SINGAPORE POLYTECHNIC SP

Security Information & Event Management (SIEM)

VALUE

CHALLENGES

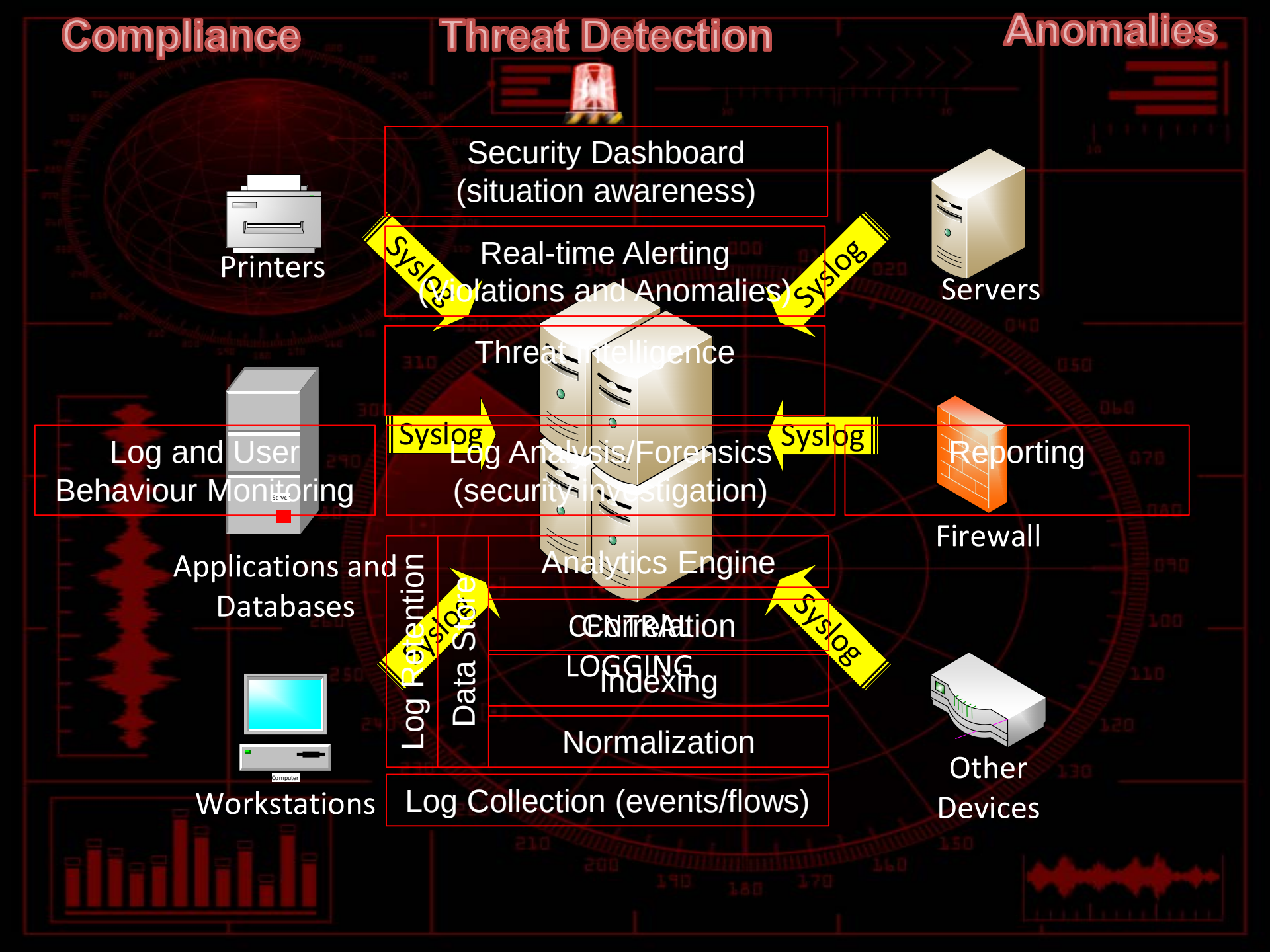
Jason Tseng (jason_tseng@sp.edu.sg)

