Improve your resilience with cyber security table-top excercises

Stefan Schörling, Mattias Borg

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Stefan Schörling
Microsoft MVP · Security – SIEM & XDR

Role
Manager

Focus
Security

Blog, Hobbies and more
Being awesome

Mattias Borg
Microsoft MVP · Security – SIEM & XDR

Role
Magician

Focus
Cyber Security & Research

Blog, Hobbies and more
Write stuff, Build stuff, Break stuff, Paint stuff

Agenda

- What’s is a table-top exercise
- Incident management fundamentals
- How to conduct a table-top
- Table-top scenario examples
- Summary

Hey ChatGPT

"A tabletop exercise in cybersecurity is a simulation-based training activity where participants discuss and work through various scenarios related to a cyber incident."

A tabletop exercise is also referred to as gold teaming

Incident Management Fundamentals

Approaches and methodologies

Crisis

- Deviates from the normal
- Sudden and unexpected
- Threatens survival and fundamental values
- Requires quick decisions
- Loss of ability to operate
- Economic impact

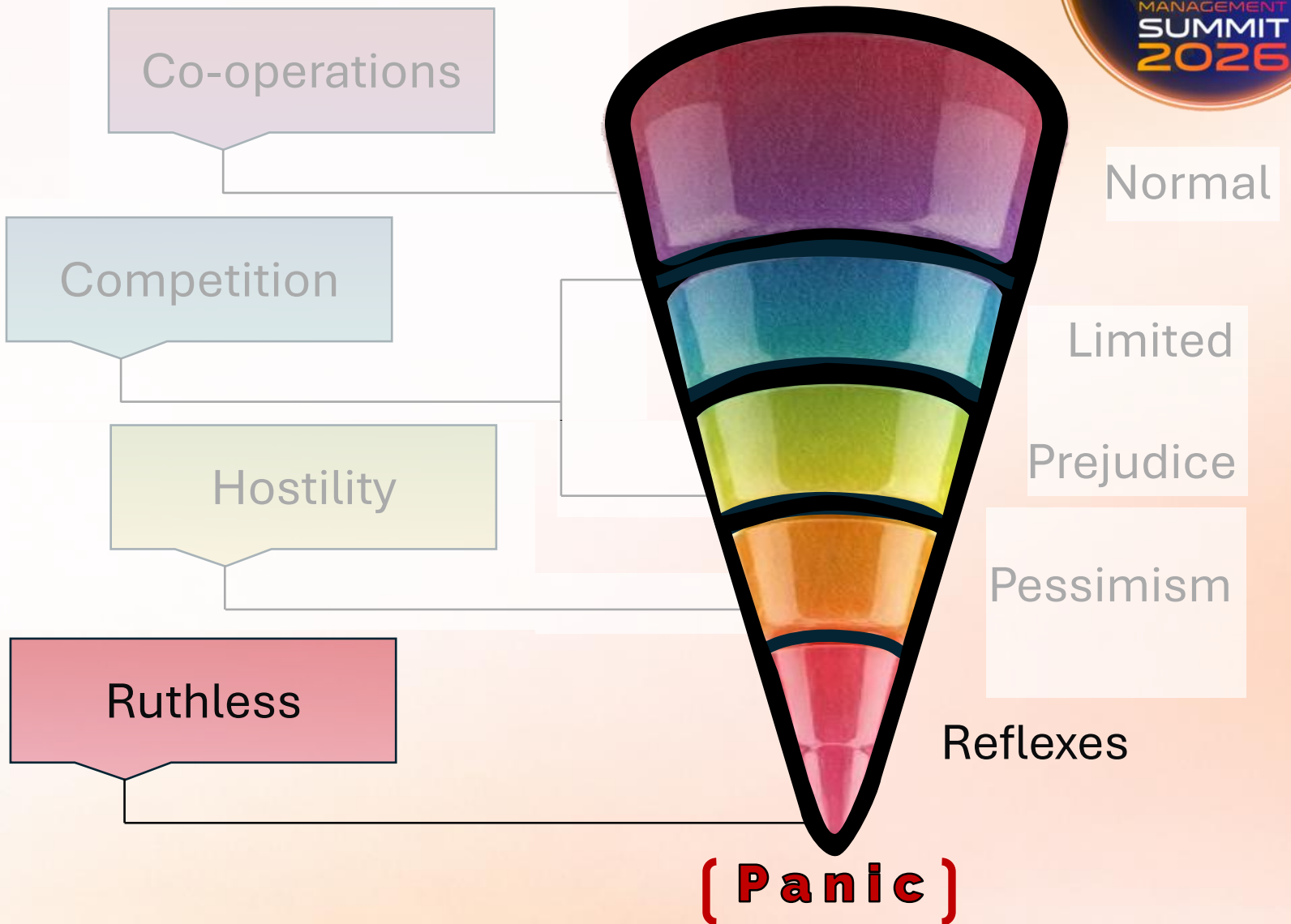
Overwhelming reaction to a threatening situation

