Presentation of the demo

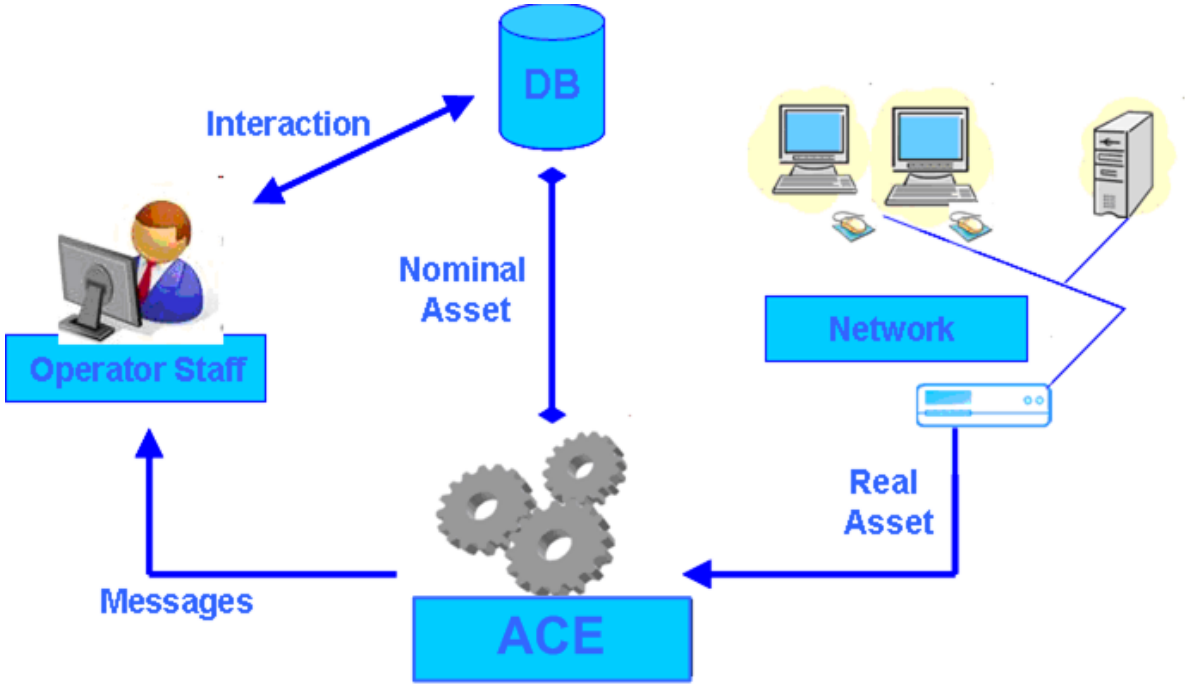
27 May 2014

ICT Demo Performed Scenarios

- Scenario 1: Asset Control
  - Unauthorised PC Connection or Disconnection of authorised devices;
- Scenario 2 : Asset Integrity
  - Cyber Attack: Conficker exploit against Win XP through a customized Metasploit distro.

Demo tools: ACE

Asset Control Engine detects differences in real time between real and nominal asset in the network, and outputs related alarms.

