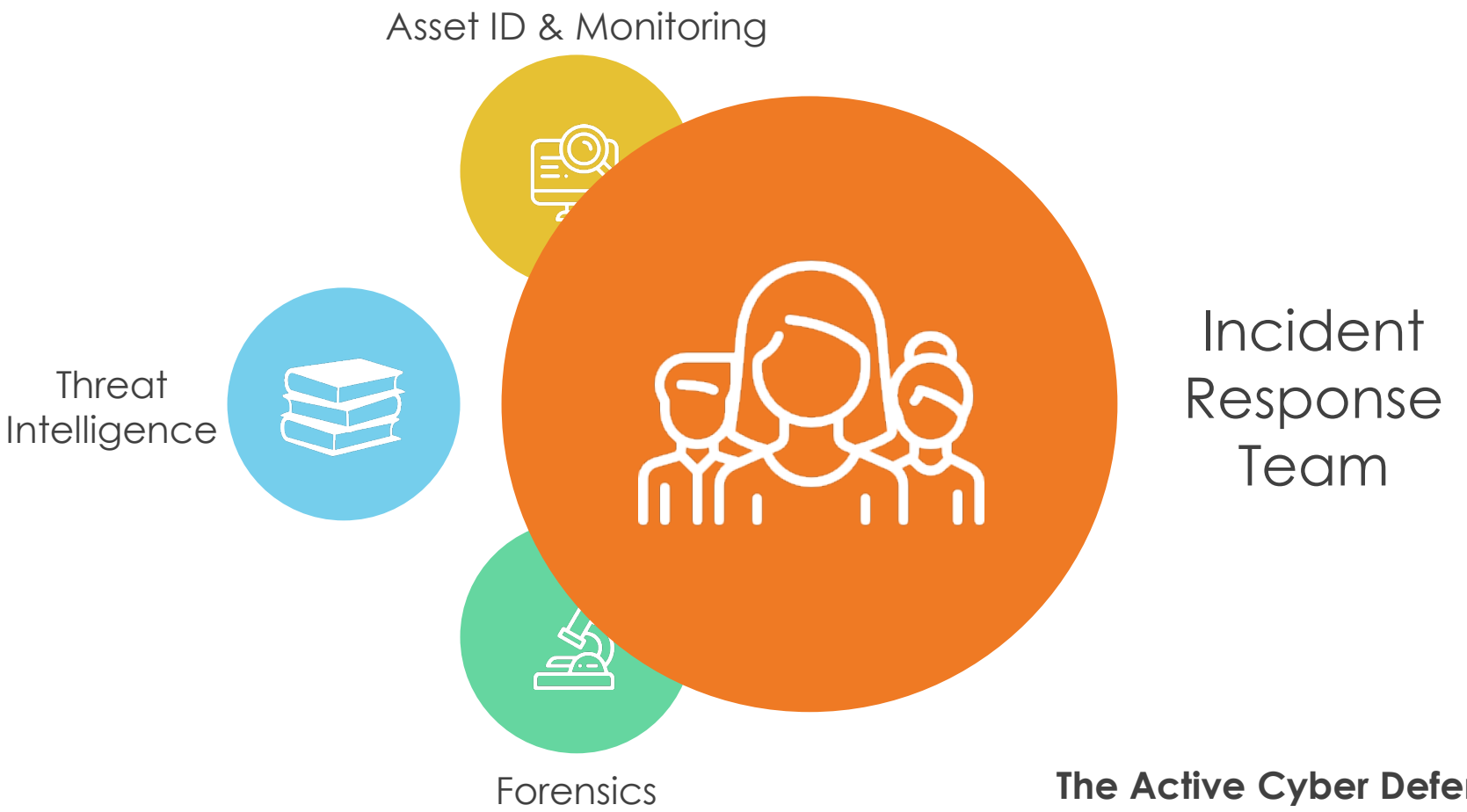
CYBER OT

Incident Response Team - Under Construction!

