The Register®

Manage security in real time

SIEMs like a good idea

intel® Security

Why are we here?

Security today requires real-time reporting and action.

Is SIEM up to the job

How do we fix it if it isn’t?

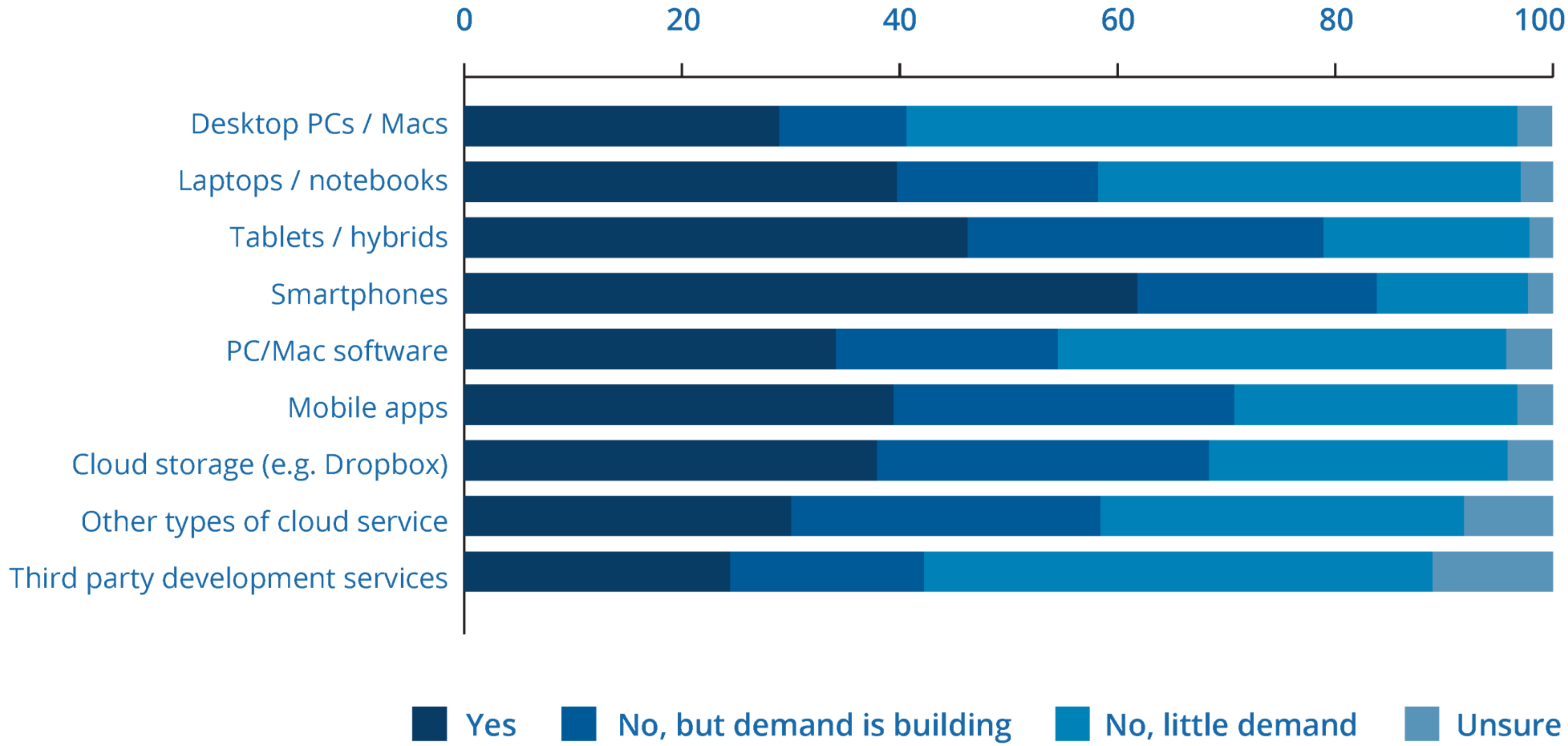
On our Regcast today

Raj Samani, **McAfee - Part of Intel Security**

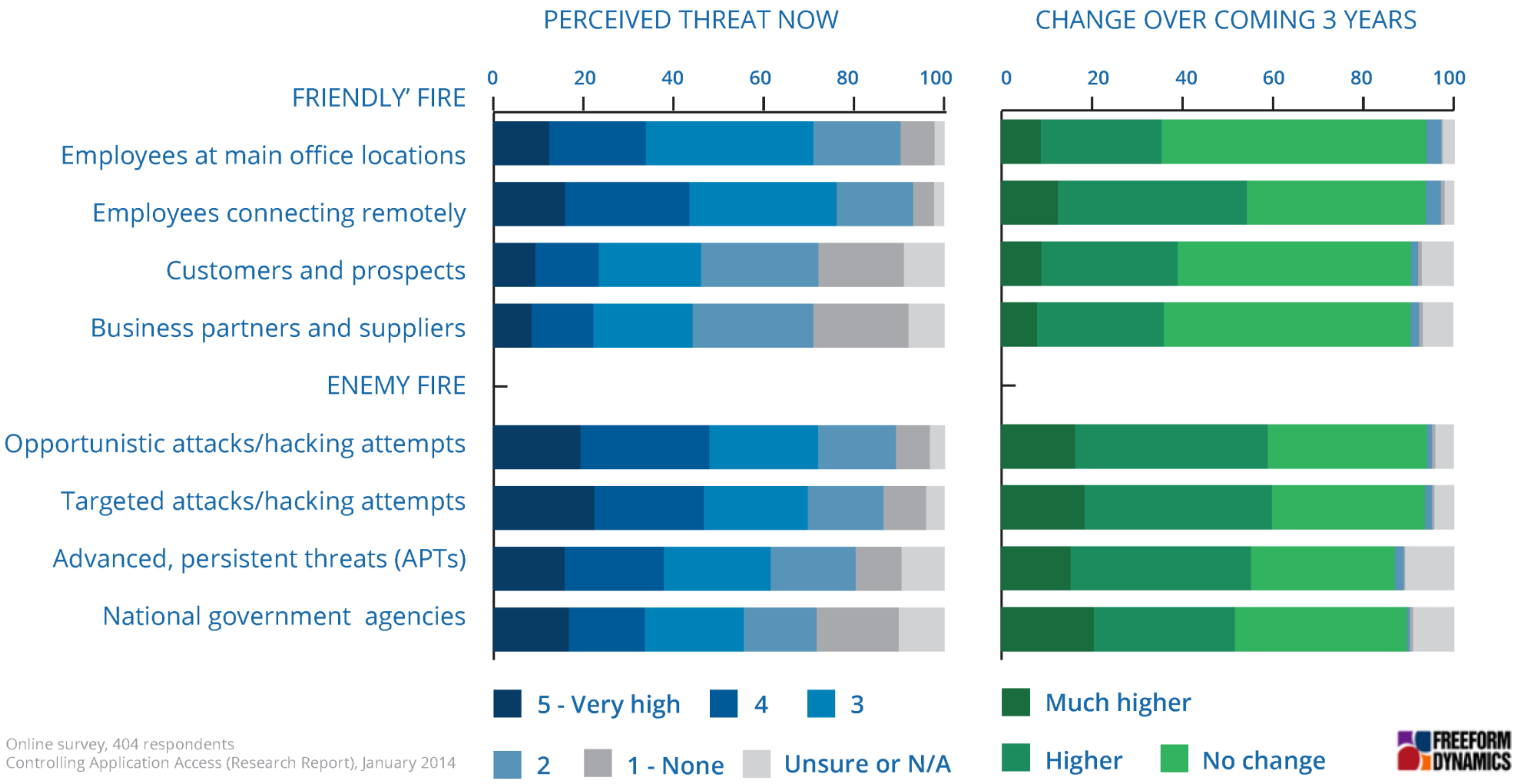
Tony “White hat” Lock, **Freeform Dynamics**

Tim Phillips, **The Register**

Do you see a significant amount of user or business driven adoption of the following independently of the IT department?

