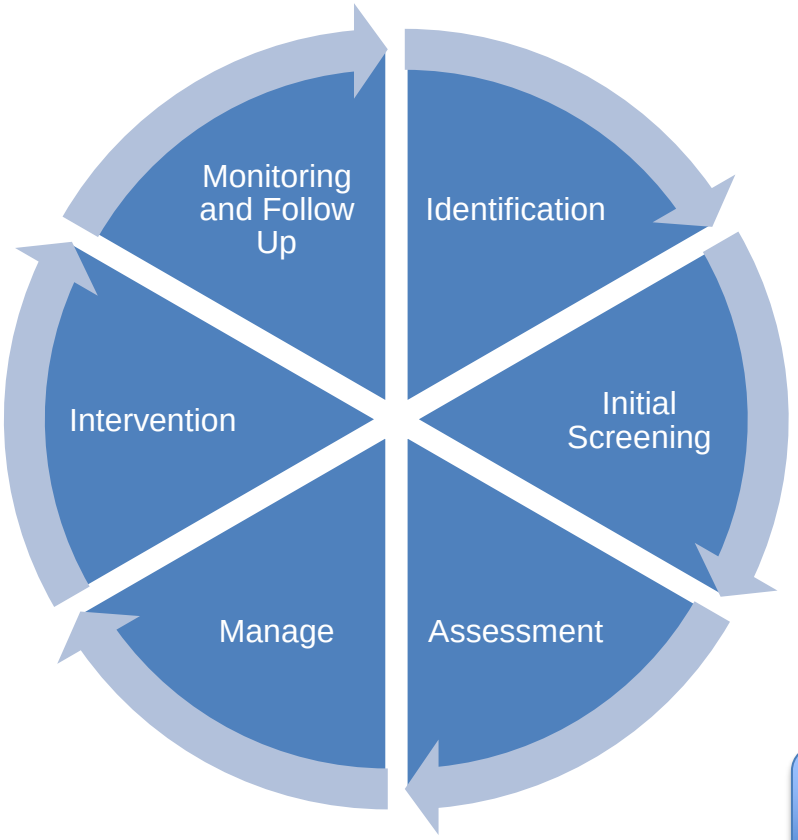
- **Process and Examples covered are considered best practice and either publicly available known examples or hypothetical**
- **Due to sensitivities I will not discuss any specific processes or examples related to Urenco**
- **Any opinion given is based on my own personal experience and may not form company policy**

Why are we here?

TLP – White

Threat assessments against insider threat specifically around nuclear sites and how we apply that to protect the organisation

Traditional Threat Assessment Process



Nuclear Insider Threat Considerations

Definition

TLP – White

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

- An insider is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems.

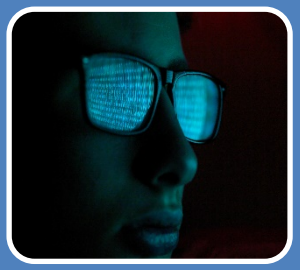
National Cyber Security Centre

- Deliberate or accidental threat to an organisation's security from someone who has authorised access (such as an employee).

Types of Insider Threats

TLP – White

A Nuclear operator has significant physical and cyber insider threats. Often the two can blend into one individual insider threat.



Intentional Threat

- **Malicious Insider**
  - Actions taken to harm an organization for personal benefit or to act on a personal grievance

Unintentional Threats

- **Negligence**
  - Negligent insiders are generally familiar with security and/or IT policies but choose to ignore them
- **Accidental**
  - Mistakenly causes an unintended risk to an organization

Other Threats

- **Collusive Threats**
  - Insiders collaborate with an external threat actor to compromise an organization
- **Third-Party Threats**
  - Contractors or vendors who are not formal members of an organization, but who have been granted some level of access to facilities, systems, networks, or people to complete their work

How Does Insider Threat Occur?

TLP – White

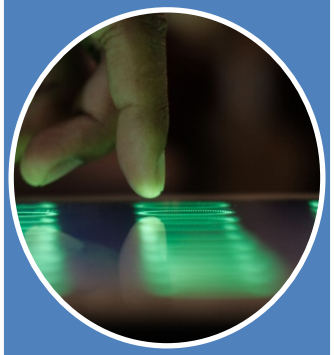
A Nuclear operator has significant physical and cyber insider threats. Often the two can blend into one individual insider threat.