Humans and the stress of a crisis

Incidents and crisis Management

=

Increased stress levels

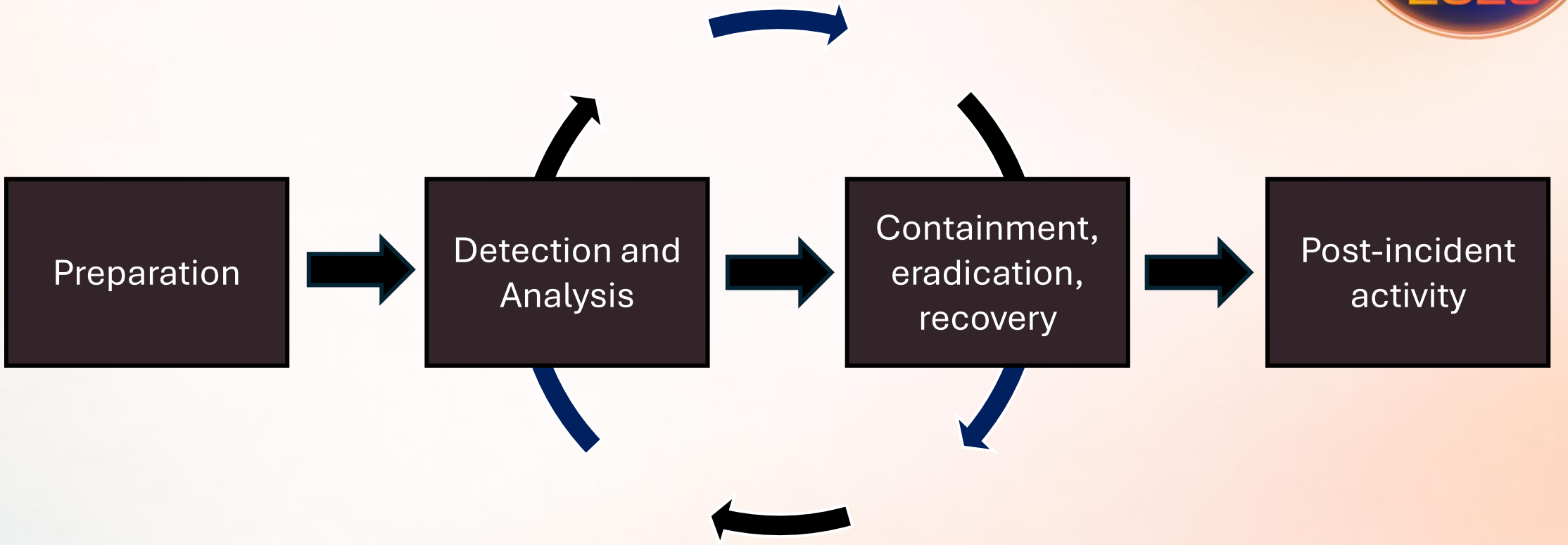


OODA Loops

- **Observe:** Collect data from relevant sources before any decisions are made.
- **Orient:** Identify useful and relevant data and organize according to rules and filters
- **Decide:** Define an action plan based on the data available
- **Act:** Follow through on decision; observe responses and re-orient if needed.

If your OODA loops are faster than your adversary's, *YOU WIN*.

Incident Response Lifecycle



Preparation

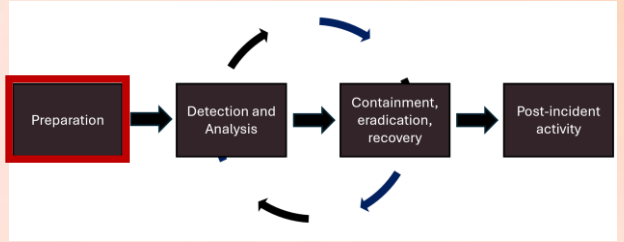
Sun Tzu** (Art of War)**: "Every battle is won before it is ever fought."

The **Preparation** phase is arguably the most important step in incident response.

Topics to discuss may include:

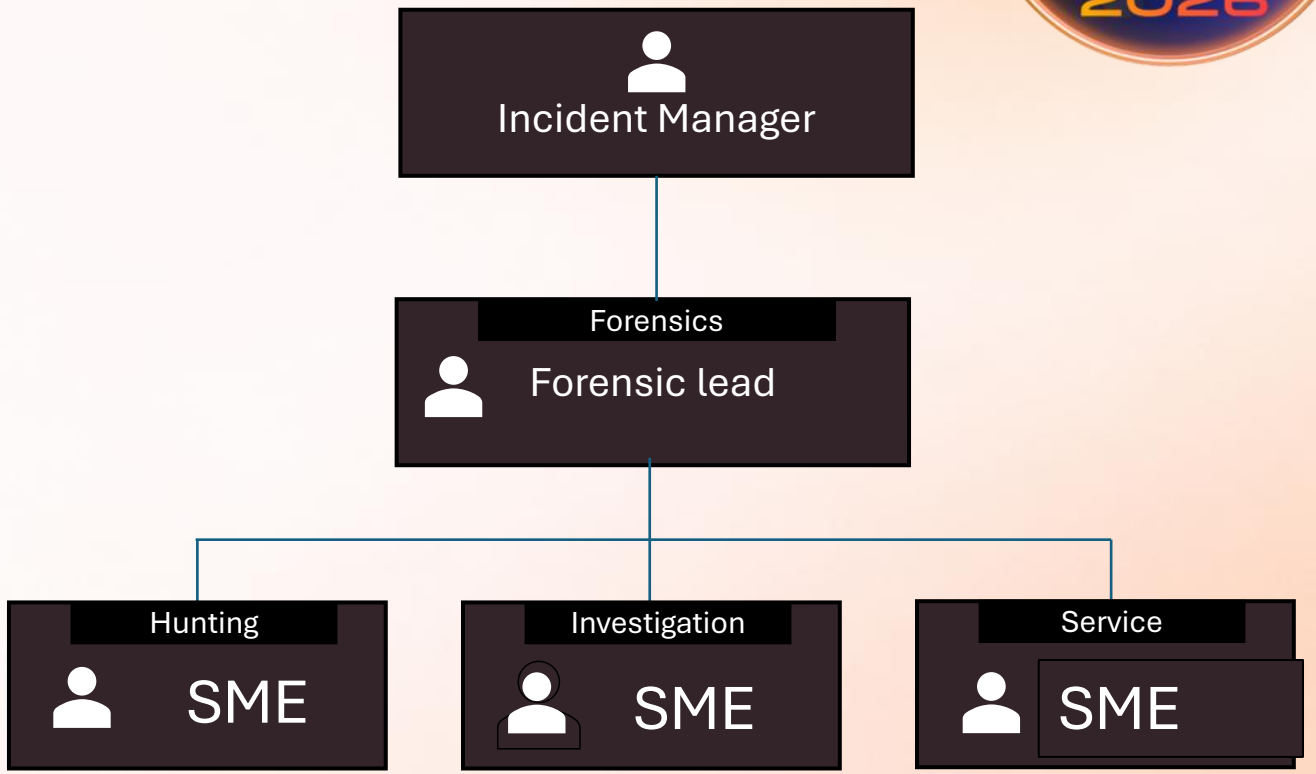
- Policies and Procedures
- Technical Capabilities
- Communication plans
- Organizational aspects
- Continuity plans