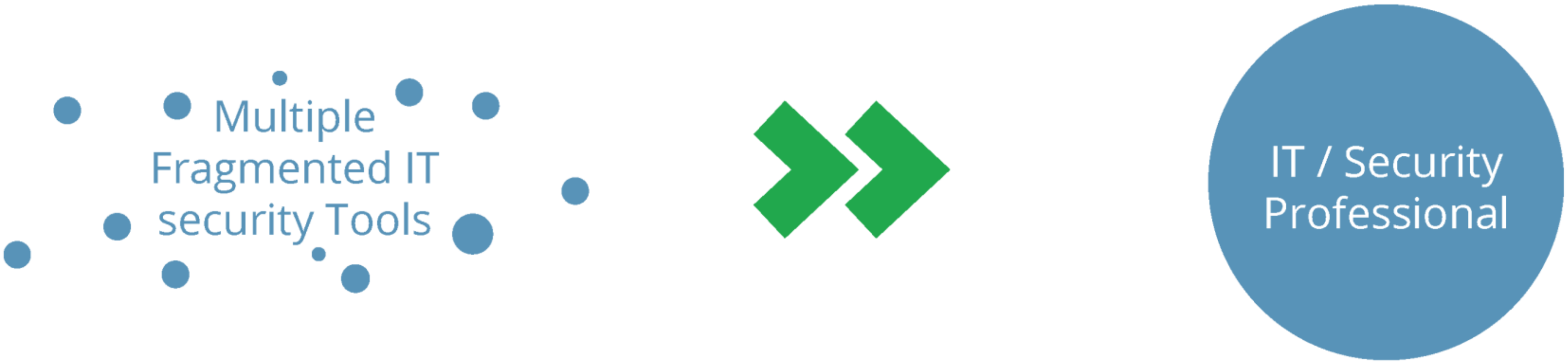


How much of a perceived security threat is associated with the following (now and in three years)?



Online survey, 404 respondents
Controlling Application Access (Research Report), January 2014

Security management

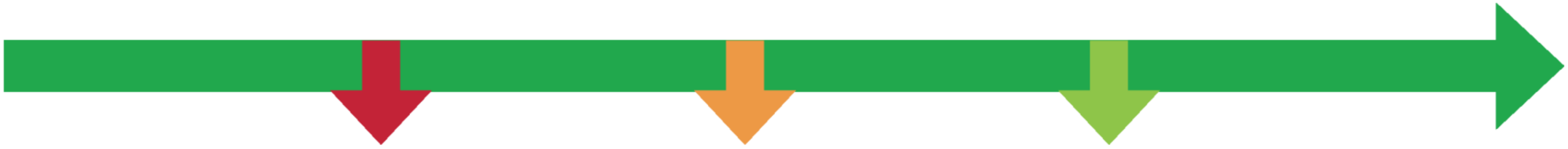


Multiple Fragmented IT security Tools

IT / Security Professional

- Little Integration
- Too much data
- Or too little
- Scant Automation

- Firefighting
- Guesswork
- Slow to respond

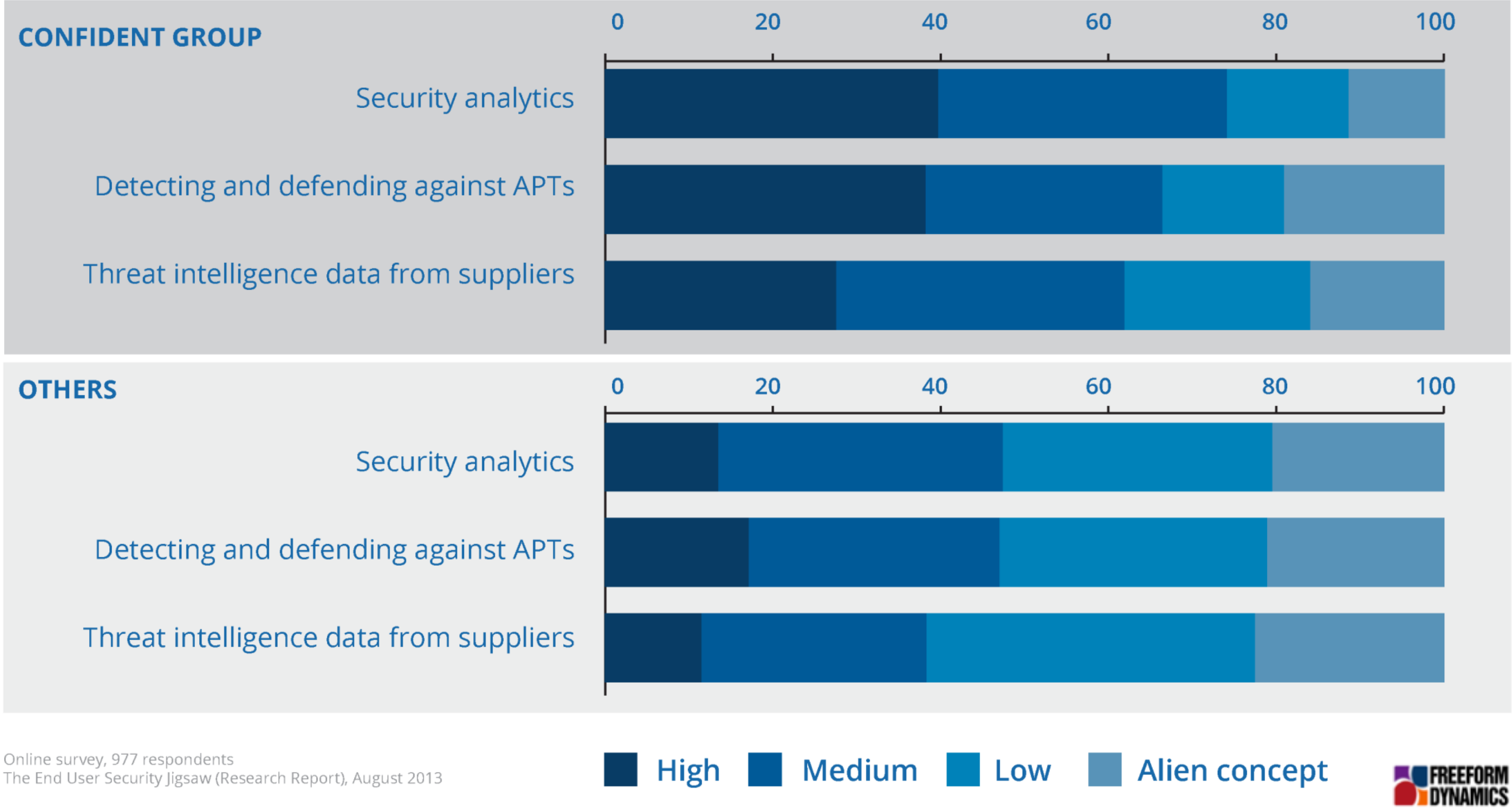


Find data

Understand what's happening

Work out what to do

How much emphasis is there on the following in your organisation?



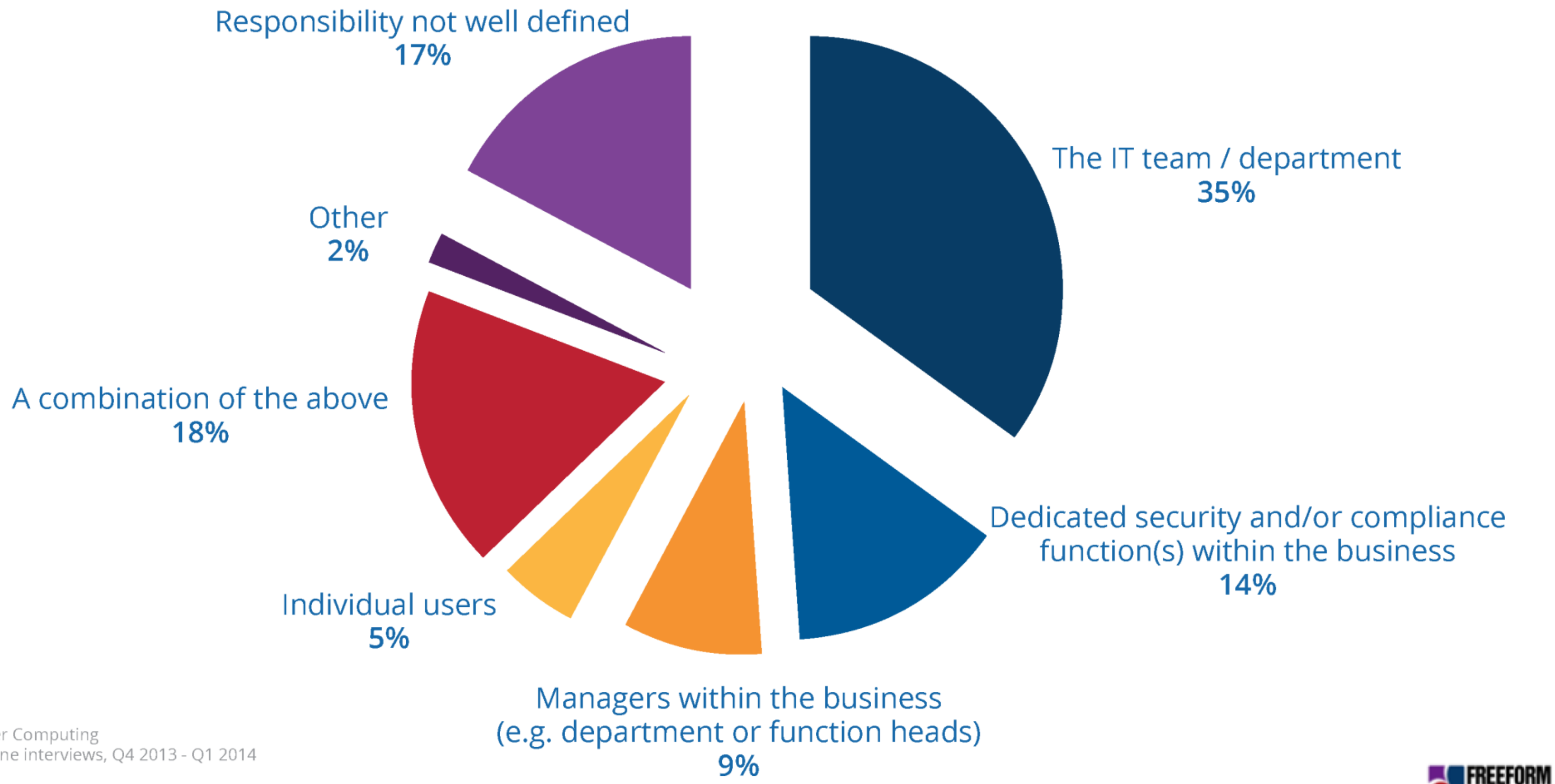
Online survey, 977 respondents
The End User Security Jigsaw (Research Report), August 2013

