Responding to incidents in industrial environments

@themyops (Hinne Hettema)

Agenda

1. Some ‘wisdom’ on building Security Operation Centres
2. Risk profile of operational technology (and how it’s different to IT)
3. Incident response principles for OT
4. Incident response practices for OT
5. How to get better with responding to incidents in OT

Security Operation Centres

The purpose of security operations

Don’t confuse *purpose* with *benefits*.

Purpose is narrow:

1. Ensure attackers don’t achieve their objectives
2. Reduce dwell time
3. Evict effectively

Benefits are wider: environmental hygiene, systemic effectiveness, support for root cause analysis, attack analysis, threat intelligence, visibility and agility through fact based decision making.

CSOC life stages and maturity

Strategy	-	Main challenge is to devise and practice engagement strategies for new attacks, rapid response and service optimisation
Action / Operation	6	Main challenge is collecting, categorising and storing incident data and derive TTPs from it
Context	12	Main challenge is driving better operational practices (certificates, user accounts, websites, remote access) and simplifying the architecture
Visibility	18	Main challenge is ‘battle for the logs’

CSOC activity roadmap

Strategy	Strategy	Informed risk discussions, defence modelling
	Kill Chain	Threat modelling
	Threat Intelligence	STIX / TAXII
Action / Operation	Alerting	Security Orchestration and Response (SOAR)
	Incident Response and Closure	Planning, gamification, exercises
	Environment health	Certificates, DNS, Cloud, Infrastructure as code, Code security
Context	Log aggregation	Data normalisation, NTP, noSQL
	Configuration data	Deployment tools with code repositories
	Identity	Active Directory, Groups, Logon traffic, Bloodhound
	Analytics, playbooks	
Visibility	Logging	Everything logs
	Collection tooling	Tools needed to collect in case of an incident, practice
	Identity	Actions traceable to people (as much as possible)

OT Risk profile and kill chains

The risk profile of OT is different

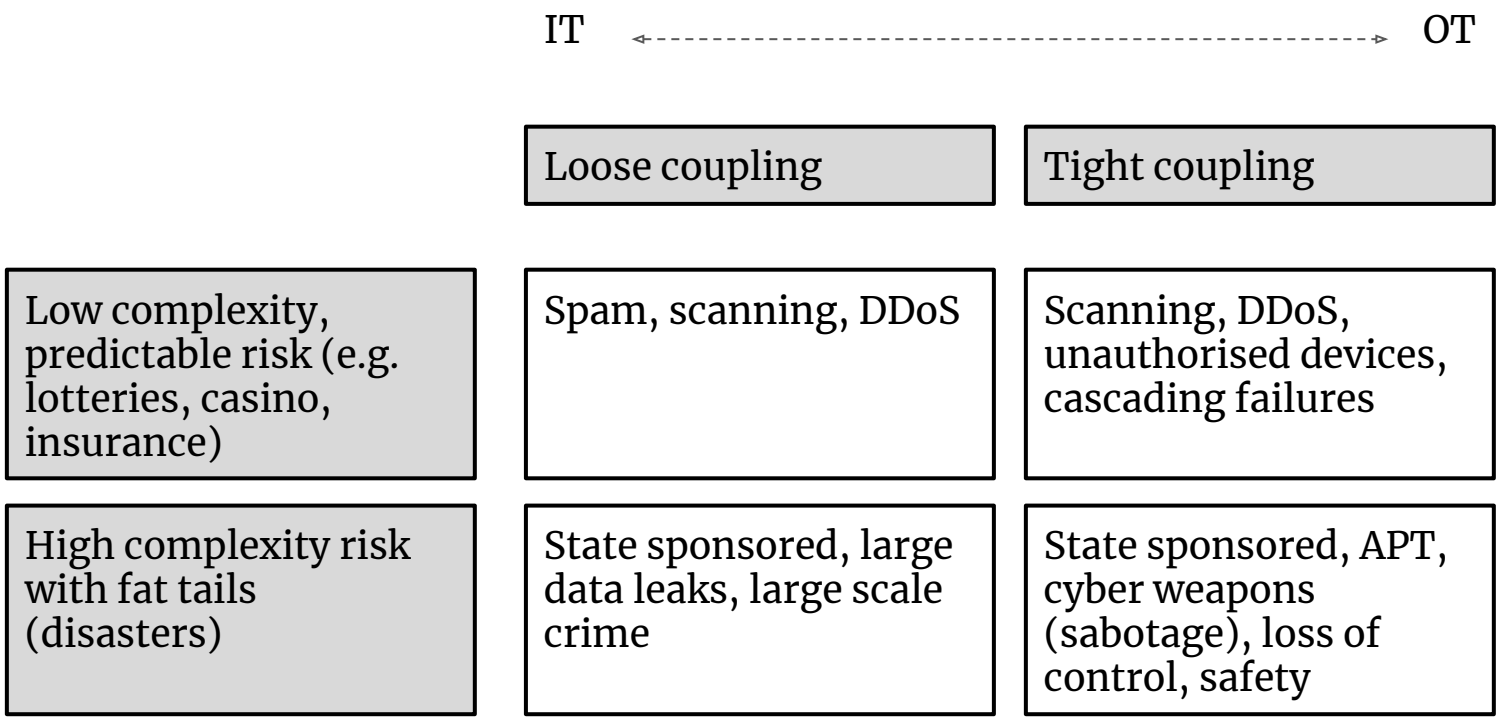
Higher risk...