- **Questions to consider**
- Have all users been trained on security policies and how to be compliant?
- Have your security policies and incident response plan been approved by management?
- Does the IR team know their individual roles and have the necessary tools, ready to go?
- Have the IR team members participated in mock drills, TT exercises, etc…?



Organize yourself

- **Incident Manager**: Owns the incident for the impacted workload, coordinates response and recovery effort and owns investigation end-to-end
- **Forensic Lead**: Drives the investigation, and the forensic investigation.
- **SMEs**: Individuals with expertise in incident response, forensics, revers engineering and specific workload knowledge etc.
- **And possibly many more..**
  - **Legal**
  - **Public Relations**
  - **Sourcing Partners**
  - **App Vendors**
  - **Etc.**



Tool - Situational Report (Sit Rep)

Known facts

- ...

Decisions made

- ...

Assumptions

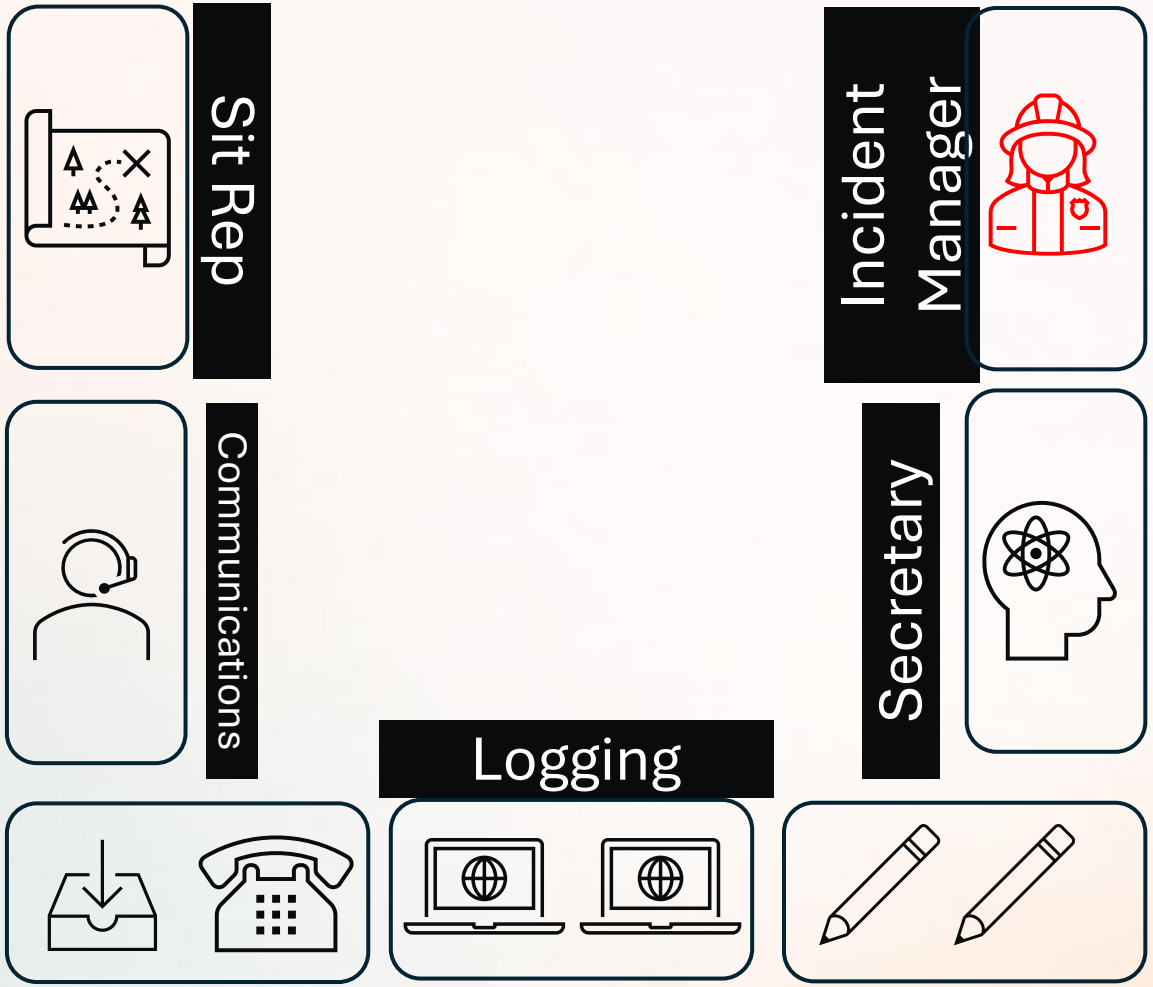
worst, best, most likely

- ...