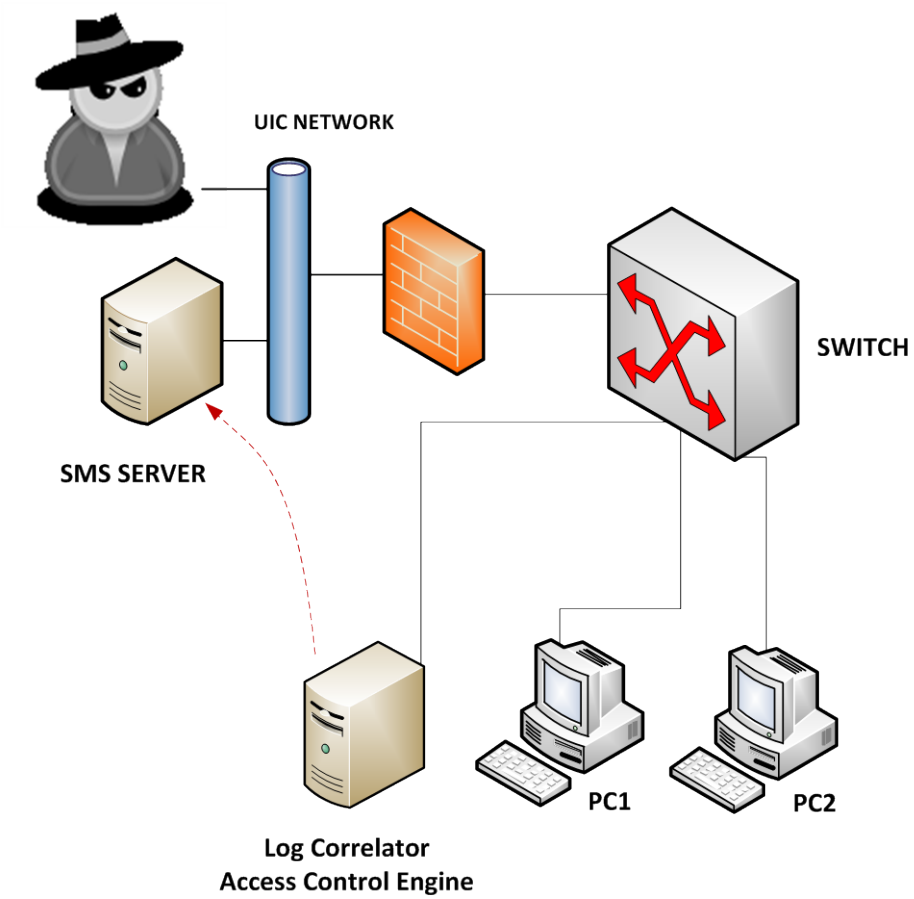


Demo tools: Log Correlator

Log Correlator collects logs incoming from security devices and performs run time correlation to detect:

- Unauthorised traffic;
- Cyber attacks.

ICT Demo Architecture

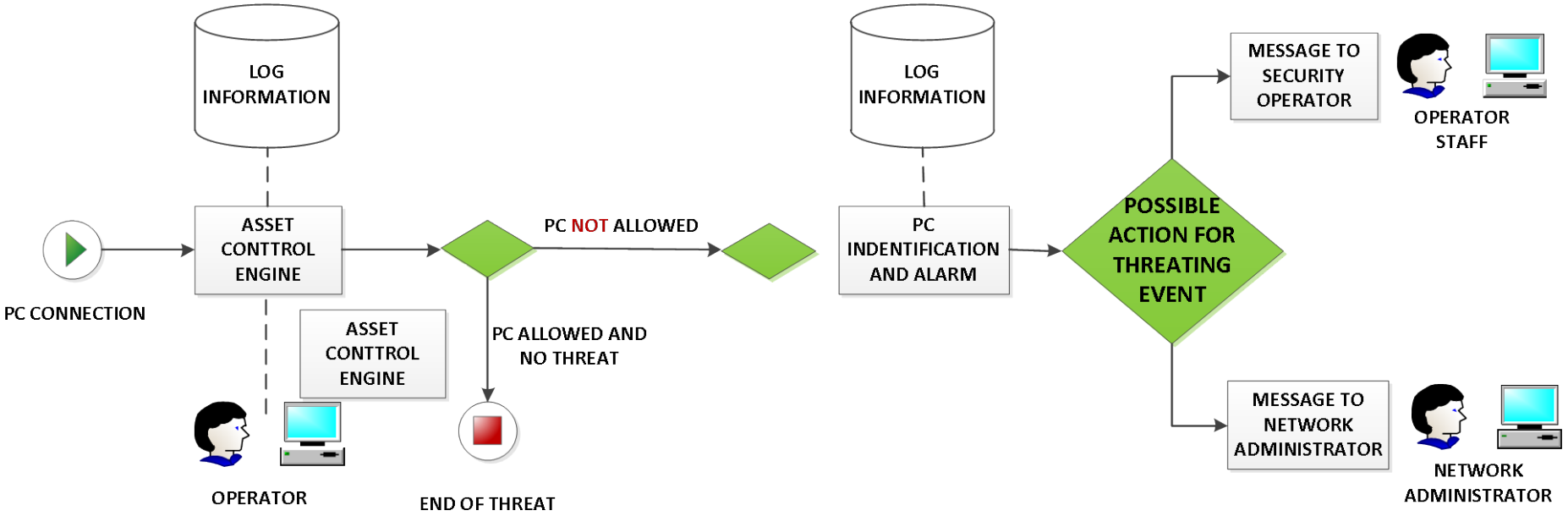


Demo Scenario 1

Scenario 1: Asset Control - Unauthorised PC connection

✓Connection of an external host to ICT network.