IHL CIO Forum 2016

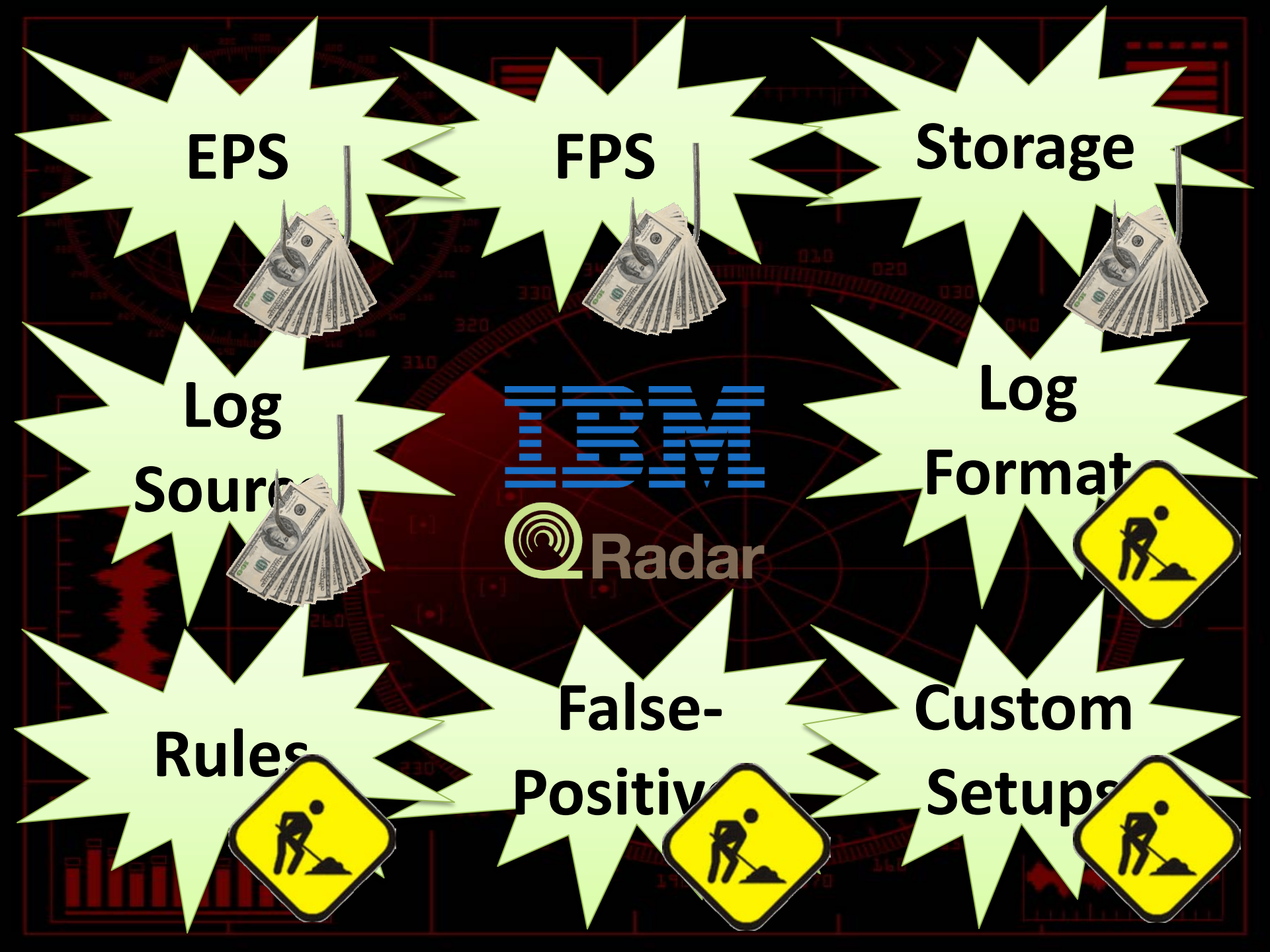
Agenda

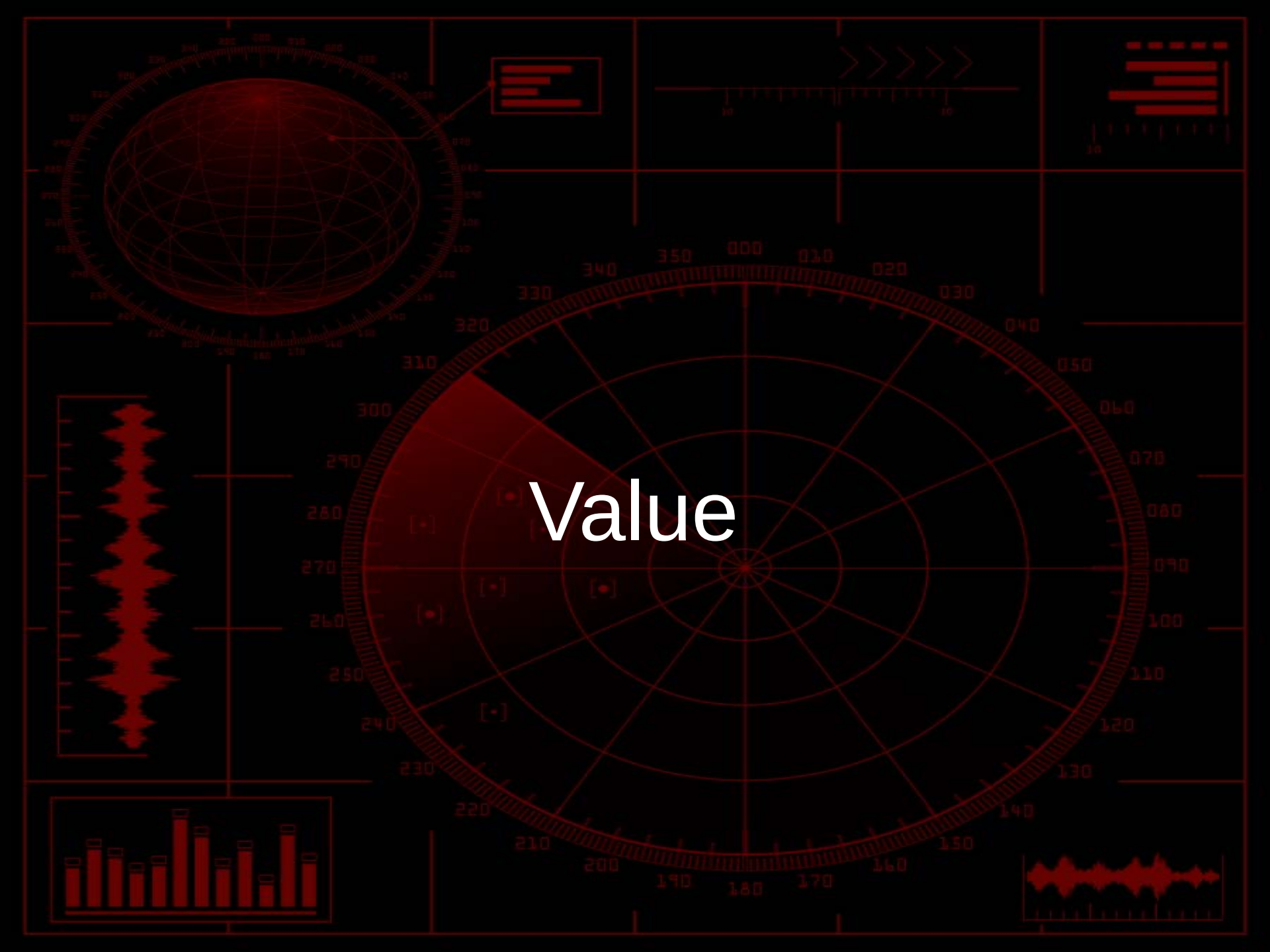
- What is and Why SIEM?
- SP’s Implementation Experience
- Value
- Challenges

What is and Why SIEM


Compliance
Threat Detection
Anomalies
Security Dashboard
(situation awareness)
Real-time Alerting
(Violations and Anomalies)
Threat Intelligence
Log Analysis/Forensics
(security investigation)
Analytics Engine
Central
LOGGING
Indexing
Normalization
Log Collection (events/flows)
Log Retention
Data Store
Syslog
Syslog
Syslog
Syslog
Syslog
Printers
Servers
Log and User
Behaviour Monitoring
Reporting
Firewall
Applications and
Databases
Workstations
Other
Devices

SP’s Implementation Experience


EPS
FPS
Storage
Log Sour
IBM
QRadar
Log Format
Rules
False-Positiv
Custom Setups


Value

Automated Log Monitoring

Authentication Brute-forcing

Early Kill-Chain Detection

C2 Communications

Baseline Anomalies

User Behaviour Analytics


Challenges

Non-Issue Alerts

Non-Actionable Alerts

Fine-tuning and Troubleshooting

Offense Chaining

Poor Reporting Features

Manual Review Required

In summary…

- SIEM is an excellent threat and anomaly monitoring tool
- Consider carefully EPS/FPS, Log Sources and Storage requirements
- Pro-actively review and act on alerts
- Be prepared to customize/troubleshoot rules and log parsers

Thank You !

I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...
I have no questions and will not use the Internet again...