- OT is often tightly coupled
- The consequences of a successful OT attack are more serious
- Basic security provisions are often primitive or absent

...but harder to execute a successful exploitation

- ‘One shot’ compromises don’t really exist, but instead campaigns are required
- Campaigns require in-depth knowledge of the processes and technology deployed by the intended victim

Risk profile of OT incidents



Kill chain models for ICS

Robert Lee (1)

- ICS specific kill chain

Pols (2)

- Unified kill chain

Hassanzadeh-Burkett (3)

- SAMIT (Spiral model)

(1) https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
(2) https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf
(3) https://ewic.bcs.org/upload/pdf/ewic_icscsr18_paper2.pdf

OT Architecture (Purdue) and kill chains

Enterprise networks (IT)
5 DMZ
4 Corporate LAN

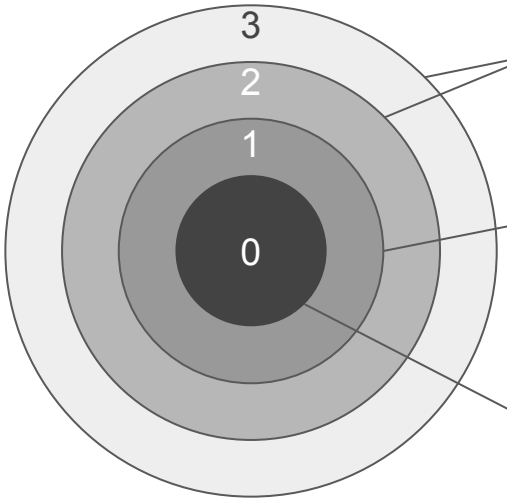
Traditional kill chains (IT Focus)