Eran Salfati, Lital Badash et al

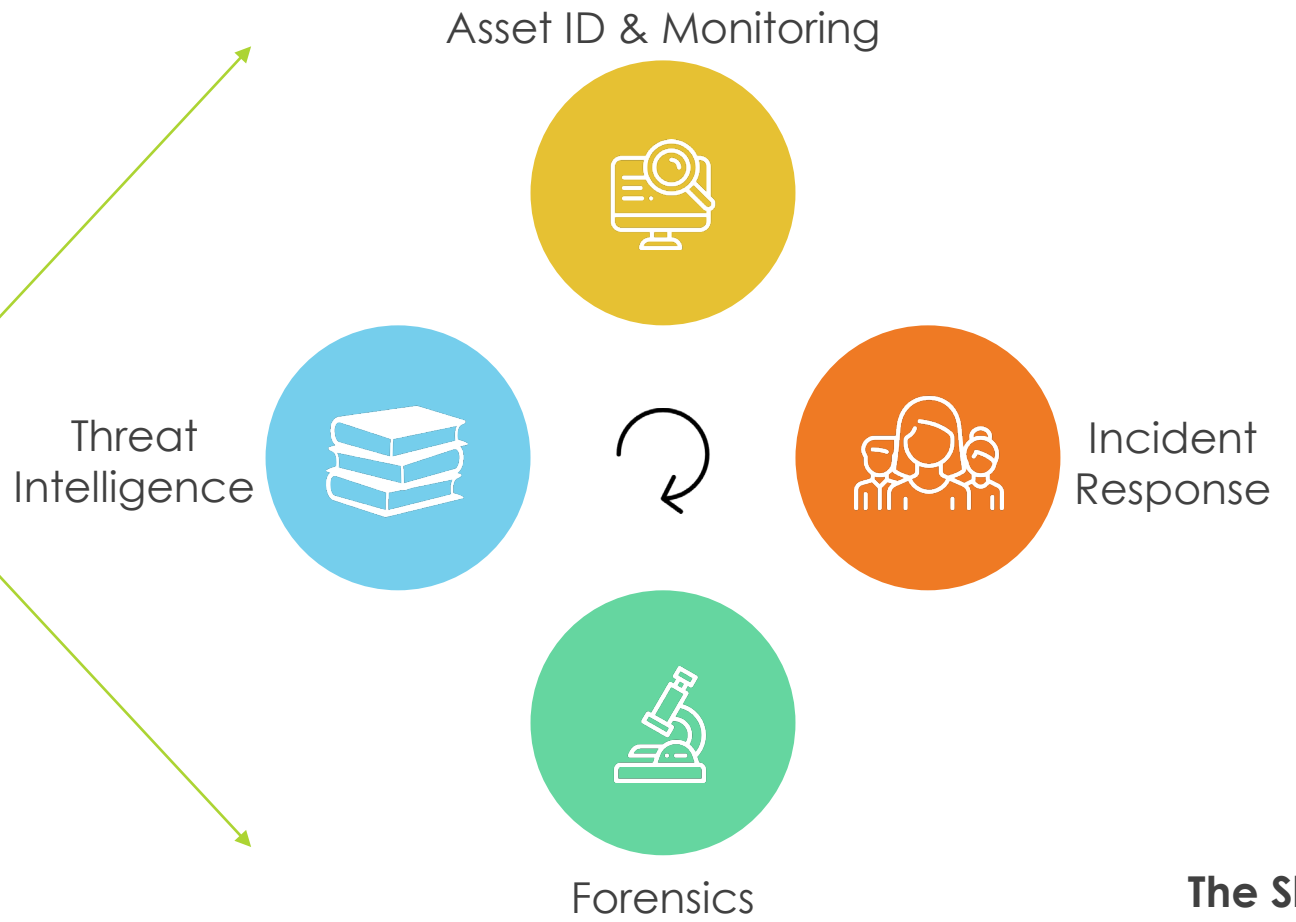
Intro



The Active Cyber Defense Cycle

The Sliding Scale of Cyber Security

- Architecture
- Passive Defense
- **Active Defense**
- Intelligence
- Offensive



- Architecture
- Passive Defense
- Active Defense
- Intelligence
- Offensive

Policy

Supply Chain

Patch & Backup

Awareness

- Architecture
- Passive Defense
- Active Defense
- Intelligence
- Offensive

Network Architecture

Anti-Malware

IDS

Diode

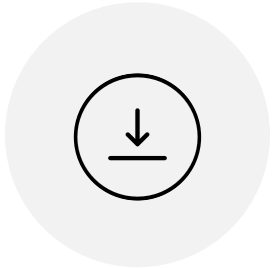
SCADA Security – Where Should we Start?

