INCIDENT DETECTION & RESPONSE

Top 10 Fails – and how to avoid them
YOUR IDR TEAM FOR TODAY

Tom
- Windows
- Firewall

Anna
- Linux
- Vulnerability scans

Max
- Database
- Endpoint protection
THE SCENARIO: ANOTHER EVENING IN THE SOC
20:10 – WebServer Alarm
SQL injection

Checking: SQL service
Action: False Positive

WHAT THE ATTACKER ACTUALLY DID

Scan for directories ...
success

Upload malicious software
WHAT TO DO ABOUT IT

- **Verification**
  - ✓ Involve others

- **False positives**
  - ✓ Clear incident list

- **Toolstack**
  - ✓ Know & be critical of tools
**WHAT THE ATTACKER ACTUALLY DID**

- **20:50 - Portscan at internal firewall**
  - Success: open port for communication to internal SQL server
  - Access to SQL server

- **21:00 - Manual check at the firewall**
  - Potential portscan from WebServer
  - No action

**IDR VIEW**

- **21:00 - Manual check at the firewall**
  - Potential portscan from WebServer

- **Closer investigation:**
  - Increased traffic to SQL server
  - No action
WHAT TO DO ABOUT IT

- **Time stamps**: ✓ Pay attention to time stamp
- **IDR processes**: ✓ Optimise playbook
- **Collecting evidence**: ✓ Documentation
22:00 - SIEM Alarm
SQL server connecting to known C&C server

Action:
Escalation process

WHAT THE ATTACKER ACTUALLY DID

Cover tracks

Persistence
Try to download additional tools for pass-the-hash attack

Spreading
Using previous credentials to create own accounts and compromise the core network
WHAT TO DO ABOUT IT

- Business Impact Analysis
  - Should be available

- Communication across levels
  - Train communication

- Team communication
  - Exchange information in the team
AND MOST CRUCIAL OF ALL

Connecting the dots ✓ Coordinator role

and learn from your mistakes!
MORE INFORMATION @ CYOSS

HALL 10.1 / STAND 404

CYOSS GmbH
Ganghoferstr. 66
80339 Munich, Germany

Tel: +49 89 92161-2613

office@cyoss.com
cyoss.com