# Cyber defence at the highest level

Rukhsar Khan
Innovative Business Development & Consulting – Threat Management
GIAC Certified Forensic Analyst (GCFA) Gold-level #12275

# Agenda

**1) The business problem**

Adversaries appear to be ahead of the cyber defence community

**2) SOC & deep-dive forensic findings**

212 days for identifying a breach is a SOC problem

75 days for breach containment is due to limitations in deep-dive forensic methodology

**3) Problem solution: increase SOC maturity level**

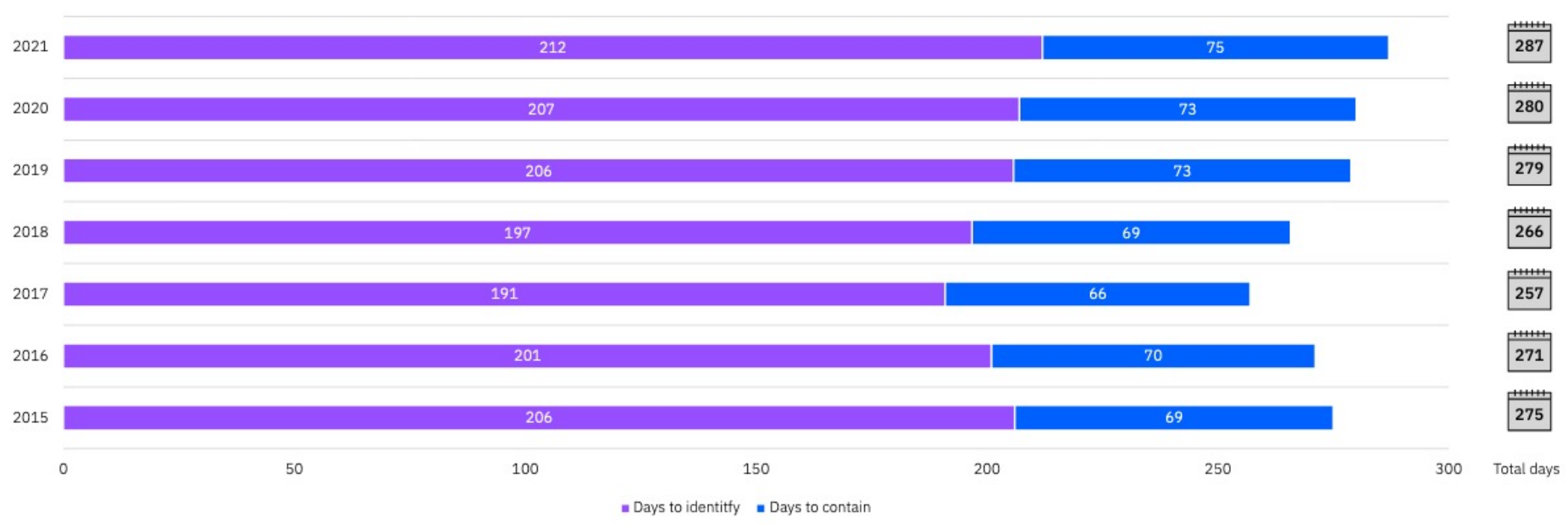
Cyber Threat Intelligence (strategic, operational)

Cyber Threat Modeling (threat-centric, asset-centric, system-centric)

Proactive Threat Hunting (forensic analysis methodology at scale)

# The business problem

# Average time to identify and contain a data breach




Source: Cost of a Data Breach Report (2021, IBM Security/Ponemon)

# Adversaries appear to be ahead of the defence community

**A data breach lifecycle of less than 200 days produced a cost savings of nearly a third over a breach lifecycle longer than 200 days.**

A breach with a lifecycle over 200 days cost an average of $4.87 million in 2021, vs. $3.61 million for a breach with a lifecycle of less than 200 days. The gap of $1.26 million represents a difference of 29.7%. This gap between breaches with a lifecycle shorter/longer than 200 days was $1.12 million in 2020. That means the beneficial cost impact of containment in less than 200 days grew from 2020 to 2021.