FREEFORM DYNAMICS

The Register®

intel® Security

Where does responsibility fall for security, compliance and data protection?



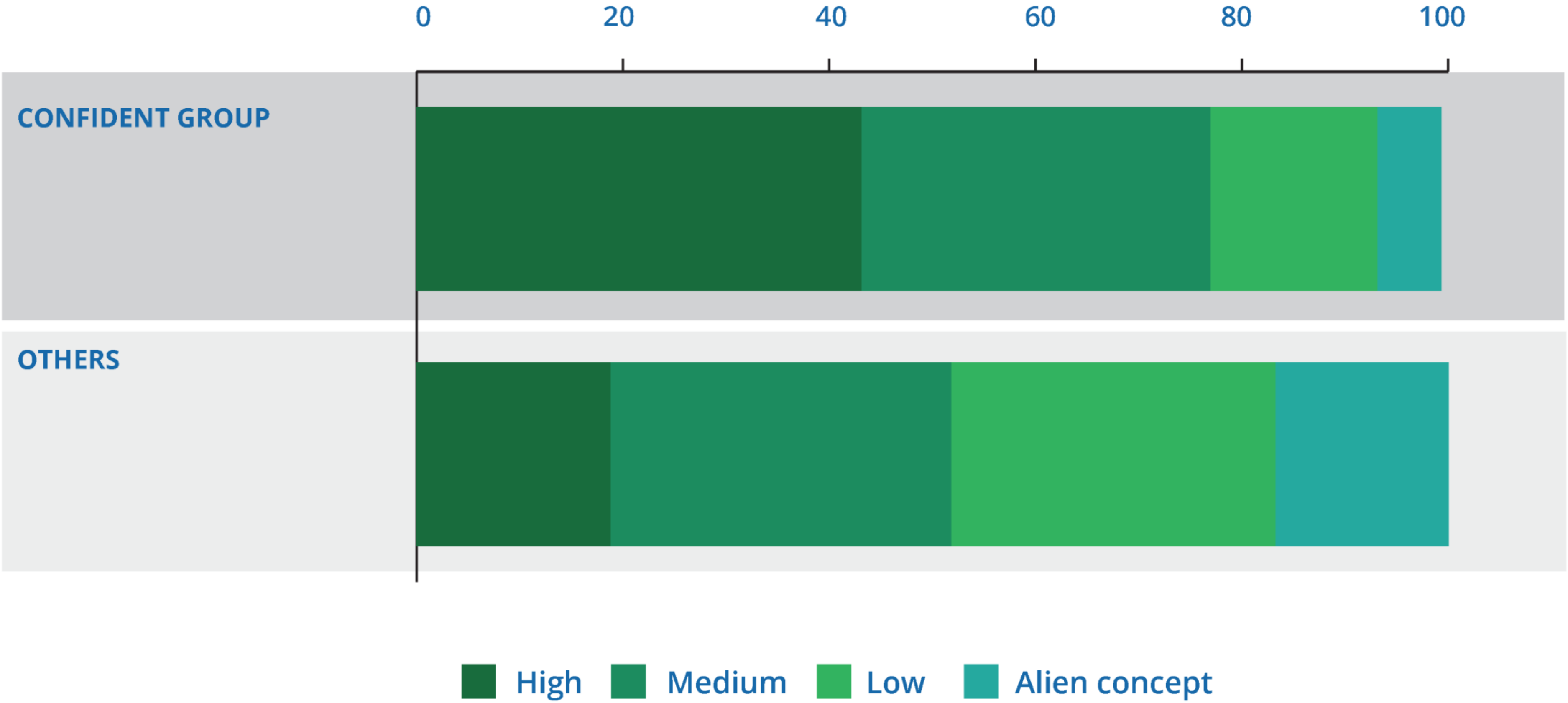
End User Computing
660 online interviews, Q4 2013 - Q1 2014

FREEFORM DYNAMICS

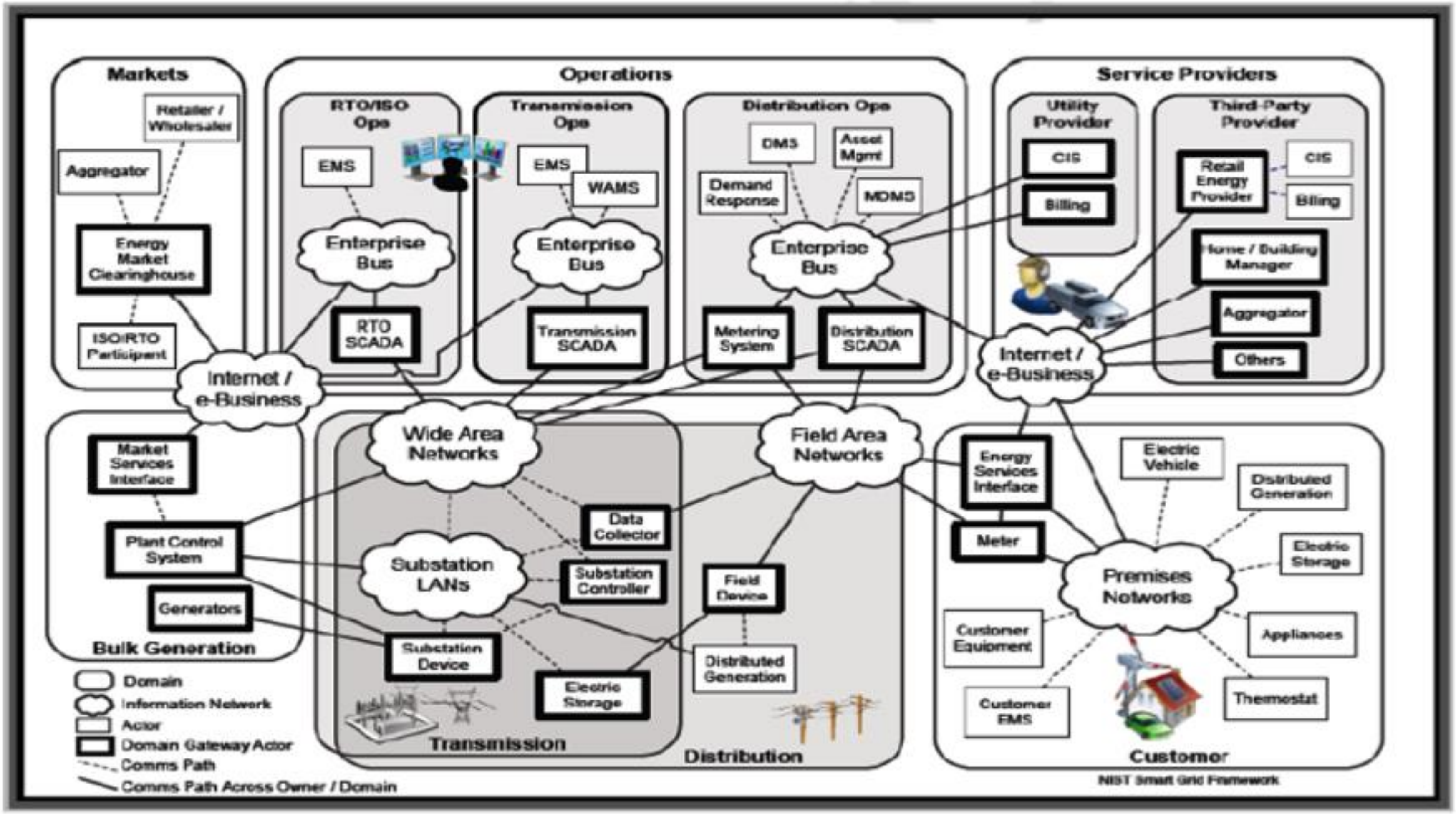
The Register®

intel Security

What's the level of awareness of security issues among your execs?