OT DMZ

Manufacturing zone
3 Operations and control

Cell / Area Zone
2 Supervisory control
1 Basic control
0 Process

OT Additions



Loss of
View
Control

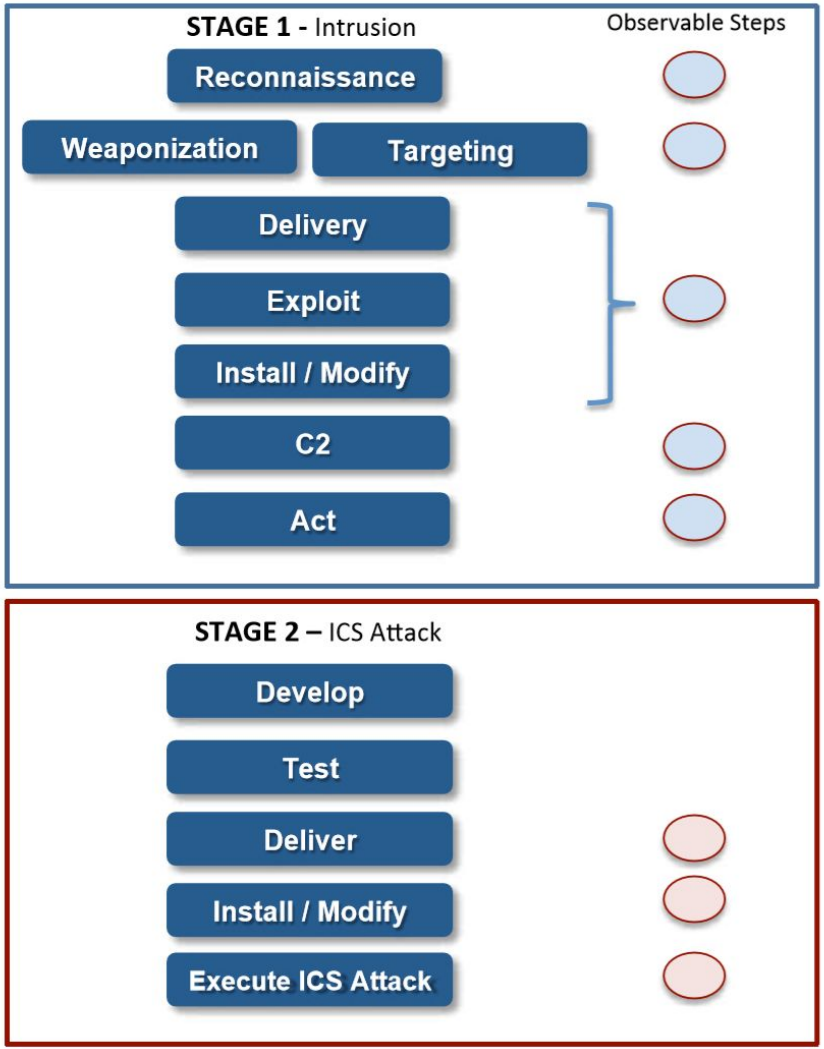
Denial of
View
Control
Safety

Manipulation of
View
Control
Sensors / instruments
Safety

ICS Cyber Kill Chain (Lee)

The ICS Cyber kill chain adds a second stage to the ‘conventional’ kill chain, to account for the specifics required to execute an ICS attack. Specifically, it includes the steps required to develop, test, deliver and even modify an attack to ensure it works.

Attackers will have to spend quite a bit of time in ‘Stage 1’ in order to successfully progress to Stage 2, or use third party vendors as a route to the required information.



Unified Kill Chain (Pols)