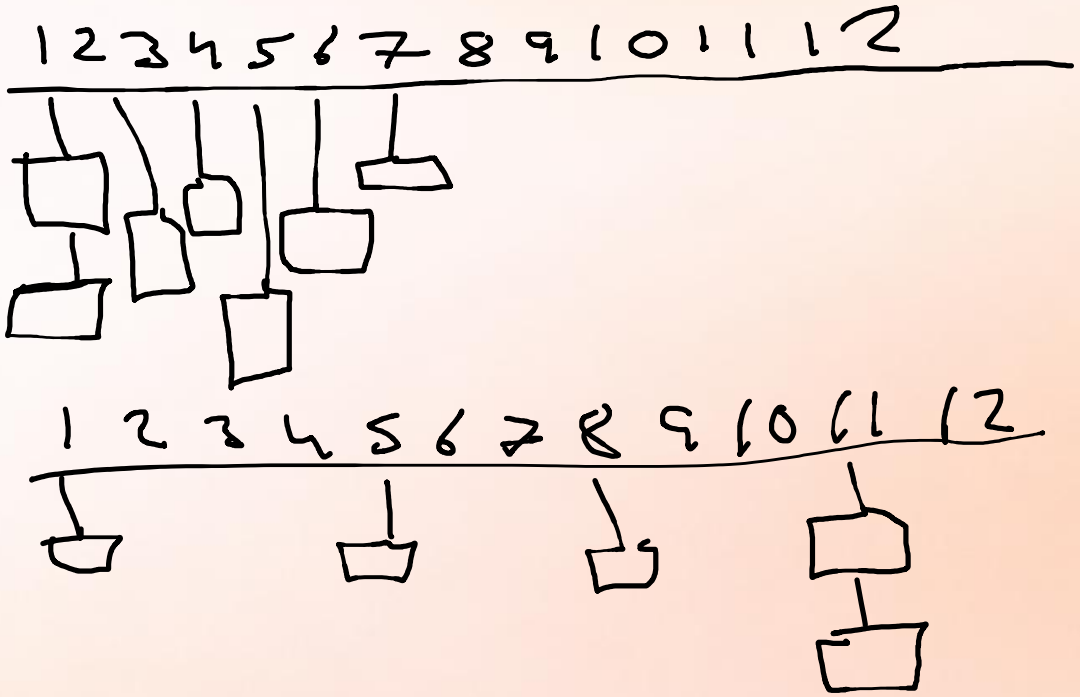
Communication

- ...

Method – Staff service



Analog Timeline



Detection and Analysis

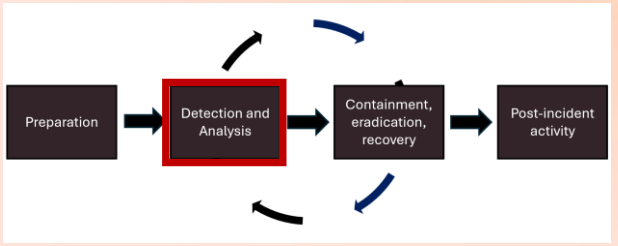
Sun Tzu** (Art of War)**: "If you know your enemies and know yourself, you will not be imperiled in a hundred battles."

In the **Detection and Analysis** phase, you triage based on known facts and extend scope and systems when needed

Gathering of initial event information
Visibility
Triage of events
Hunter team to do post breach hunting
Gather more data if required and repeat

Questions to consider:

- When did the event happen? How was it discovered?
- How did it happen?
- What is the scope of the compromise?
- What did the attacker do?
- Has the point of entry for the event been discovered?



Containment

Sun Tzu** (Art of War)**: "If you know your enemies and know yourself, you will not be imperiled in a hundred battles."

In the **Containment** phase, prevent more bad things from happening.

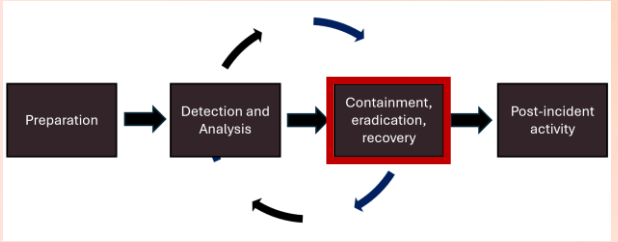
Which steps do we need to take to contain this specific threat?
Containing (secure) none-affected systems to protect the data?
Do we have all information required for the decisions?

- Cut-off internet?
- Isolate networks/systems?

How can systems be contained?