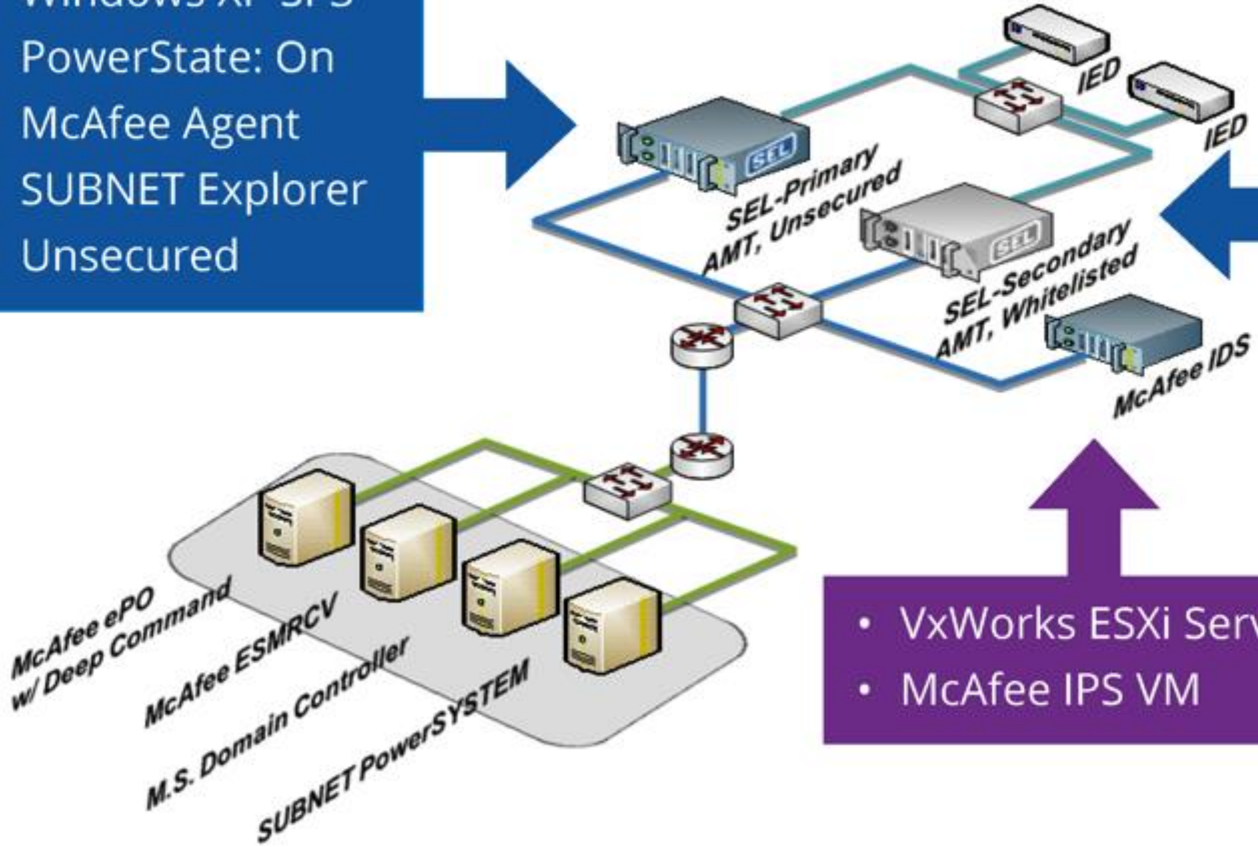
Historical information becomes interactive



NIST Smart Grid Framework

Cyber Security Solution
For critical Infrastructure PoC

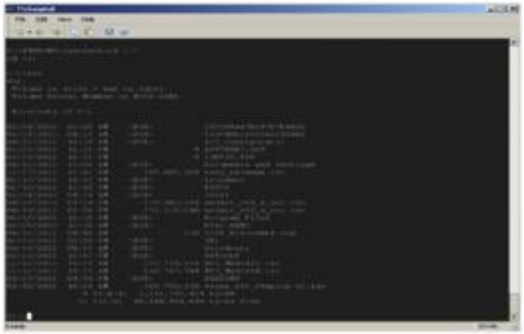
- Windows XP SP3
- PowerState: On
- McAfee Agent
- SUBNET Explorer
- Unsecured

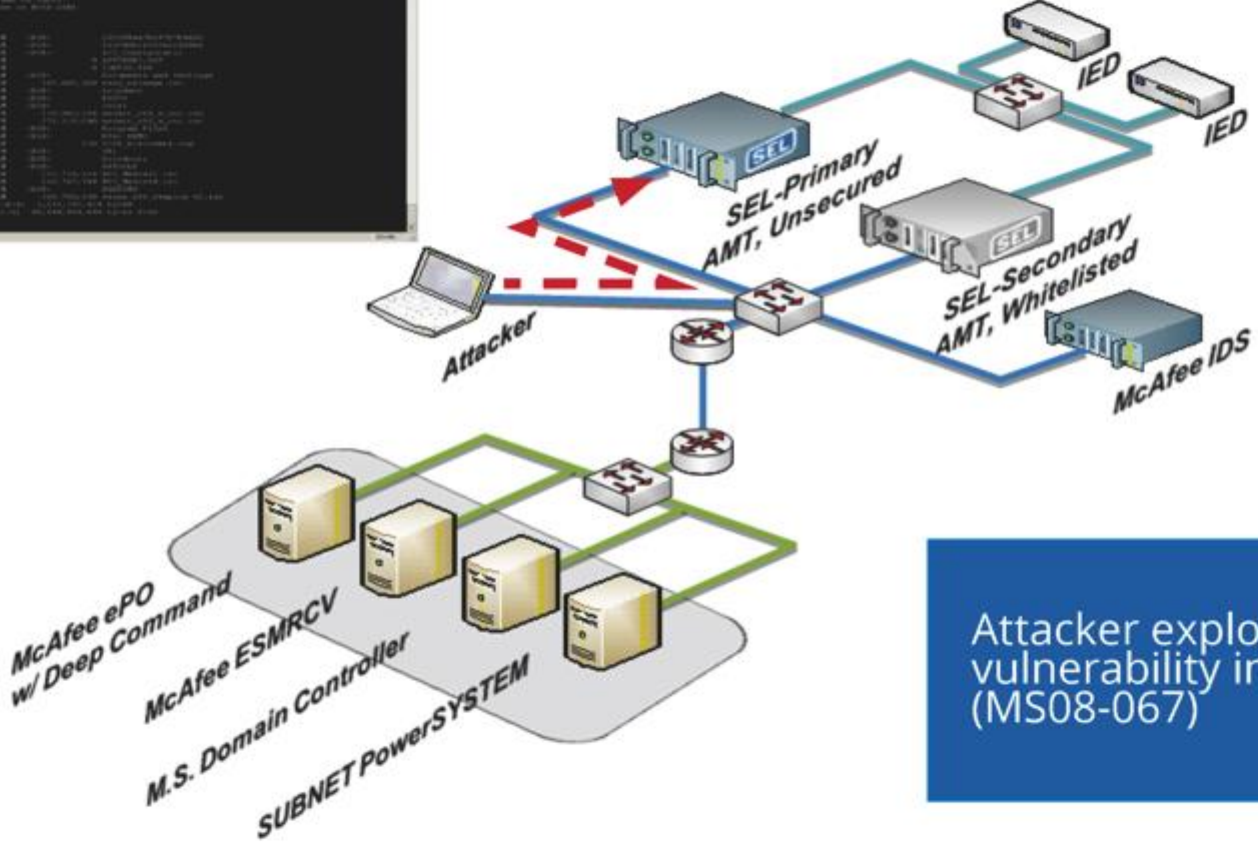


- Windows XP SP3
- PowerState: Off
- McAfee Agent
- SUBNET Explorer
- McAfee Embedded Control