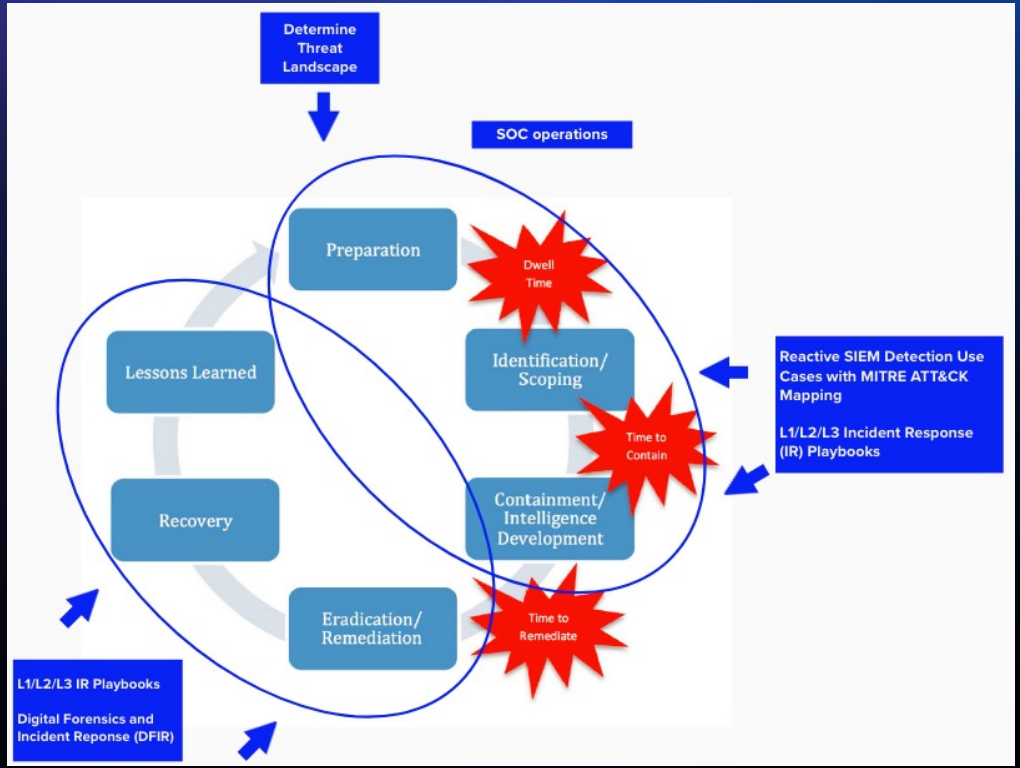
- Reducing the breach lifecycle requires an increase in the SOC maturity level

# SOC & deep dive forensic findings

IBM **Security**

IBM

# SOC operations today




Source: SANS 6-step Incident Response

# SOC findings

Negative findings:

- Scratching the surface
- Simple verifications rather than extensive analysis
- Lack knowledge and expertise to analyse and comprehend a complete breach
- Reactive in nature - wait for an incident / event to occur in order to kick in the IR process

Positive findings:

- Scales to thousands or tens of thousand endpoints
- Process-driven, therefore "well" structured

# Deep-dive forensic findings

Positive findings:

- Understand and report on the full scope and complete impact of a data breach
- Develop a strategy for completely removing an attacker's foothold from a compromised environment

Negative findings:

- Highly complex, unstructured and an entirely manual process
- Plethora of disconnected tools with uncountable inputs and different output formats used manually on CLIs
- Doesn't scale

# Problem solution: increase SOC maturity level

# Incident Preparation with Threat Intelligence / Modeling

- Determine Threat Landscape by consuming Cyber Threat Intelligence
- Know yourself
  - Determine critical functions and underlying systems and services
  - Determine business parameters (industry, relevant threat actors, etc.)
  - Digital footprint
- Cyber Threat Modeling (threat-centric)
- Extend threat-centric modeling to the modeling of critical functions and underlying systems and services while considering business parameter and digital footprint

