Operational Security Games

Pratyusa K. Manadhata
manadhata@hpe.com
A tier-1 analyst sees an alert

192.168.0.23:43987 –> 203.45.65.201:1433 SQL Injection Attack 23Mar09 1930:003 user=Calvert
The tier-1 analyst builds a context

192.168.0.23:43987 → 203.45.65.201:1433 SQL Injection Attack 23Mar09 1930:003 user=Calvert

- DeepSight
- Other Logs
- Payload
- Historical Context
- Contemporary Events
- Asset Inventory
- Port Scan
- Port Lookup
- Signature Details
- Traceroute
- nslookup
- Dshield
- Vuln Scan
- Traffic Analysis
- Address Book
- Remedy
- Pattern Analysis
- Active Directory
- Who owns this system?
- Are there any current changes?
- What is the status of this user?
- What does this person do?
- What is the timing on this?
A tier-2 analyst takes remediation actions

- Quarantine the infected machine
- Schedule/run clean up tools
- Schedule/run reimaging
1.5 billion events/day
~200 actionable alerts
~10 minutes/alert for escalation
SOCs: Repetitive, manual, and error prone

KEEP CALM AND GAME/DECISION THEORY
Remediation as ‘planning under uncertainty’ or ‘games’

Input: events and alerts from the network
partial view of the network
costs of sensor placement, false positives, and false negatives
adversary’s goals and actions
...

Output: Remediation action plan

Approach: Decision making under uncertainty
Two player games
Challenges

– Generating realistic models/inputs

– Model updates in response to network changes

– Scalable, reliable, and timely

– Interpreting results

– Incorporating analyst feedback
Thank you

Pratyusa K. Manadhata
manadhata@hpe.com