- VxWorks ESXi Server
- McAfee IPS VM

Attack on vulnerable substation controller

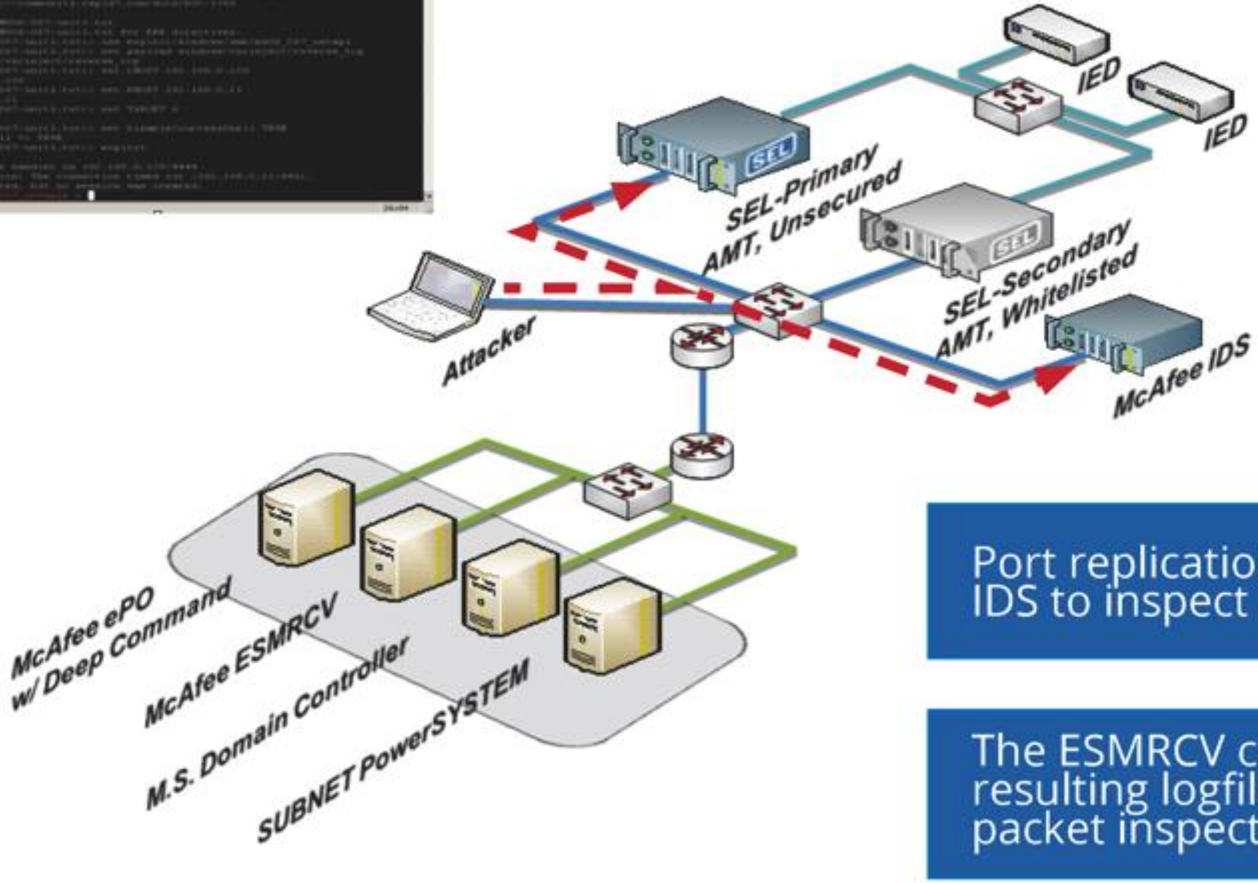




Attacker exploits a well-known vulnerability in WinXP SP3 (MS08-067)

IDS snoops network traffic

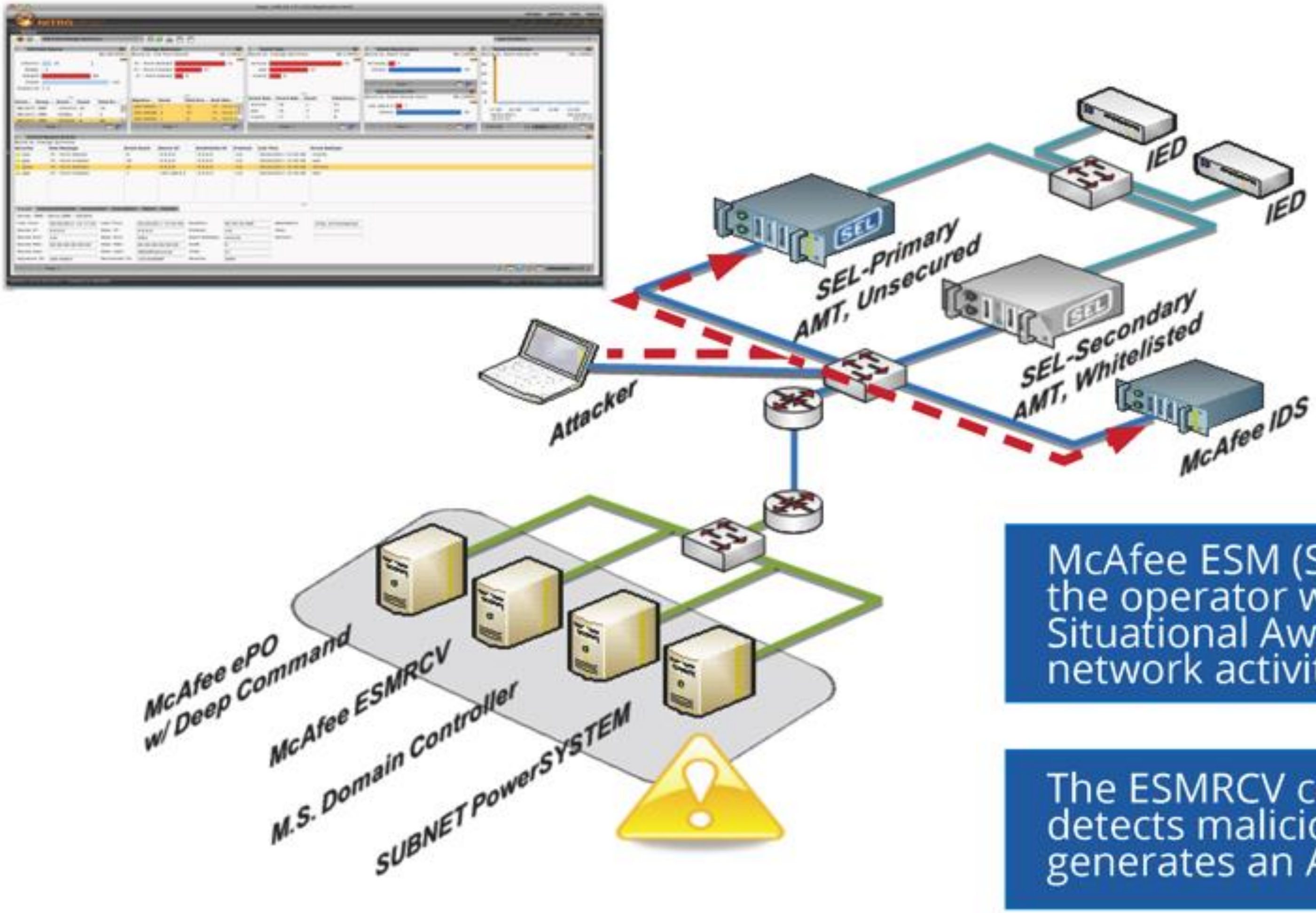
```
[illegible]
```



Port replication allows McAfee IDS to inspect all network traffic

The ESMRCV collects the resulting logfiles from the deep packet inspection process