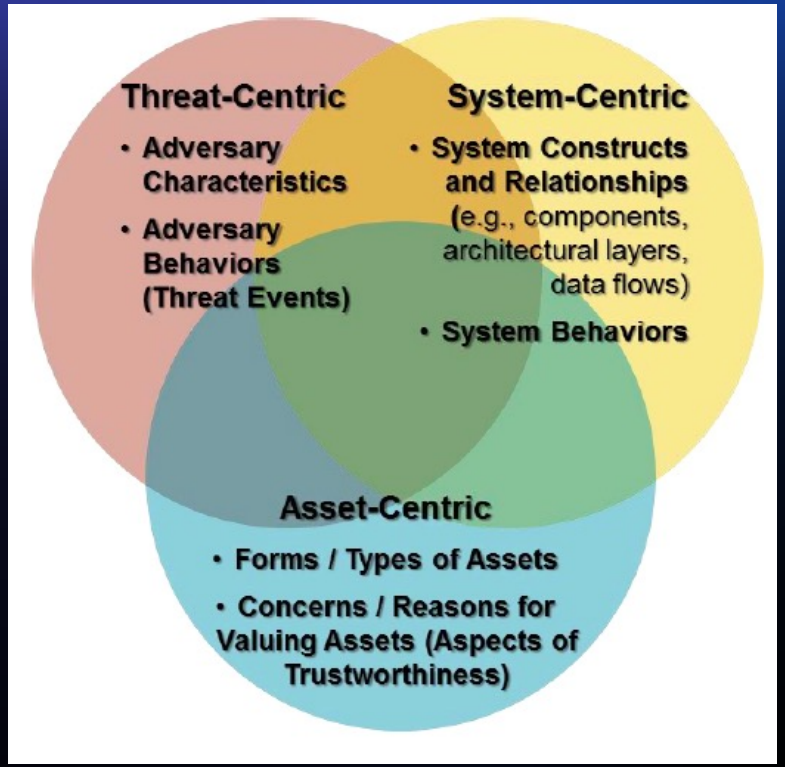
# Cyber Threat Intelligence – differentiated

- Strategic Cyber Threat Intelligence (CTI) – Answer the **Who** and **Why**. Threat Actor goals and motivations.

- Operational CTI – Answer the **When**, **Where** and **How**. Trend analysis of adversary capabilities and campaign history for current and predictive analysis. Understand adversary‘s attack ecosystem and known course of actions.

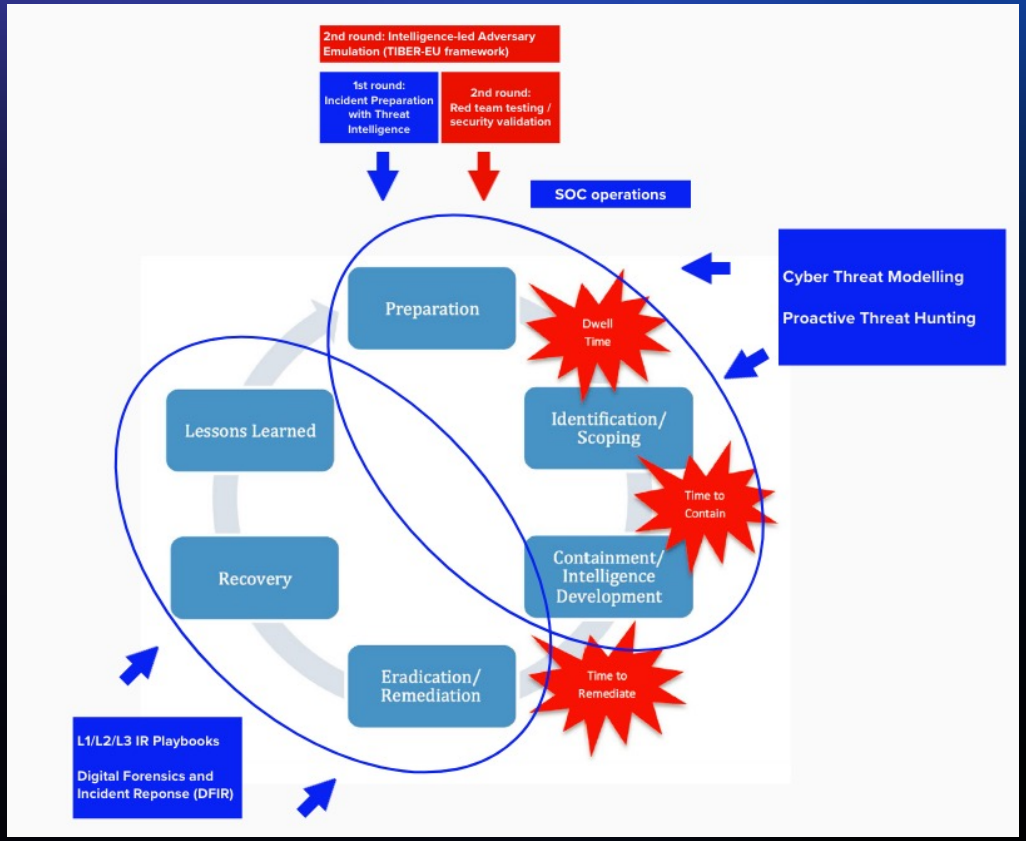
- Tactical CTI – Answer the **How** and **What**. Contextual IoCs (IP address, hash, domain name) and TTPs.
  **CAUTION:** IoCs change rapidly but TTPs are robust!