Questions to consider:

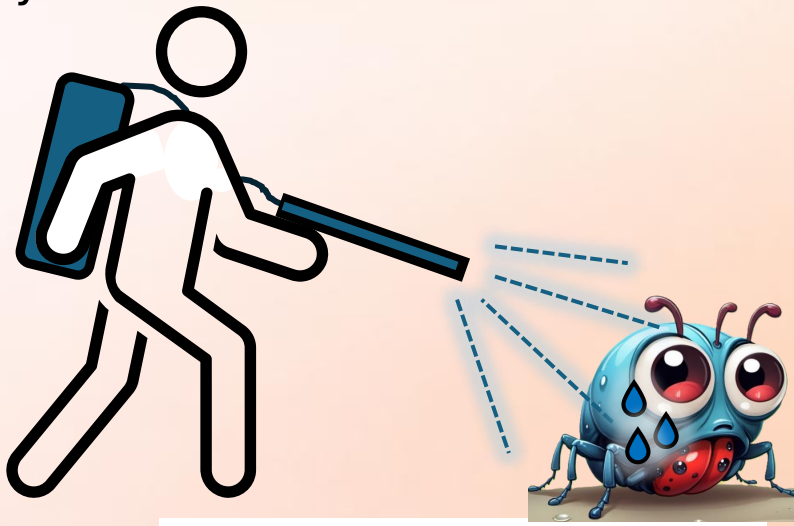
- Contain the breach in the near term? In the longer term?
- Do we need to avoid alerting attacker that we are on to them?
- When are the adversaries active?
- What is the risk to continued operations of the compromised systems?
- What is available in the toolbox



Eradication

Sun Tzu** (Art of War)**: "Quickness is the essence of the war."

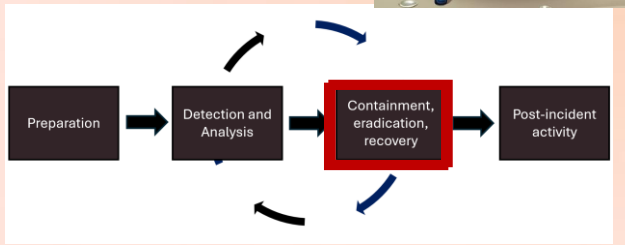
In the **Eradication** phase, the adversary is effectively removed from the environment. This is a large, coordinated effort where all the infected systems are cleaned ***AT THE SAME TIME***.



Is enough information available?
Are attacker paths secured and/or closed?
Cleaning systems
This must be done in cooperation with service and the response team

Questions to consider:

- Do we know how the attacker performed the attack so that we are securing the correct paths?
- What are the steps to be performed to evict the attacker?
- How is evidence handled?
- Has the environment been hardened to prevent a reoccurrence?
- Have artifacts/malware/rootkits from the attacker been securely removed?



Recovery

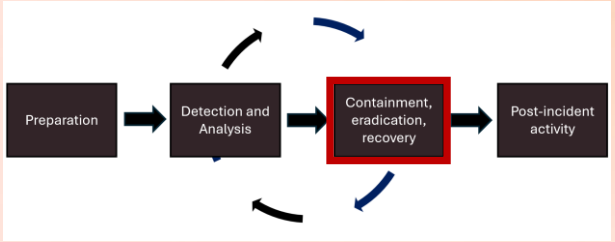
Sun Tzu** (Art of War)**: "The opportunity to secure ourselves against defeat lies in our own hands."

In the Recovery phase, we are restoring and returning affected systems and devices to the operational environment.

- When can recovery start?
- Can we trust backups?
- What was the last known good state?
- Can we restore from backup to this state?
- What will determine best recovery path? (Restore, Rebuild, Remove)
- Implement monitoring to fix previous visibility gaps

Questions to consider

- When can systems be returned to production?
- How will we confirm that vulns are not re-introduced in the last-known good state?
- How will we test for signs of repeat events?
- Can systems be restored from a trusted backup?
- What will be included in our monitoring and is alerting set up correctly?



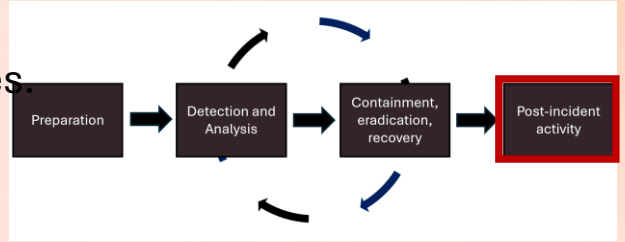
Post incident activities

Sun Tzu (Art of War): "Victory usually goes to the army who has better trained officers and men."