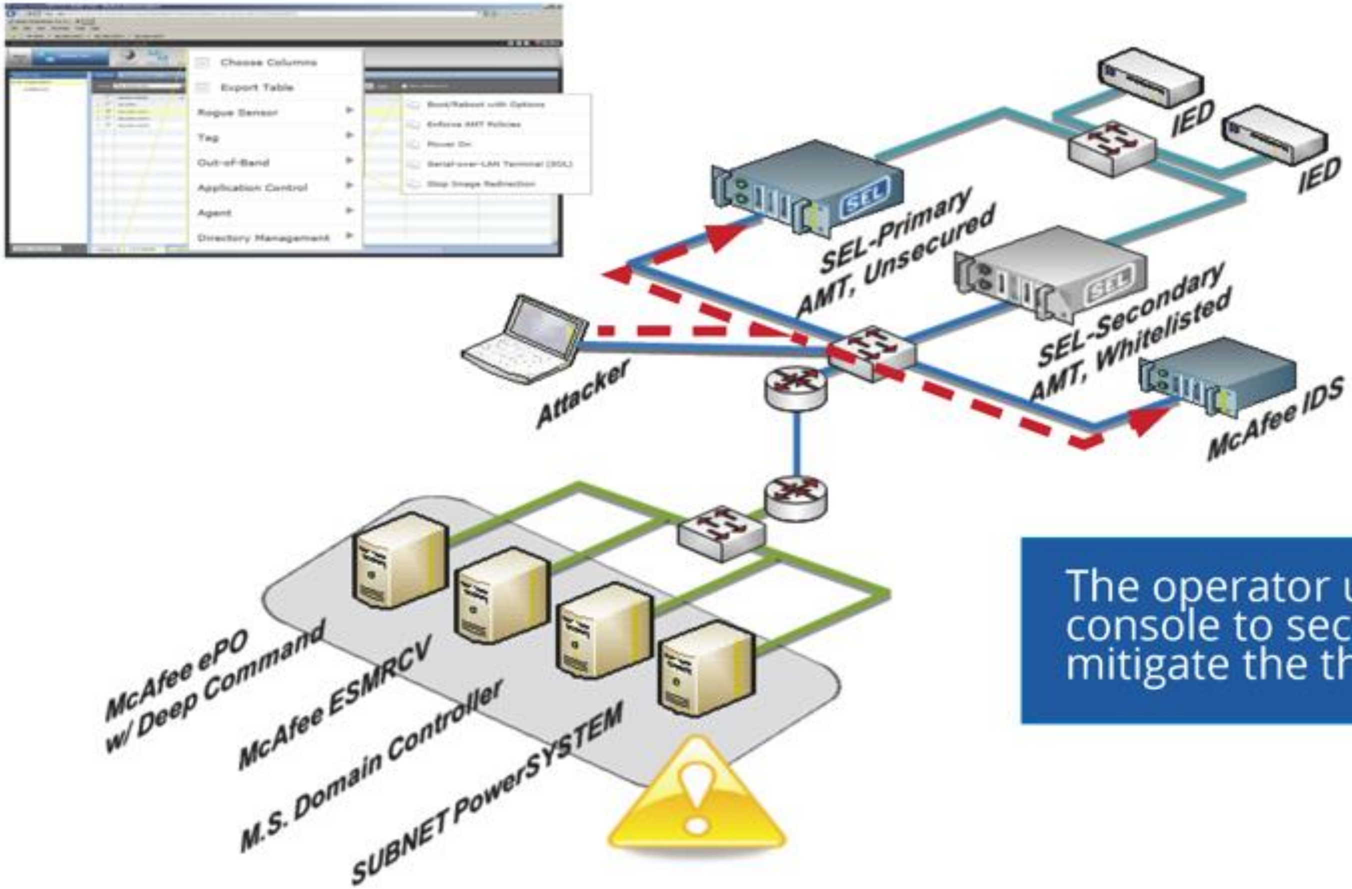
Complete situational awareness of your network



McAfee ESM (SIEM) provides the operator with complete Situational Awareness of network activity

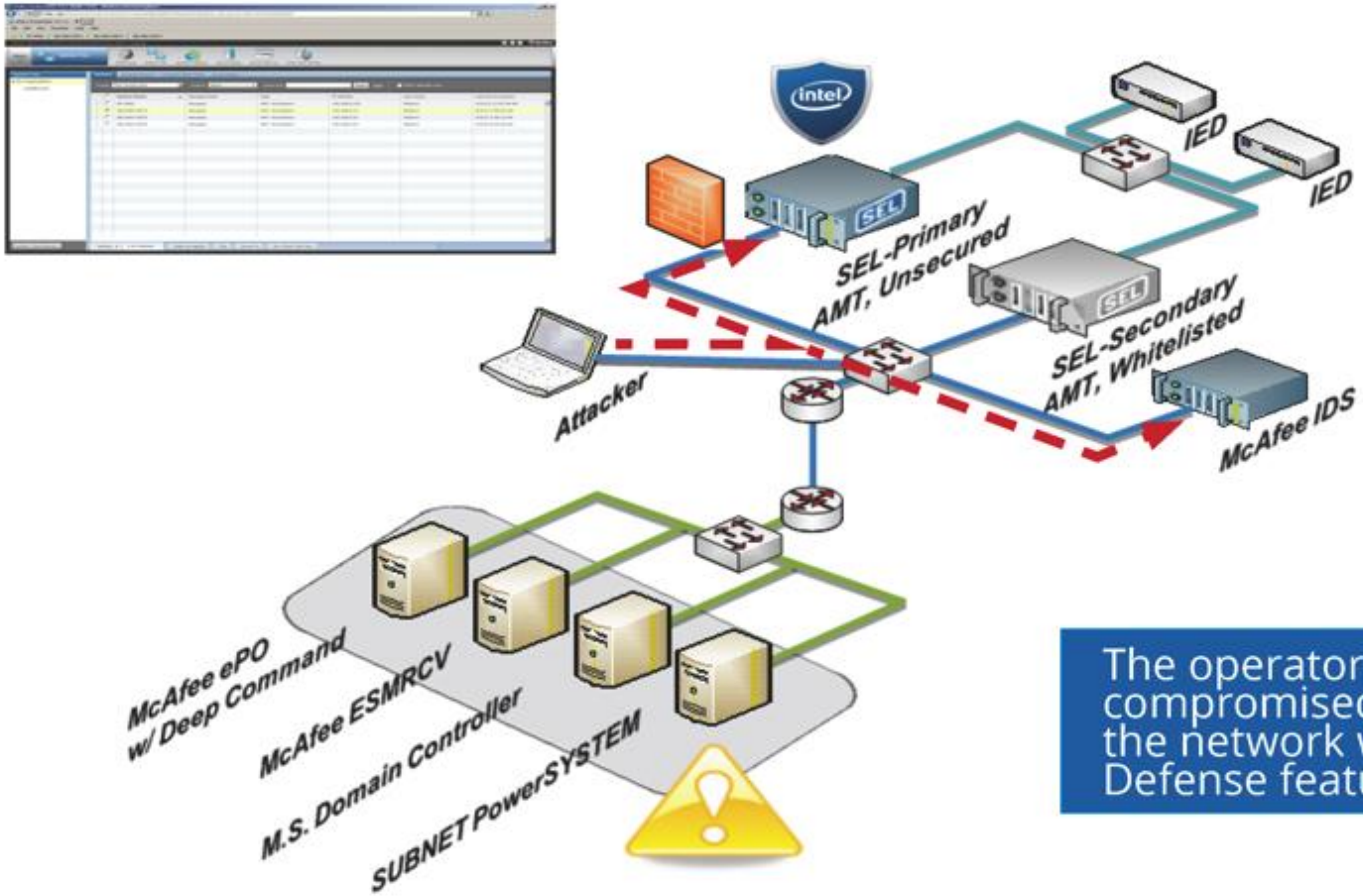
The ESMRCV correlates the data, detects malicious activity & generates an Alarm

Manage all systems with McAfee's ePO Console



The operator uses McAfee's ePO console to securely & remotely mitigate the threat

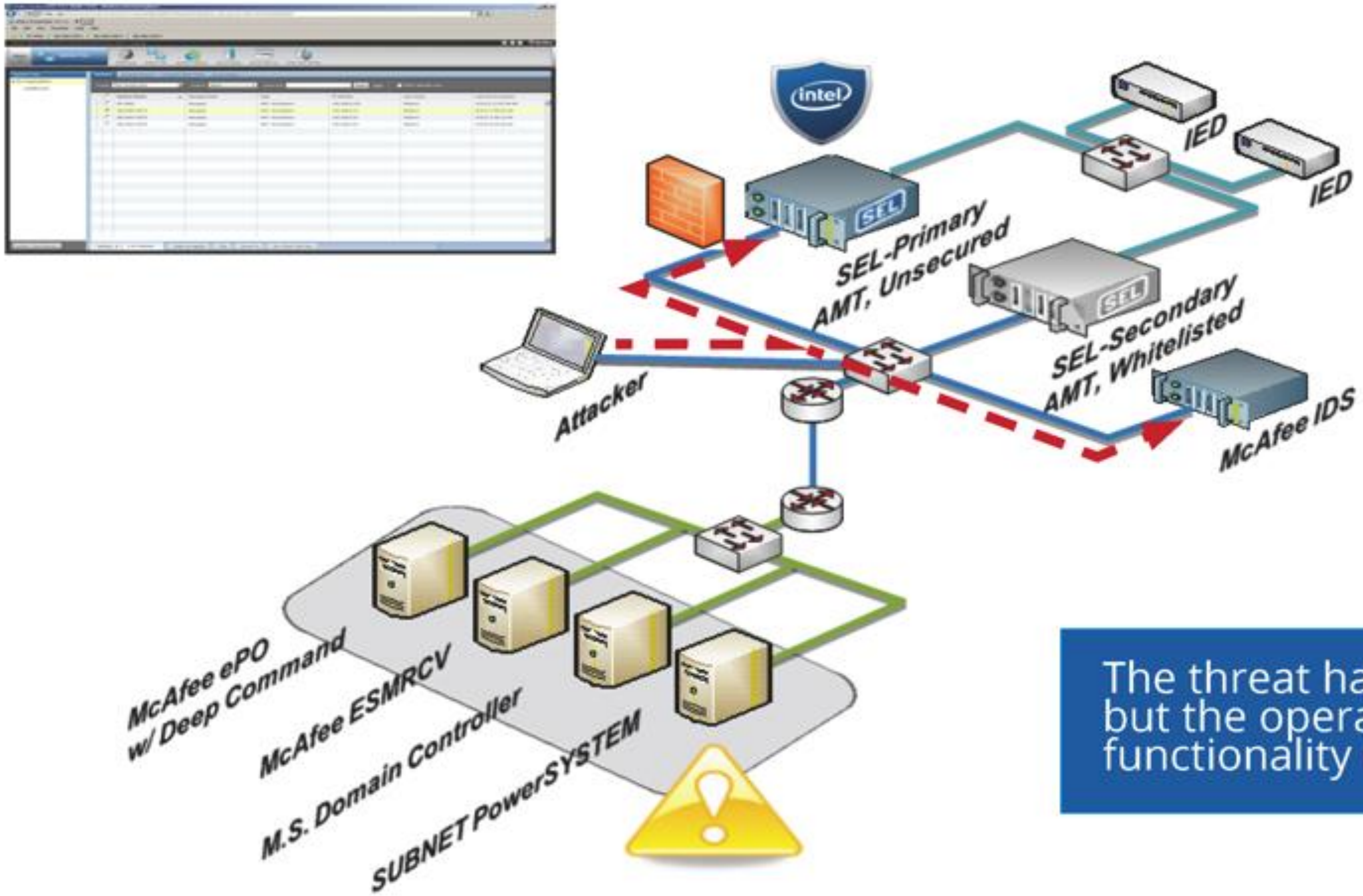
Isolate compromised machine with AMT's System Defense function