# Cyber Threat Modeling




Source: Cyber Threat Modeling: Survey, Assessment, and Representative Framework (2018, HSSEDI)

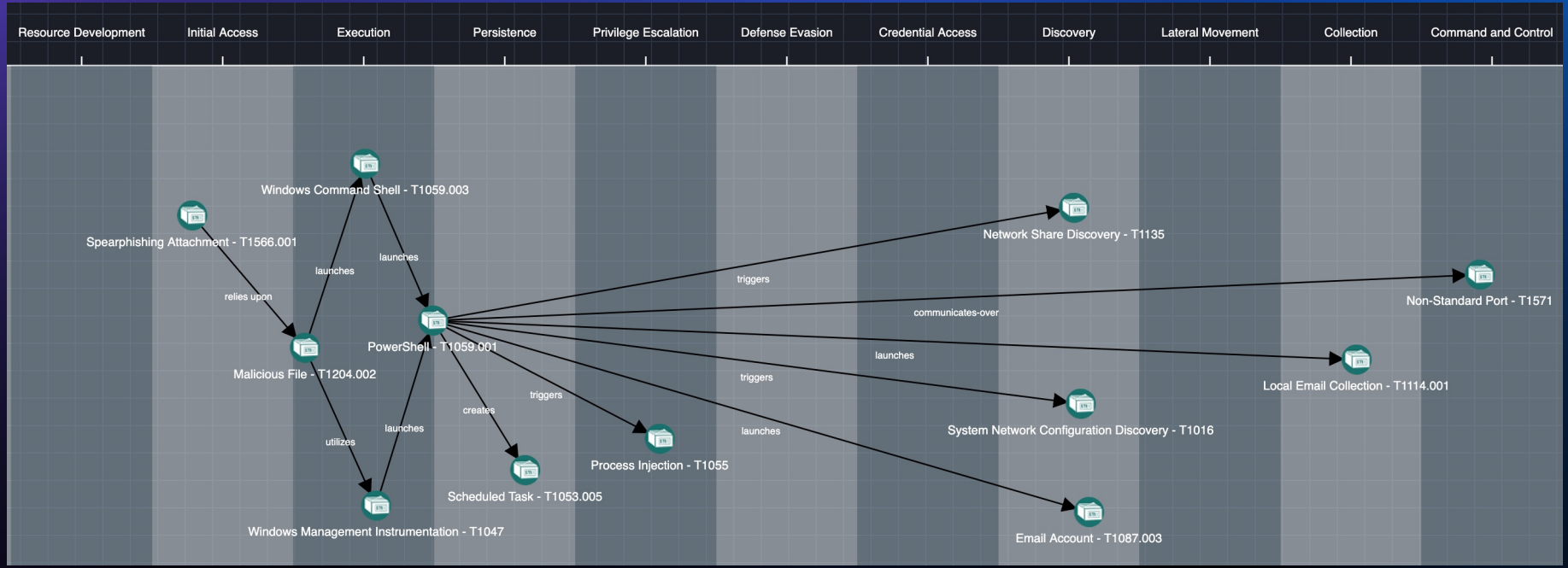
# SOC operations tomorrow



# SOC operations tomorrow – summary

- Incident preparation with Cyber Threat Intelligence / Modeling
- Proactive Threat Hunting (forensic analysis methodology that DOES scale)
  - Quickly identify and contain endeavours of cyber attackers in early stages of the attack lifecycle
  - Prevent cyber attackers from establishing a large foothold and subsequently reduce business risk and total breach costs significantly
- Security validation through Adversary Emulation

# DEMO




Source: Open source tool for visualizing STIX 2.1 content in the MITRE ATT&CK kill-chain: https://github.com/yukh1402/cti-stix-diamond-activity-attack-graph

https://www.rukhsarkhan.de
rkhan@rukhsarkhan.de