Eran Salfati et al

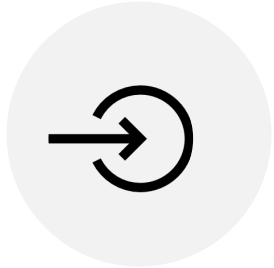
SEEEI, 2016

- Architecture
- Passive Defense
- **Active Defense**
- Intelligence
- Offensive

- Architecture
- Passive Defense
- Active Defense
- **Intelligence**
- Offensive



Internal Sources



External Sources

- Architecture
- Passive Defense
- Active Defense
- Intelligence
- Offensive

Offense for Defense

Active Defense

- Architecture
- Passive Defense
- **Active Defense**
- Intelligence
- Offensive

Before

TTP's –
Tactics
Techniques
Procedures

Baseline
Collection
Detection
Analysis

After

Reverse Eng
Behavior
Static
Automated

Incident Response

NIST SP 800-61

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lesson Learned

Pre Preparation

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lesson Learned

- Skills
- Previous knowledge

- Team Size
- Interfaces
- Organizational Structure

- Tools
- Safety
- Procedures
- Evidence Collection Toolkit

- Event Management Center

Routine

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lesson Learned

Instruction **Training**

Reports Study

Know Architecture **Know Risks**

Baseline **“Forensability”**

Policy & Procedures Update

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lesson Learned

Chain of Events

Dynamic Data **Static Data**

Initial Forensics **Timeline**

Whitelist **Assessment**

Initial Report

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lesson Learned

Safe Operational continuity

Prevention of proliferation

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lesson Learned

Remove & Clean

Restore from Backup

Patch & Update

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lesson Learned

Back to Operation

Validation & Verification

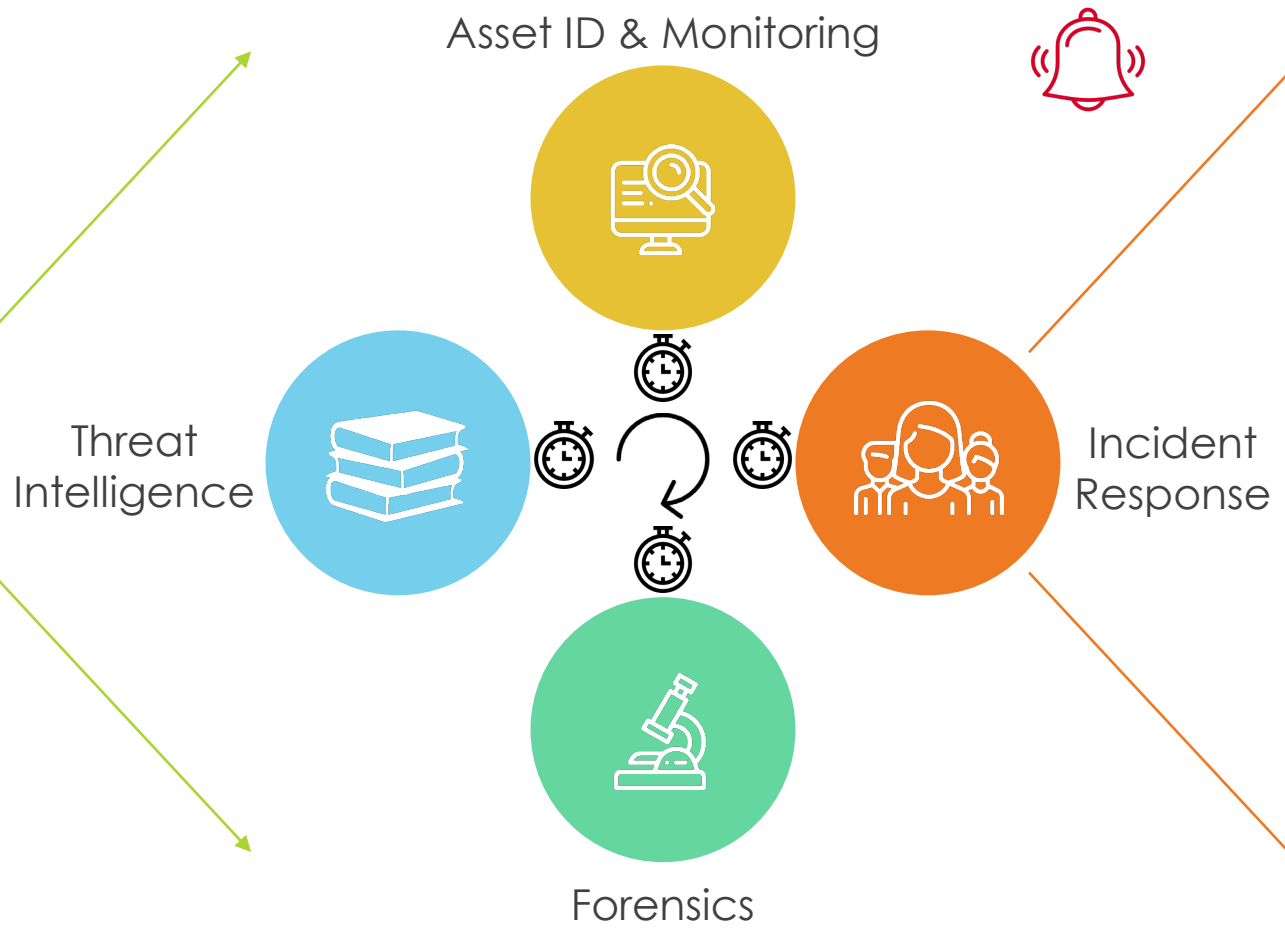
- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lesson Learned

Final Report

Share

Summary

- Architecture
- Passive Defense
- Active Defense
- Intelligence
- Offensive



- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lesson Learned

CYBER OT

Incident Response Team - Under Construction!

Eran Salfati, Lital Badash et al