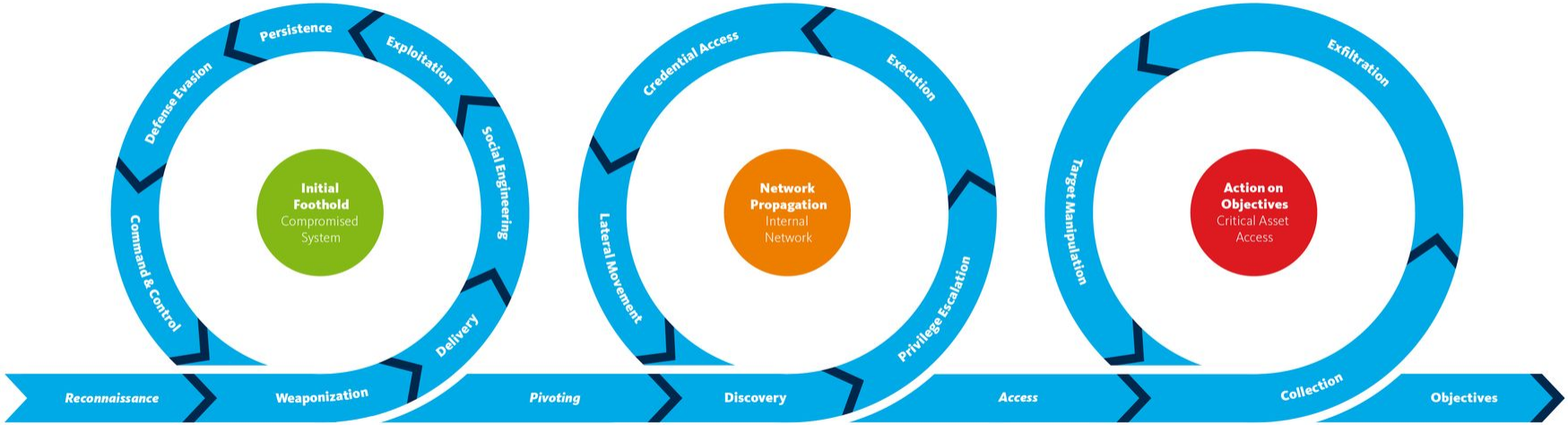
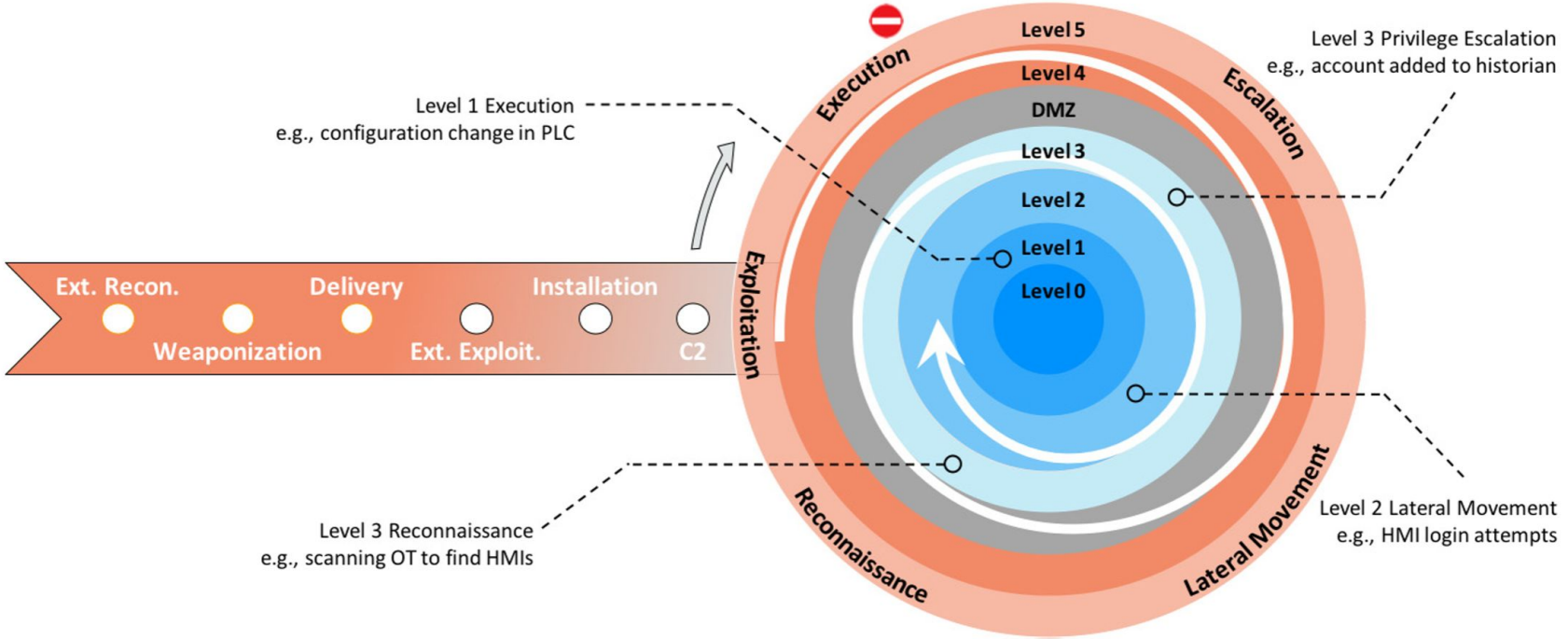


Image source: https://mitigatehub.com/the-unified-kill-chain-part-2/

Spiral Attack Model for IOT (Hassanzadeh)



Kill chains and operational technology

A benefit of the use of kill chains in operational technology is that they set us up for a defence strategy.