IED
IED
SEL-Primary AMT, Unsecured
SEL-Secondary AMT, Whitelisted
McAfee IDS
Attacker
McAfee ePO w/ Deep Command
McAfee ESMRCV
M.S. Domain Controller
SUBNET PowerSYSTEM

The operator creates hardware filters to firewall all non-AMT network traffic

The operator "quarantines" the compromised system from the network with AMT's System Defense feature

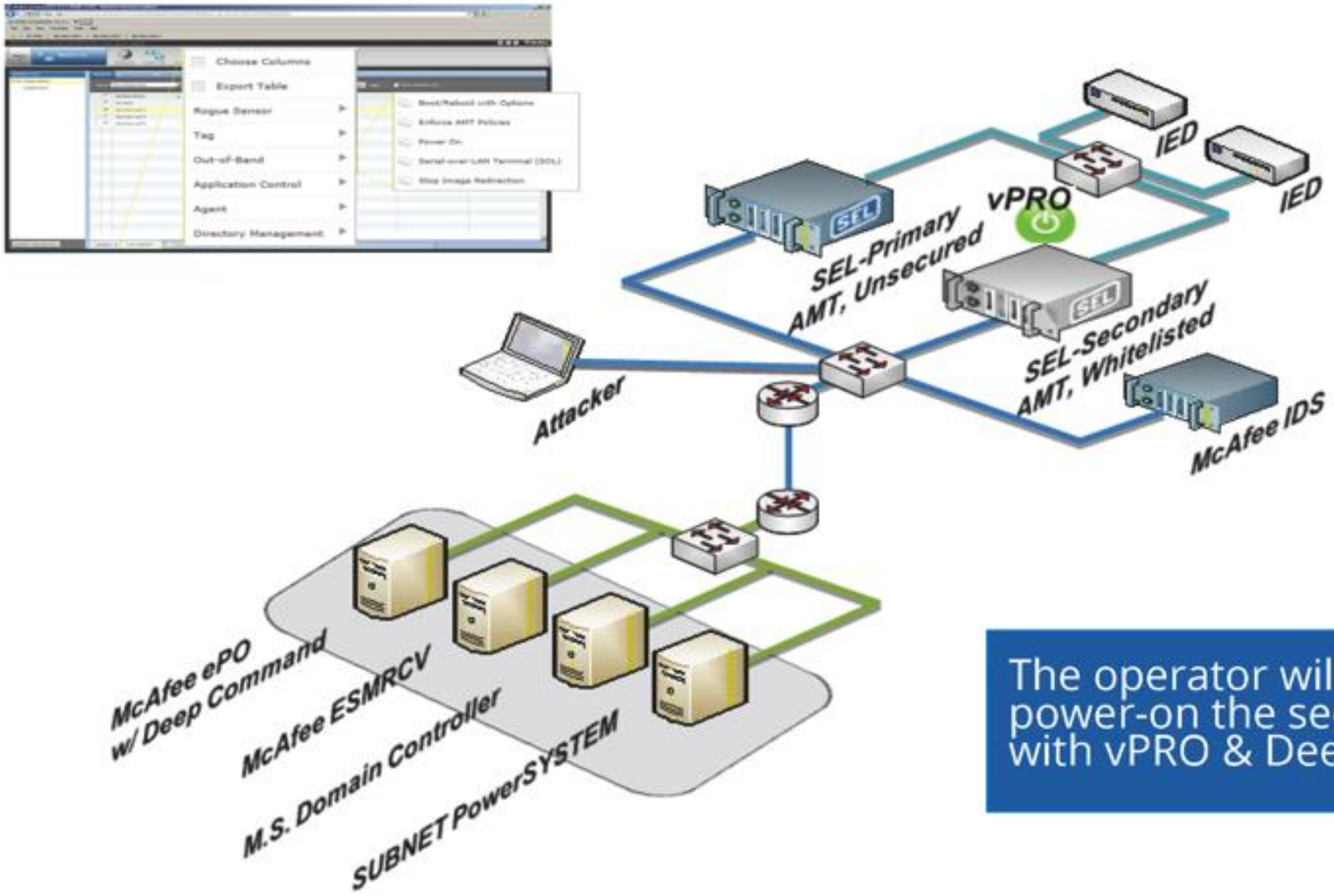
Out-of-Band Management with Deep Command



The compromised machine is quarantined from the network until remediation is complete

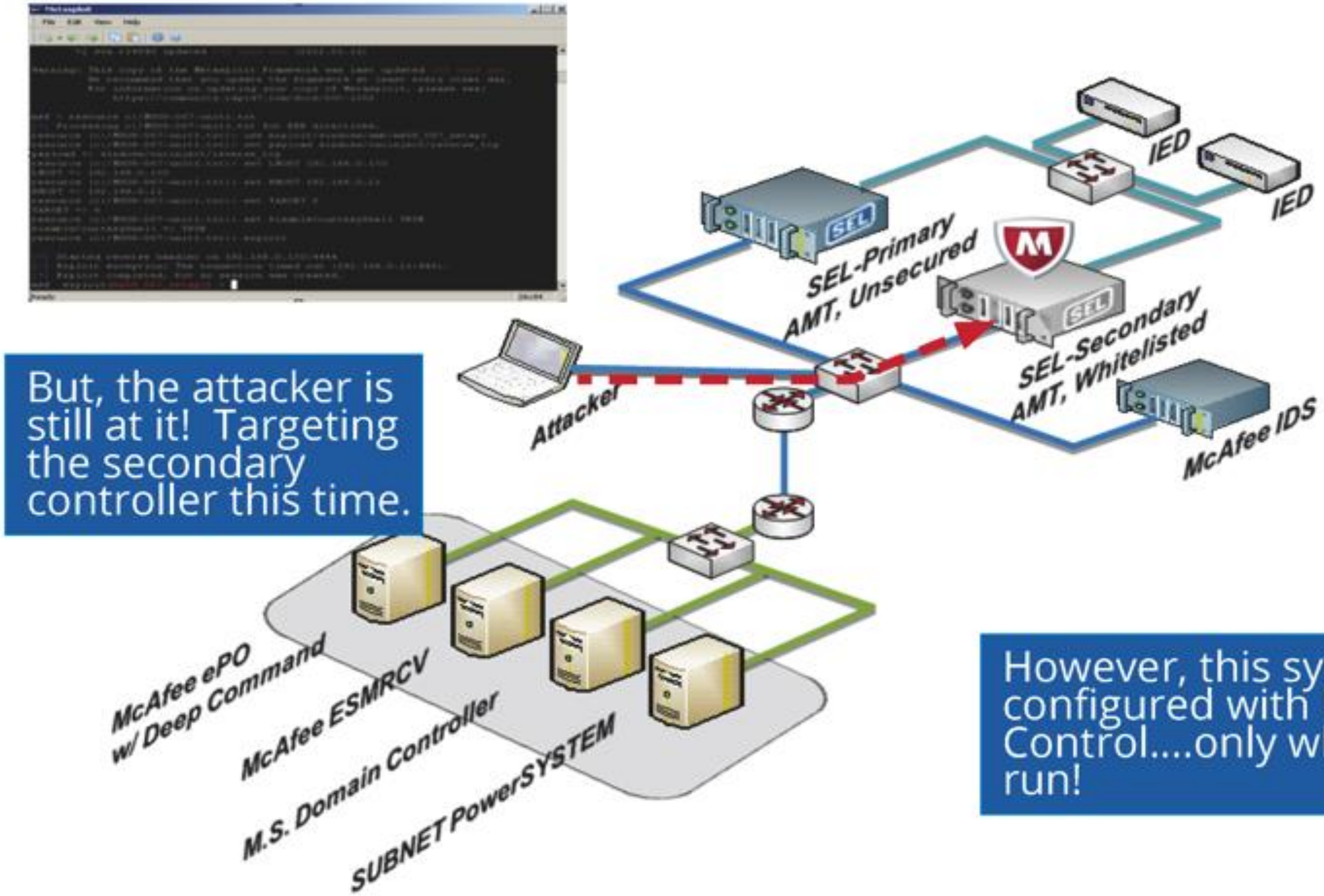
The threat has been eliminated, but the operator must restore functionality of the system