Violence

- Workplace
- Terrorism

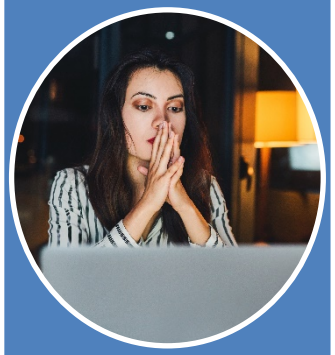
Espionage

- Economic
- Government
- Criminal



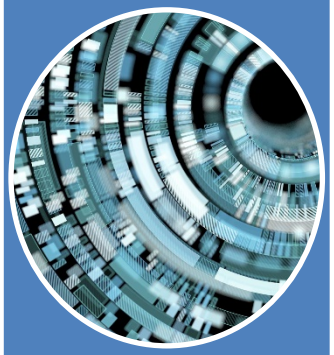
Sabotage

- Physical
- Virtual



Theft

- Financial
- Intellectual Property



Cyber

- Intentional
- Unintentional

HYBRID

Why is Nuclear a Target for Insider Threats?

TLP – White

What makes the nuclear industry more attractive to insider threats?

- Privileged Access
- Large Financial Incentives
- Potential for Significant Harm
- Small Industry
  - ➢There are not many of us with the data we hold

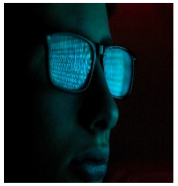
What makes the nuclear industry less attractive to an insider threat?

- Strict Security Measures
- Analog Systems (in some locations)
- Limited Digital Footprint

What does all that mean?

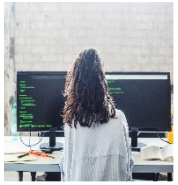
TLP – White

A Nuclear operator has significant physical and cyber insider threats. Often the two can blend into one individual insider threat.



Physical Insider Threat

- Have physical access to assets, like a building or equipment.
- They might steal sensitive information
- Steal physical assets such as a laptop
- Cause damage to buildings or physical assets
- Could threaten physical violence



Cyber Insider Threat

- Have access to an organisation's IT networks
- Have access to the OT networks
- Could download or transfer data – Steal IP
- Could install malware
- Conduct Espionage
- Install local devices – Monitor or Access

Blended Insider Attack

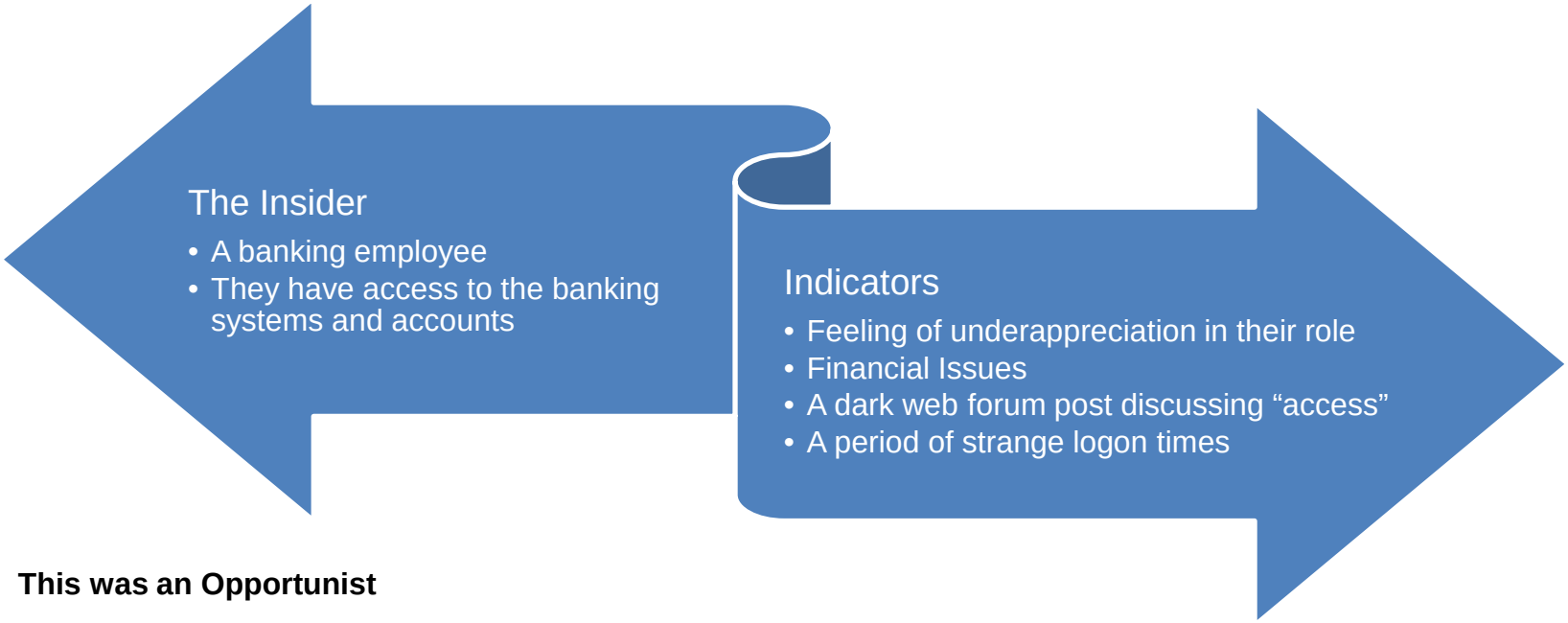
- The insider uses there access to disable the local CCTV
- The insider then causes physical damage or steals assets
- Their accomplice takes advantage of the known missing control