To execute a *successful* OT attack an adversary must:

1. Traverse several layers
2. Employ a variety of methods
3. Understand the specifics of what they are dealing with
4. Have a long dwell time in the IT layers of an environment (or compromise one of our vendors who has that knowledge)
5. Potentially stage and test several attacks

Principles for OT Incident Response

Prepare for OT Incident Response

1. Get eyes on your surroundings: attackers have to spend a long time there, traverse several environments, pivot, and elevate. All of this leaves traces
2. Know the specifics of your engineering and OT tooling. This is what the attackers need to generate once they are in the front door (i.e. the IT environment). In the event of an incident you need to ‘collect’ these items and need to know what you’re dealing with.
3. Don’t forget about vendors and contractors, who have very specific knowledge about your environment (but perhaps not the same level of security)

SAIC principles

The order of protection in OT incidents is almost always:

1. Safety
2. Availability
3. Integrity
4. Confidentiality

Usually in IT, we worry about things in the ‘CIA’ order

1. Confidentiality
2. Integrity
3. Availability

Execute OT Incident Response

A team must

- Work to the SAIC security priorities (IT people need to learn this!)
- Have right training and certifications to access these environments to collect and inspect
- Work with engineering to determine consequences / risks to processes etc.
- Develop situational awareness in OT environments

Amounts to: Know industrial environments so you can work in them under pressure

Two keys: visibility and collection readiness

Visibility: make sure everything logs

- Centrally (log collection strategy)
- Use tools like splunk or elastic to aggregate

Collection readiness

- Instead of knowing every asset know as much as possible the types of asset
- Be ready to collect these assets during incidents (practice this)
- Windows collection tools (Need to also include collection for Windows XP, Windows CE)
- PLC collection tools, e.g. snap7 or Siemens native
- Practice on old equipment