✓Asset Control Engine monitors ICT network configuration and detects any potential unauthorised intrusion.



Description

✓ ACE performs SNMP requests to switches and looks for differences between the real network and nominal asset in data-base

✓ ACE rises an Unknown Host Alarm if it is detected:

- an IP address that is not included in the nominal asset.
- a pair MAC and IP addresses not corresponding to the pair present in the nominal asset

Demo Scenario 2

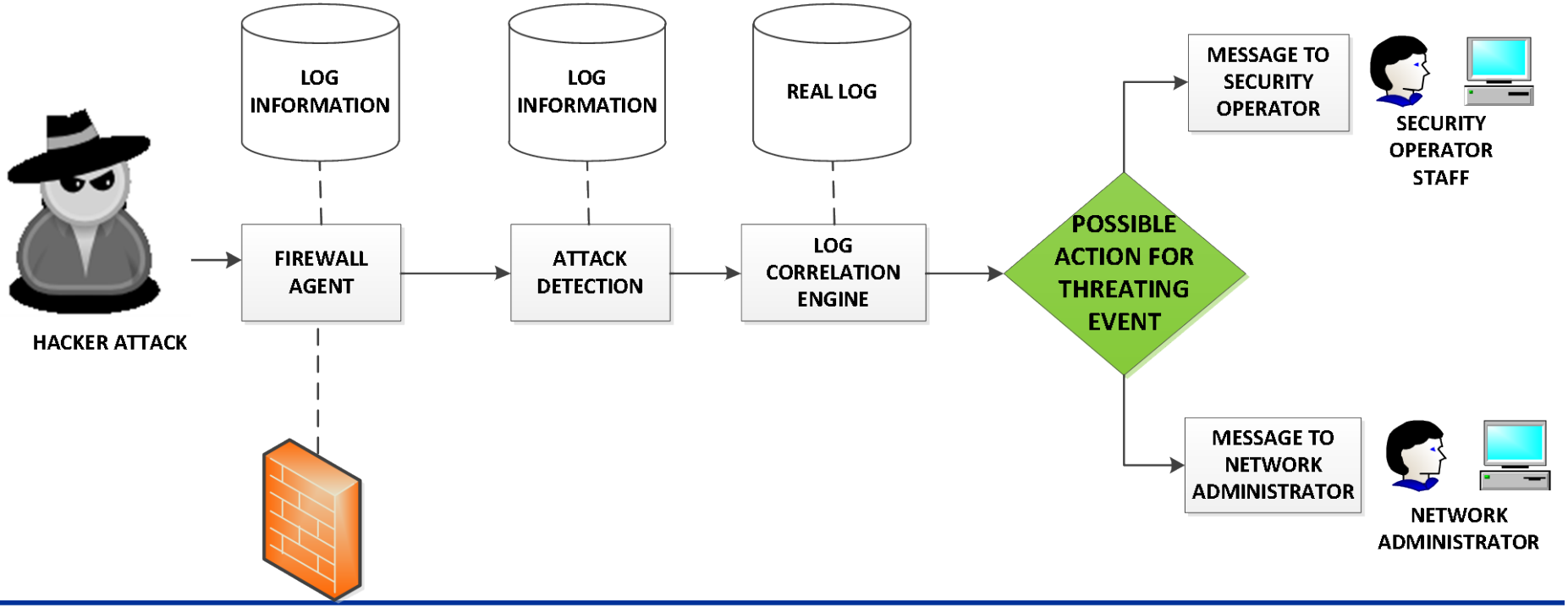
Scenario 2: Asset Integrity - Cyber Attack

✓ Hacker attacks for obtaining confidential information and/or compromise the availability of the ICT structure.

Description

✓ As the malicious connection (e.g. conficker exploitation) has been detected by the Firewall Agent, Log Correlation Engine performs a real time analysis of the recorded logs and detects the incoming anomaly.

✓ Armitage Metasploit tool will be used in order to simulate the attack scenario.



Thank you for your attention