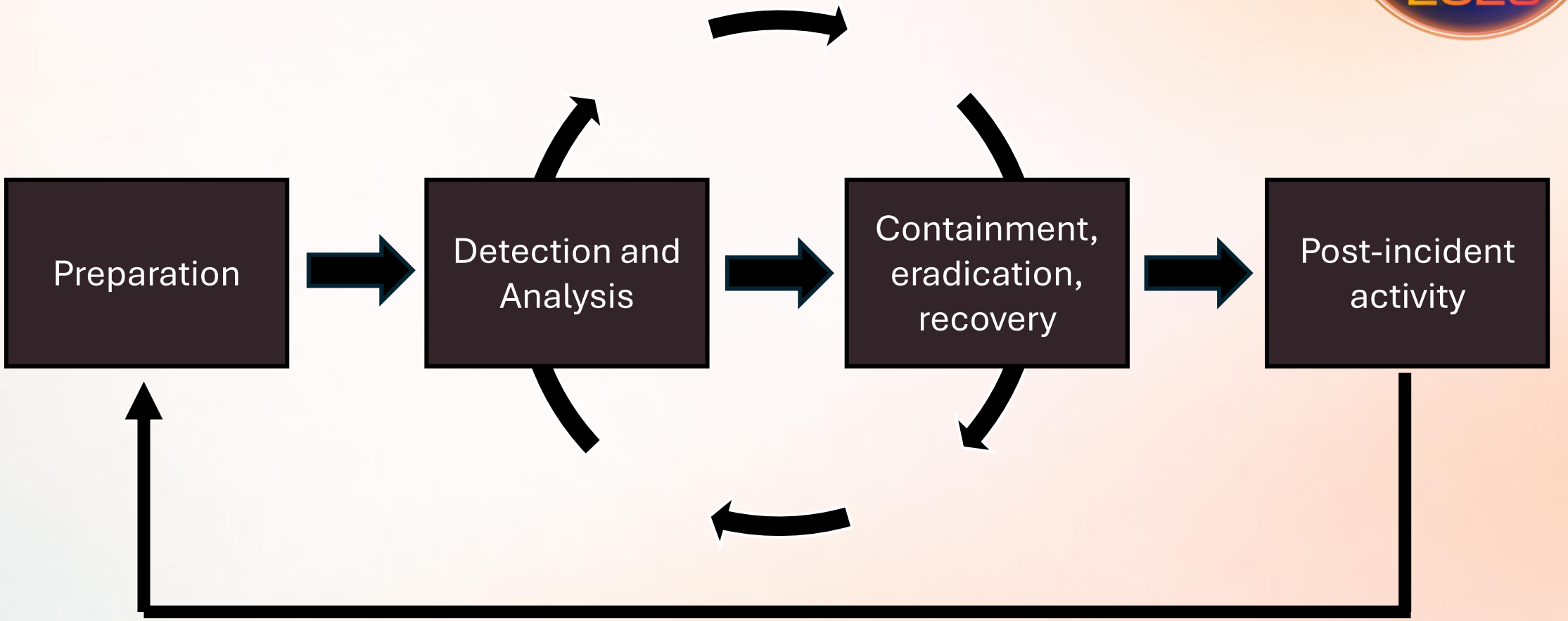
In the **Post-incident activity** phase, we are preventing reoccurrence and evaluating how to improve defenses based upon the actual incident.

- Incident report
- Lessons learned
- Determining follow up steps

- **Questions to address**
- What are the recommended changes to improve security?
- Technical gaps, procedural failures, manual errors, process flaws, and communication glitches.
- Is training required for employees involved in the incident
- How can we ensure that a similar breach doesn't happen again?



Process improvement is continuous
It's a *circle*, not a *line*



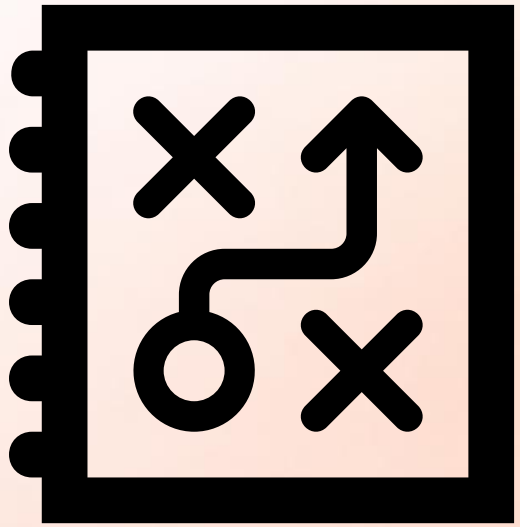
Microsoft IR Playbooks

- Incident Response Playbooks provide structure and a tested process to help ensure incident responders respond in a consistent manner to incidents and make fewer mistakes during high-pressure situations.

Microsoft incident response playbooks

IR Playbooks from Microsoft include:

- Phishing
- Password spray
- App consent grant
- Compromised and malicious applications



Each playbook includes:

- Prerequisites
- Workflow
- Checklist
- Investigation steps

Other IR Playbooks

CERT Societe Generale has created a set of Incident Response Methodologies that can be used as a template for building your own. (https://github.com/certsocietegenerale/IRM)

18 existing IRM's include:

- Social engineering
- Phishing
- Ransomware
- DDoS
- Blackmail
- Insider Threat
- Worm infection
- Windows compromise
- Etc…

How to conduct a tabletop

Elements of Tabletop

Pre - tabletop

- Purpose
- Goal
- Target Audience
- Pre-assessment
- Plan exercise scenario

Tabletop exercise

- Exercise
- Debriefing

Post - Exercise

- Report
- Next Steps

Tabletop goals

Define the goal for the exercise, use chain of events and tasks to reach the goals.

- Identity capability gaps (Technical, Org, Processes)
- Prove something someone is aware of
- …

Remember it is ok to fail, we are here to practice!

Tabletop Target Audience

Very important element to be able to prepare and to play a relevant scenario to be able to reach the goals of the exercise!

Management vs Technical
Role specifics

Tabletop purpose

Define the purpose for the exercise

- Test an existing plan
- Establish Awareness for - Management | Board | Org
- Test Human behavior

Tabletop pre-assessment

Probe the knowledge of target audience

- Analyze existing documentation
- Pre-assessment in advance
- Interviews
- Assessment during day
- Hand raise

Make the plan

Audience focused

TI Based Preface

Relevant Initial Event

Goal oriented chain of events

Go Play!