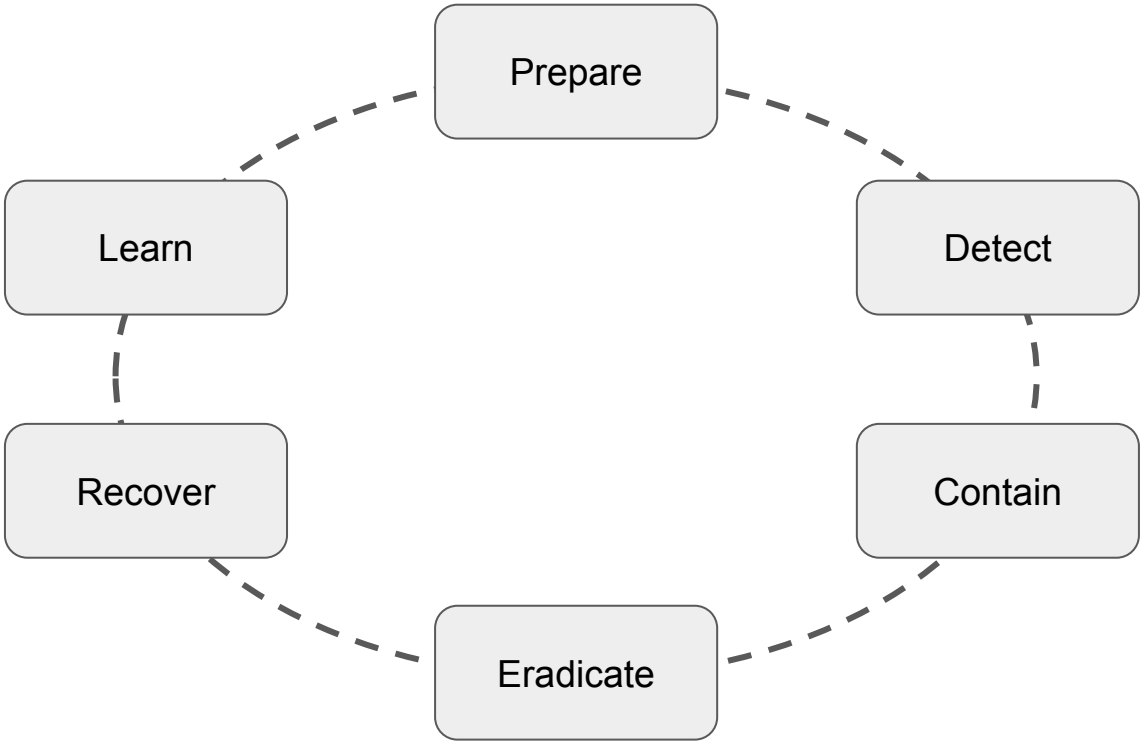
Similar view from Dragos: IR advice

- Establish and maintain knowledge of all the assets in the OT and IT environment.
- Prepare tools and procedures to gather evidence and intelligence from every corner of the OT and IT networks. This includes building relationships across organizations who will support each other in case of an event.
- Pre-establish visibility into OT networks – gathering intelligence after-the-fact in an industrial network is one of the easiest ways of slowing a response.
- Build relationships with vendors, integrators, industry consortiums, government, partners, and security companies which can help respond quickly to a situation.
- Integrate cyber, digital, and physical response and recovery plans assuming threats may cross these boundaries.
- Document and know the decision makers, decision points, and key legal and policy issues.
- Know how and when information will flow – one of the most confusing elements of any situation is communication within and outside an organization.

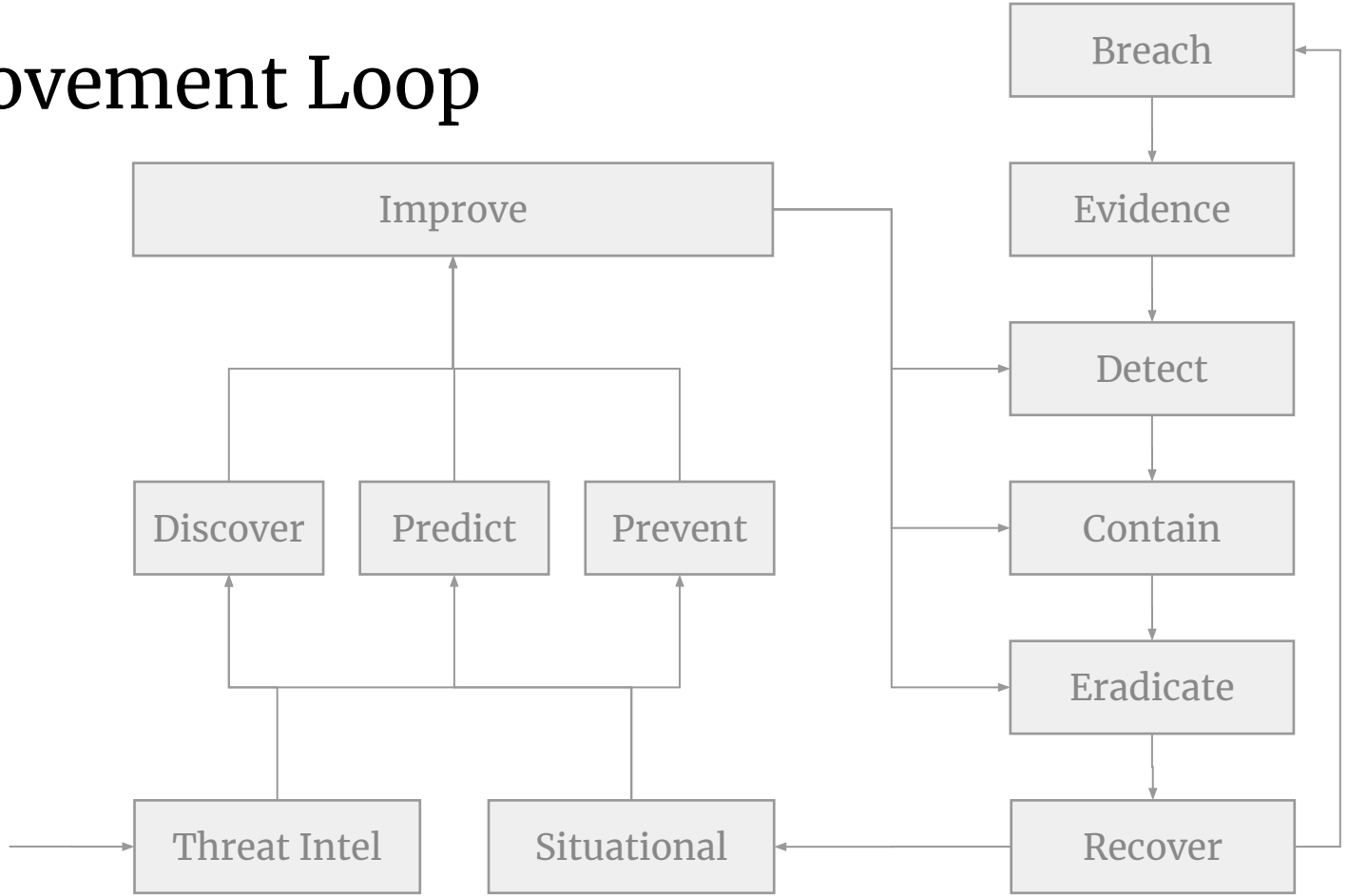
https://dragos.com/blog/industry-news/5-things-ics-operators-and-critical-infrastructure-must-do-in-the-face-of-cyber-escalation/

