Automated Response based on SecuriCAD Recommendations
Workshop on Next Generation Security Operations Centers (NG-SOC 2019) | Ir. F. Fransen
EVOLUTION OF RESILIENCE STRATEGIES

Traditional prevention
put up walls and hope for the best

Monitoring & response construct
detect (potential) attacks and limit damage

Threat intelligence capabilities
anticipate and take proactive precautions

Autonomous response & recovery
reduce dependency on human operation

- shortage of skilled resources
- increasing volume of security events
- detection & response time is lagging behind
- ICT infrastructure increasingly complex

often induced by (severe) incident
SECURITY AUTOMATION & ORCHESTRATION
MAPE-K / OODA
SECURITY AUTOMATION & ORCHESTRATION
TNO’s view

Trigger events:
1) attack detection
2) new threat / CTI
3) new vulnerability
4) system or config. change
**SECURITY AUTOMATION & ORCHESTRATION**

**TNO's view**

1) automation to provide insight in state of security (situational awareness)

2) automation to provide insight in the best Courses of Action (CoAs) (option awareness)

3) automation to (semi) automatically respond to attack or mitigate the threat / vulnerability

Automated Security (MAPE-K control loop)

Monitor, Analyse, Plan, Execute

Managed Resources

SOAR tools for playbook driven automation

SOC analyst, system owner / administrator

Authorize response action

(NEW) Security Automation & Orchestration tools

TNO, innovation for life
SECURITY AUTOMATION & ORCHESTRATION

Also referred to as Security Orchestration, Automation & Response (SOAR) tools

IDS/ SIEM

ICT Infrastructure

Reconfiguration
Automating Security Operations

Observe
Point Products
- Firewall
- IDS / IPS
- Endpoint
- WAF
- Advanced Malware
- Forensics
- Malware Detonation

Orient
Analytics
- SIEM
- Threat Intel Platform
- Hadoop
- GRC

Decide

Act
- Tier 1
- Tier 2
- Tier 3

Automated

Automated with Phantom

Same People x Less Time = Lower Cost
Automating Security Operations

Observe: Point Products

Orient: Analytics

Decide

Act

Phantom

extrahop_detect_data_exfiltration

Repo: community

90%

Same People x Less Time = Lower Cost
AUTOMATIC PLAYBOOK GENERATION
Project concept

Infrastructure model

JSON

TNO Research Cloud

ICT infrastructure

Re-configure

Playbook Generator

• Suggested Mitigations
• Missing Security Controls

Playbook

Phantom

secuICAD®
ENTERPRISE
SECURICAD – RECOMMENDATIONS

- API call to fetch simulation results in json
- Suggested mitigations are high-level / abstract, not all technical (e.g. train users to be security-aware)
SECURICAD – RECOMMENDATIONS
We are able to generate a playbook for a recommended CoA by combining pre-defined Python code and assigning parameters for the particular case.

Phantom does not provide an API to load a (externally) created playbooks. Phantom does have a rest API to run a playbook. We have to ‘trick’ Phantom in executing our (externally) generated playbook.
AUTOMATIC PLAYBOOK GENERATION

Tool chain

API calls
- upload model
- start simulation
- view simulation results

Playbook for:
- securiCAD & playbook generation

Tricked in running automatically generated playbook

API call to run playbook

Playbook Generator

TNO Research Cloud

Automated Security
AUTOMATIC PLAYBOOK GENERATION

Conclusion

- State of the art is not yet ready for this automated response scenario
- SecuriCAD recommendation are a bit high level / abstract
- Playbooks can be automatically generated, but Phantom is not designed for this scenario

has some work to do
THANK YOU FOR YOUR ATTENTION

Take a look: TIME.TNO.NL

innovation
for life