Organizing Team

Game Lead

- Plans and leads the exercise

Documentation Lead

- Documents conclusions and discussions of relevance

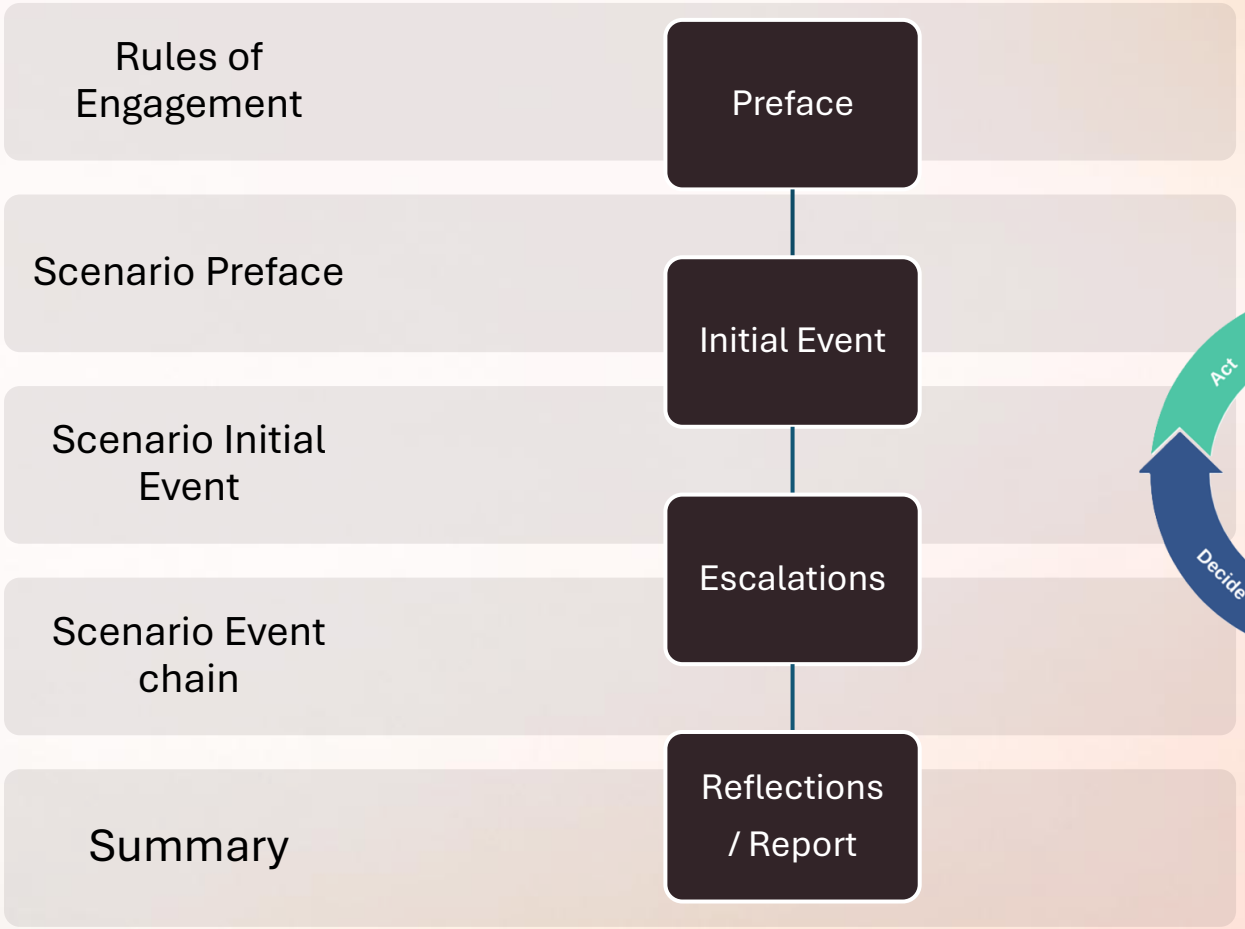
Optional: SME

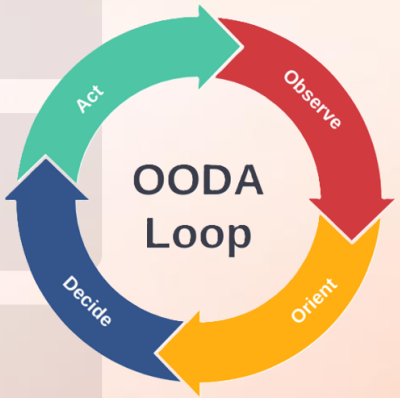
- Supports the Game lead with relevant chain of events or mimics certain roles with role play.

Target Audience

- Participates and works in groups, either mixed groups or in the line org depending on goal.

Exercise format





Tabletop example scenario

Situational preface

Cybersecurity in Europe faces increasing threats, primarily from state-sponsored actors, particularly Russia and China.

Key targets include critical infrastructure, government systems, and financial institutions. Cyberattacks, disinformation campaigns, and espionage are major concerns.

The European Union is strengthening defenses, with countries like Estonia leading in innovation, and a growing focus on protecting vital infrastructure like energy grids.

The EU is also working on regulatory frameworks, like the *NIS Directive* and *Cybersecurity Act*, to enhance digital resilience across member states. However, cyber threats remain a critical security challenge for the region.