Practices for OT Incident Response

Incident response cycle



IR Improvement Loop



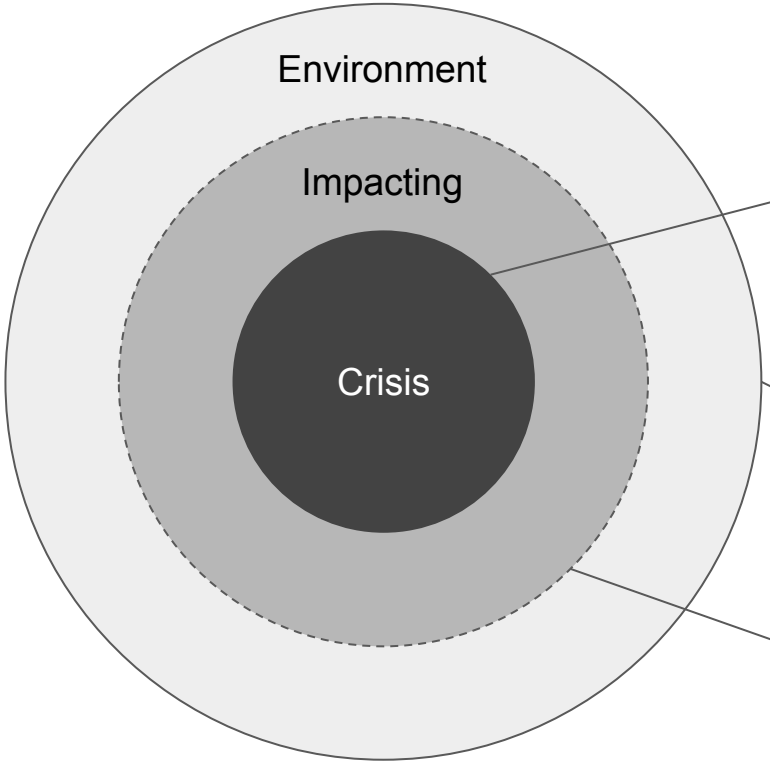
http://frodehommedal.no/presentations/first-tc-oslo-2015

‘Situational’: Operational context

What is ‘situational’ in the case of OT?

- OT attacks don’t happen in isolation: a successful attack depends on pivoting, dwell time and development in its surroundings.
- At the site of crisis you need specific technical skills, but a successful OT attack should prompt you to consider the *entire* environment, not just ‘ground zero’
- Speed and effectiveness of incident response critically depend on effectiveness of day to day SOC operations

Handling OT incidents: Look wider



Directly Affected components:
- Collection
- Analysis
- Containment
- Visibility
- Asset management

Embedding environment:
- Environment health
- Attack path Analysis (pivots, elevations)

Boundary
- Hunting

OT Specialised collection

- This is very environment specific!
- Some tooling is available, e.g. snap7 for Siemens
- Many HMIs run Windows of some sort (CE, XP embedded)
- Try and get some spare equipment off engineering
- Then practice

Environment: Engineering PCs

- Level 0 equipment runs unauthenticated, but generally is embedded in a computer network with PCs to facilitate programming
- These are most likely stand alone, with local accounts, no or out of date AV, no logging, no monitoring and no tooling, and possibly out of date OS, with certainly no recent patches
- But to punch through to these, attackers will have needed to pivot there.