Nuclear Insider Threat

- A combination of both physical and cyber insider threats – **A Blended Insider Attack**
- Motivated by:
  - Personal gain
  - Ideology (Nation State, Anti Nuclear etc)
  - Revenge
- Difficult to detect (IT vs IOT vs OT logging monitoring)
- Exploit existing trust relationships
- Both physical and cyber insider threats can cause:
  - Damage to reputation
  - Damage to finances
  - Damage operations
  - **SAFETY INCIDENT**

A Cyber Insider Threat Example

TLP – White



This was an Opportunist

The banking employee saw an opportunity in selling their access to threat actors

The Red Flags:

- Darkweb forums discussing access to banks
- Use of USB devices
- Strange network connections/downloads
- The employee becomes “withdrawn” at work

“Create Malware for bypass internal Bank computer Security” – Posted on Exploit

“I have physical access to bank computer that can pull up all customer info, wire funds from any customer, make changes to account, etc. I can get task manager process list, av/edr versions, etc. Need someone to assist in custom designed malware for intrusion to covert use the software to make changes to bank account. PM me with xmpp detail if you are expert”

A Cyber Insider Threat Example

TLP – White

The Insider

- A Principal Software Engineer

Indicators

- A series of suspicious activities were detected on that user account
- When questioned, gave an excuse of having router issues
- Began transferring and deleting files

This was a North Korean Fake IT Worker

Based on the report it was suspected and discovered the IT worker was an Insider Threat/Nation State Actor.

The Red Flags:

- Resume/CV career inconsistencies
- Shipping address of IT equipment different to the resume/CV
- Unable to attend physical interview and no camera facility during virtual interview
- Use of VOIP numbers

Insider Threat Mitigations

TLP – White

To effectively identify credible cyber insider threats, Nuclear organisations should focus on key areas.

Risk Management Program

Joiners Movers Leavers (JML) – Vetting, Separation of Duties, IDAM

Create a Safe and Supportive Environment

- Build a Culture of Reporting and Prevention
- Establish a Supportive and Protective Culture
- Build a culture where employees care
- Insider Threat Reporting Portal
- Implement an Insider Threat Training & Awareness Program

Apply a Detection and Mitigation Framework

IT, IOT & OT

- Regular Audits and Access Control
- Incident Response Plan in case of an insider threat incident
- Threat Hunt for Cyber Insider Threats
- Vulnerability Management & Security Testing
- Threat Intelligence
- Limit privileged access
- Data Leak Protection (DLP)
- Monitor for Suspicious Activity
  - Unusual login times or locations
  - Excessive data downloads or transfers
  - Changes to system configurations
- Table Top Exercise based on an Insider Threat
- Regular Reporting
- Dark Web Monitoring
- Credential Monitoring

Engage/Report to Business, Technical & Functional Stakeholders (HR, Legal, WC etc)

Questions