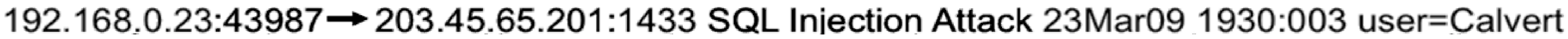
Hewlett Packard
Enterprise

Operational Security Games

Pratyusa K. Manadhata
manadhata@hpe.com

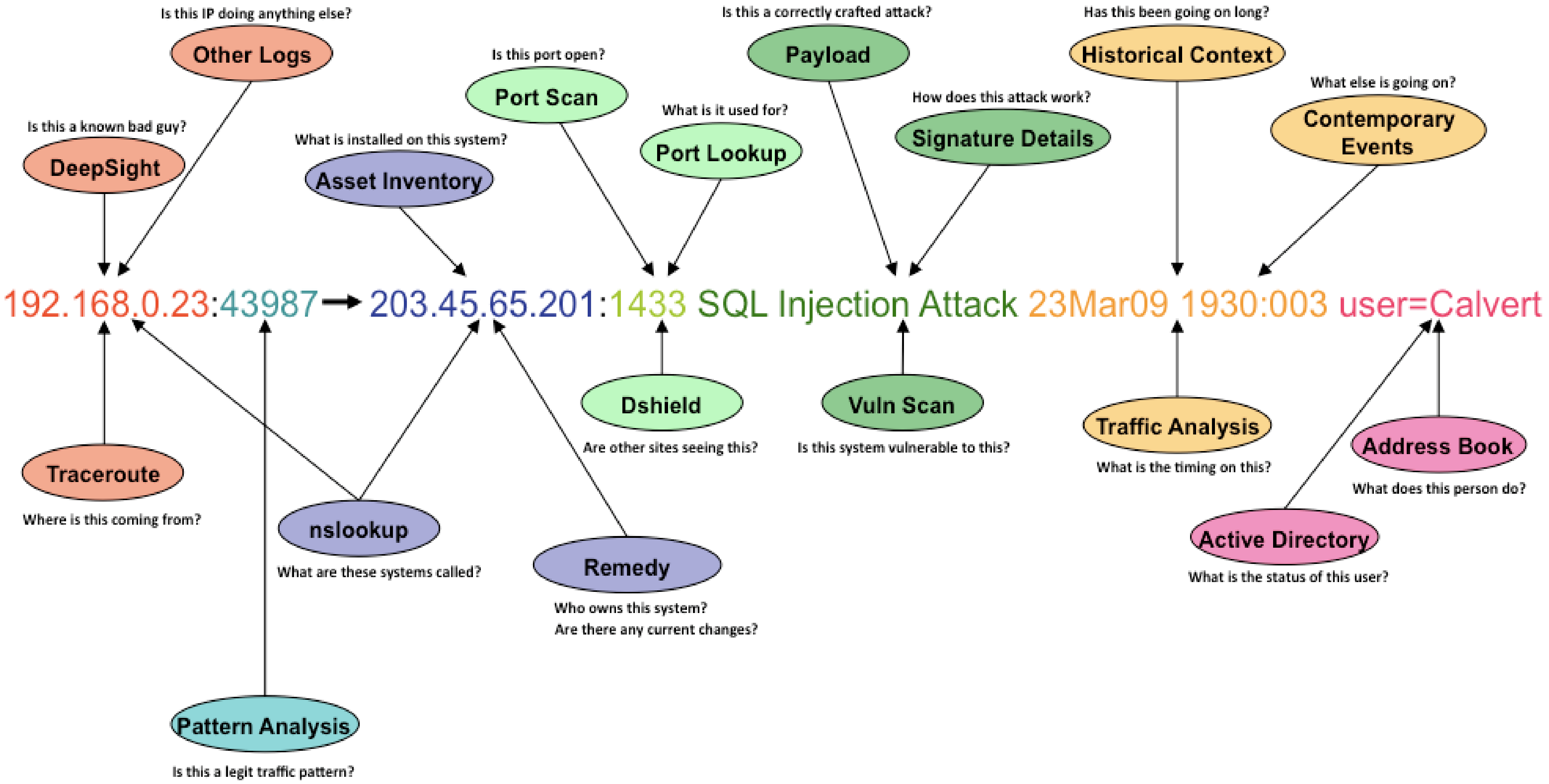
01:36
MOSCOW
05:36
SINGAPORE
06:36
TOKYO
14:36
PALO ALTO
16:36
HOUSTON
17:37
23:36
BERLIN
Mail Calendar People Tasks

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


Is this IP doing anything else?
Other Logs
Is this port open?
Port Scan
Is this a correctly crafted attack?
Payload
Has this been going on long?
Historical Context
What else is going on?
Contemporary Events
Is this a known bad guy?
DeepSight
What is installed on this system?
Asset Inventory
What is it used for?
Port Lookup
How does this attack work?
Signature Details
192.168.0.23:43987 → 203.45.65.201:1433 SQL Injection Attack 23Mar09 1930:003 user=Calvert
Dshield
Are other sites seeing this?
Vuln Scan
Is this system vulnerable to this?
Traffic Analysis
What is the timing on this?
Address Book
What does this person do?
Traceroute
Where is this coming from?
nslookup
What are these systems called?
Remedy
Who owns this system?
Are there any current changes?
Active Directory
What is the status of this user?
Pattern Analysis
Is this a legit traffic pattern?

Hewlett Packard Enterprise

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

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

Hewlett Packard
Enterprise

Thank you

Pratyusa K. Manadhata
manadhata@hpe.com