Environment: Software

- Software to manage these environments is specific, and you need to get it from engineering
- Licensing often requires dongles and the like
- There are repositories of pirated software in this area too, and it will come with ‘strings attached’
- Vendors bringing their own remote access software in, e.g. teamviewer

Environment: Memory analysis

Memory forensics is a useful tool on engineering PCs

Especially useful are volatility commands such as

- timeliner
- shimcache

These tend to display software that is run irregularly.

This can then be compared with what is running and what is connecting on the machine

Environment: network

If you can get tcpdumps off the network, then this opens new possibilities

- Network traffic monitoring with specialised solutions
- Network traffic monitoring with open source solutions
- Monitoring with threat hunting applications, such as RITA
- Value captures of PNIO packets

Attack paths: AD

Logging in AD can tell you some of the actions an attacker took, especially privilege escalation (did they add themselves to particular groups?)

Attack path mapping through AD in the IT (level 5 and 4) and OT (level 3) environment also gives a view of risky assets such as

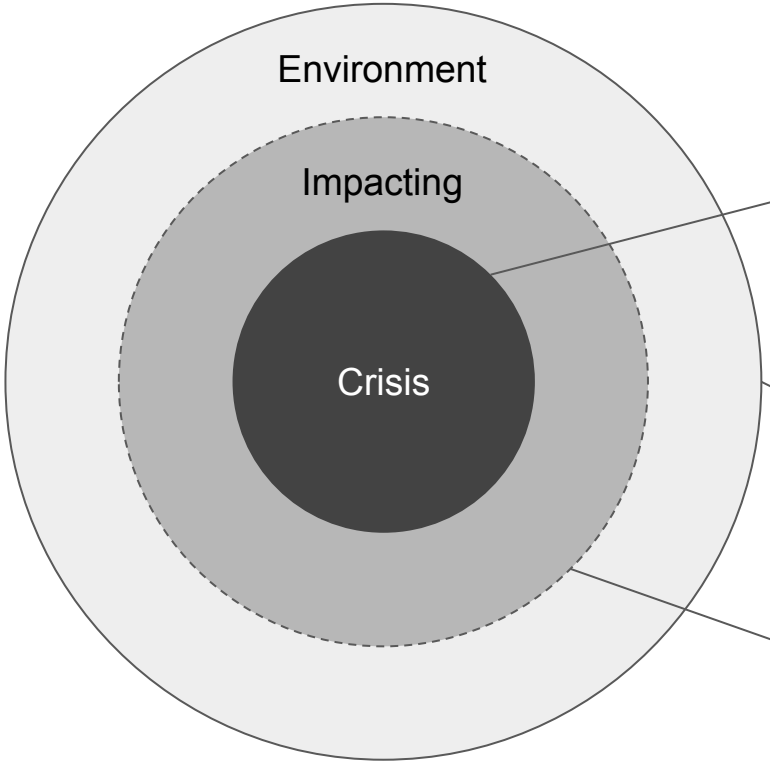
- Machines
- Accounts
- Objects

Conclusion

Different profiles for incident response

- Different priorities: SAIC vs. CIA
- Different consequences: tightly coupled and potential catastrophic consequences vs. loosely coupled and largely manageable consequences
- Different audiences: you do need to work with process engineers to understand what's going on
- All tooling needs to work on legacy technology, potentially a decade or more after it has disappeared from the IT environment

Handling OT incidents: Look wider



Directly Affected components:
- Collection
- Analysis
- Containment
- Visibility
- Asset management

Embedding environment:
- Environment health
- Attack path Analysis (pivots, elevations)

Boundary
- Hunting

Questions?