Initial Event - Friday 13 Sept 08:30

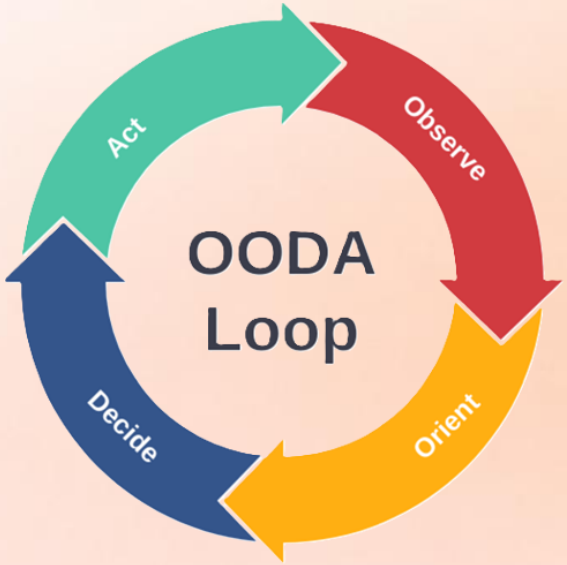
ENISA, and the "country CERT" have during the last weeks seen an increasing number of ransomware attacks targeting enterprises and organisations, vital for critical functions within the society.

Early Friday morning “Your CEO” contacts the Cybersecurity function. An adversary has sent him and others in the management team a note by e-mail. The note states the adversary has taken control over the network and exported large amounts of data. At the end there is a demand for extortion payment with a link with further instructions to pay $10M in bitcoin or the actor will make further harm

Observe, Orient, Decide, Act

- Initial actions by team?
- Which contacts, internal or external are made?
- Need of additional resources?
- Any routines, checklists or tools are used

Team presentation of key decisions in 25 minutes



Escalation of events

Friday 13 Sept 09:05

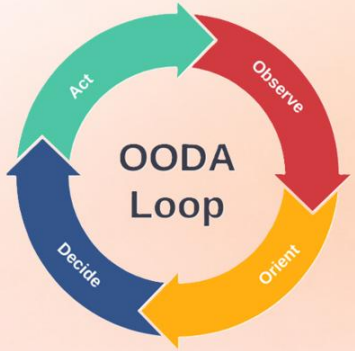
An anomaly has been foun
uploaded over 150GB of dat

On the server 35 administra
past week. A handful of th
access to all servers.
with privileged administrati

Observe, Orient, Decide, Act

- Initial actions by team?
- Which contacts, internal or external are made?
- Need of additional resources?
- Any routines, checklists or tools are used

Team presentation of key decisions in 25 minutes

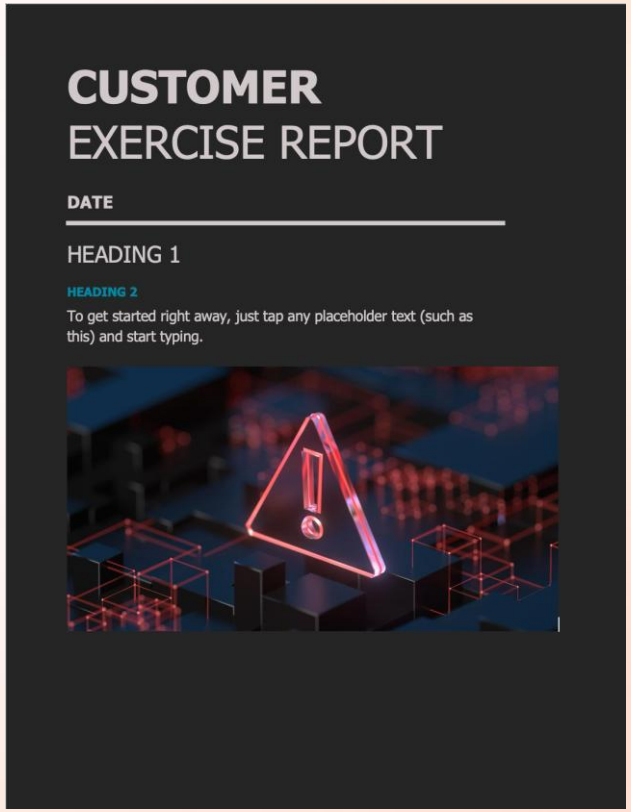


Event chain escalation examples

- Further evidence discovered
- Access to key resources
- Media attention (TV, Radio, Newspapers)
- Vendor actions
- Customer actions

Exercise Summary

- Debriefing (Attendees, Game Masters)
- Lessons Learned (Attendees)
- Exercise Report (Game Masters)



Session Summary

- Keep calm
- Use the plan, if you don’t have a plan get a plan!
- Involve the right resources including getting help when needed

Train, Train, Train and continue training in your daily work

Tabletop resources

- CISA – Tabletop Exercise Package
  - https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages

- Backdoors & Breaches
  - https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

Session summary

Use, tabletop exercises to improve organization and individual abilities!

Agenda

- My First Point
- My Second Point
- And so on …

Demo

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!


MODERN
ENDPOINT
MANAGEMENT
SUMMIT
2026

Sponsors

onedeploy
Windows Deployment Reimagined

ZERO TOUCH

Insight

control up

PATCH MY PC

Rimo3

robopack

numecent

Microsoft

Michael Scott
Microsoft MVP · Endpoint & Security

Role
Manager

Focus
Intune · Windows 365 · Security

Blog, Hobbies and more
Being awesome

Agenda

- My First Point
- My Second Point
- And so on...

Demo

Please rate this session on Sched.com

We would love to hear what you liked and how we could improve!

Thanks!