Out-of-Band Management with Deep Command



The operator will remotely & securely power-on the secondary controller with vPRO & Deep Command

Endpoint security with McAfee's embedded control



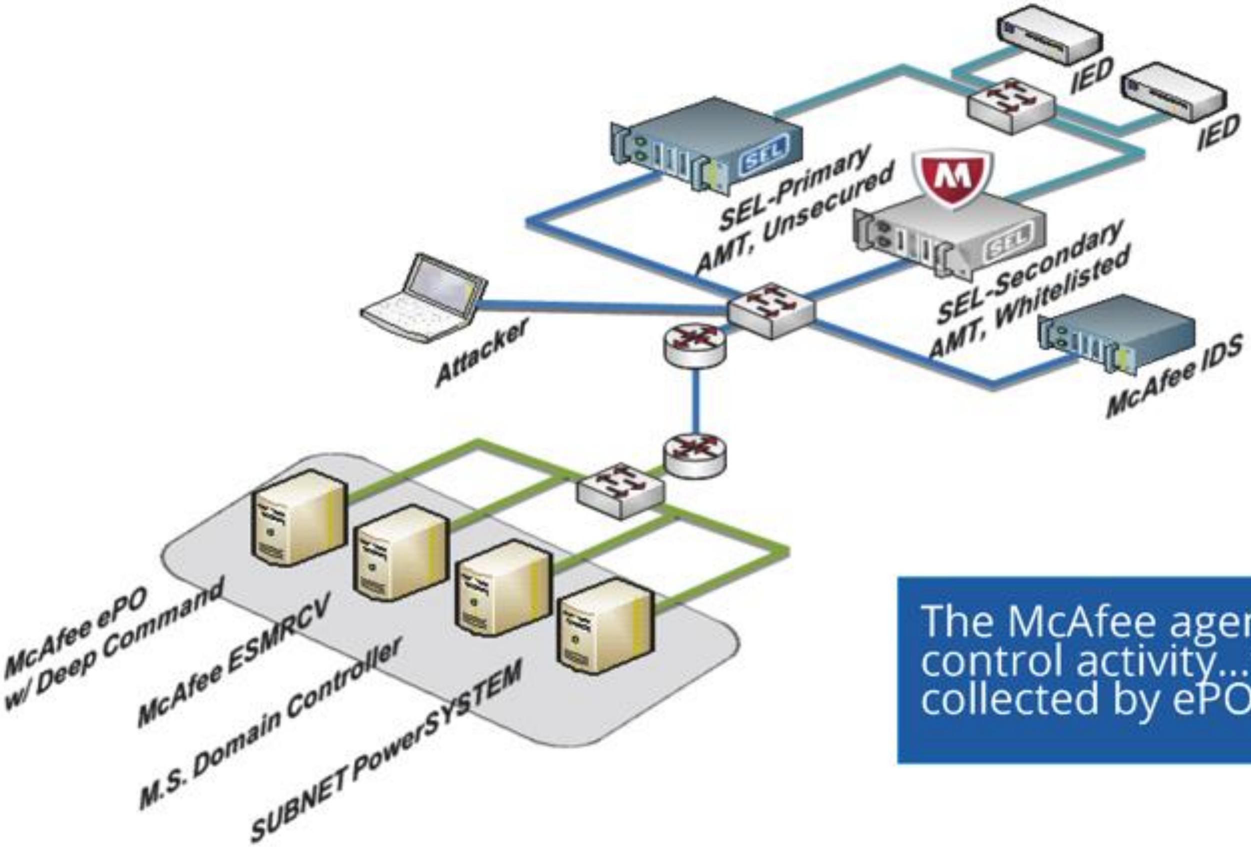
[illegible]

But, the attacker is still at it! Targeting the secondary controller this time.

The secondary controller is online and normal operation has resumed

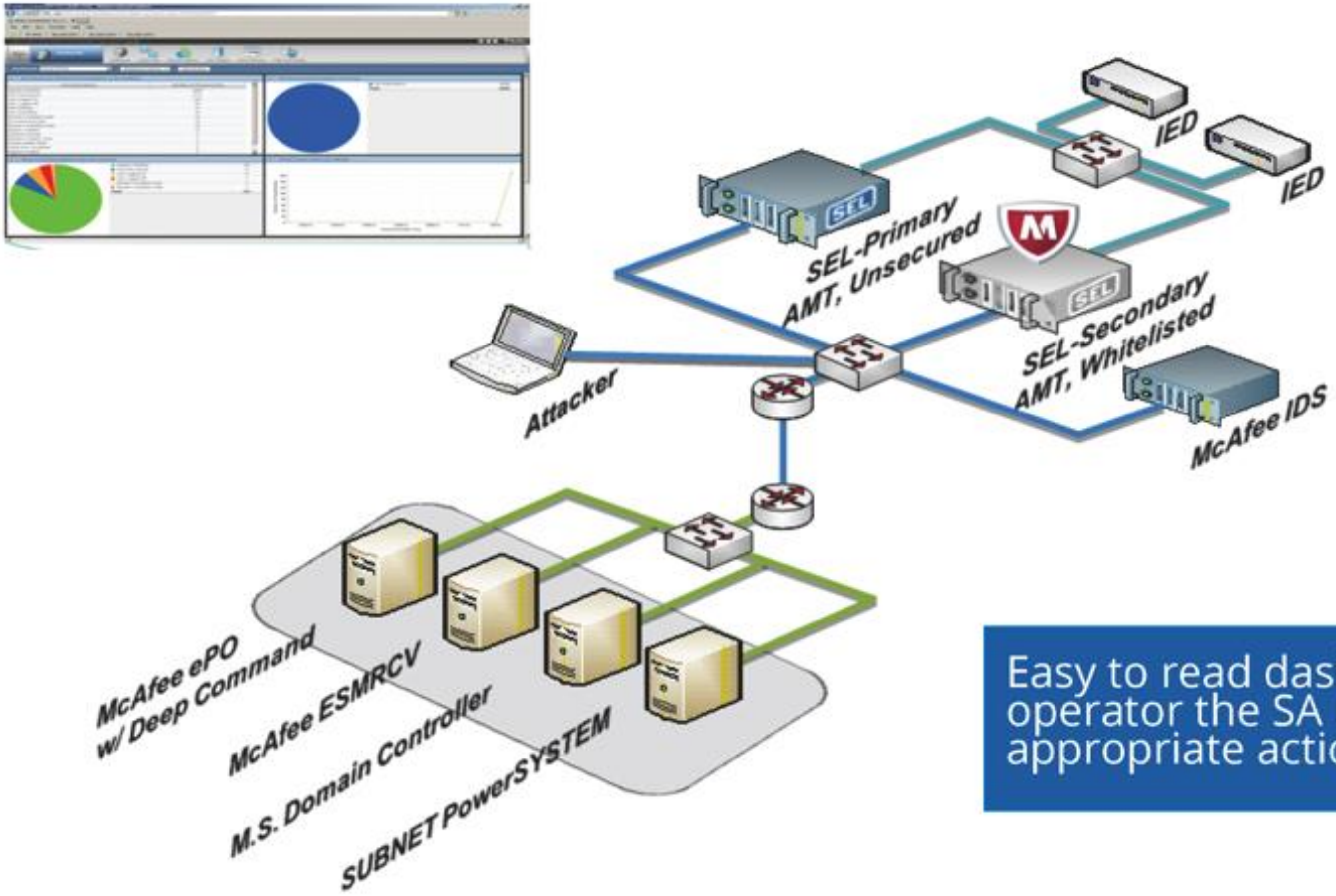
However, this system is properly configured with McAfee's Embedded Control....only whitelisted code can run!

No event goes undetected

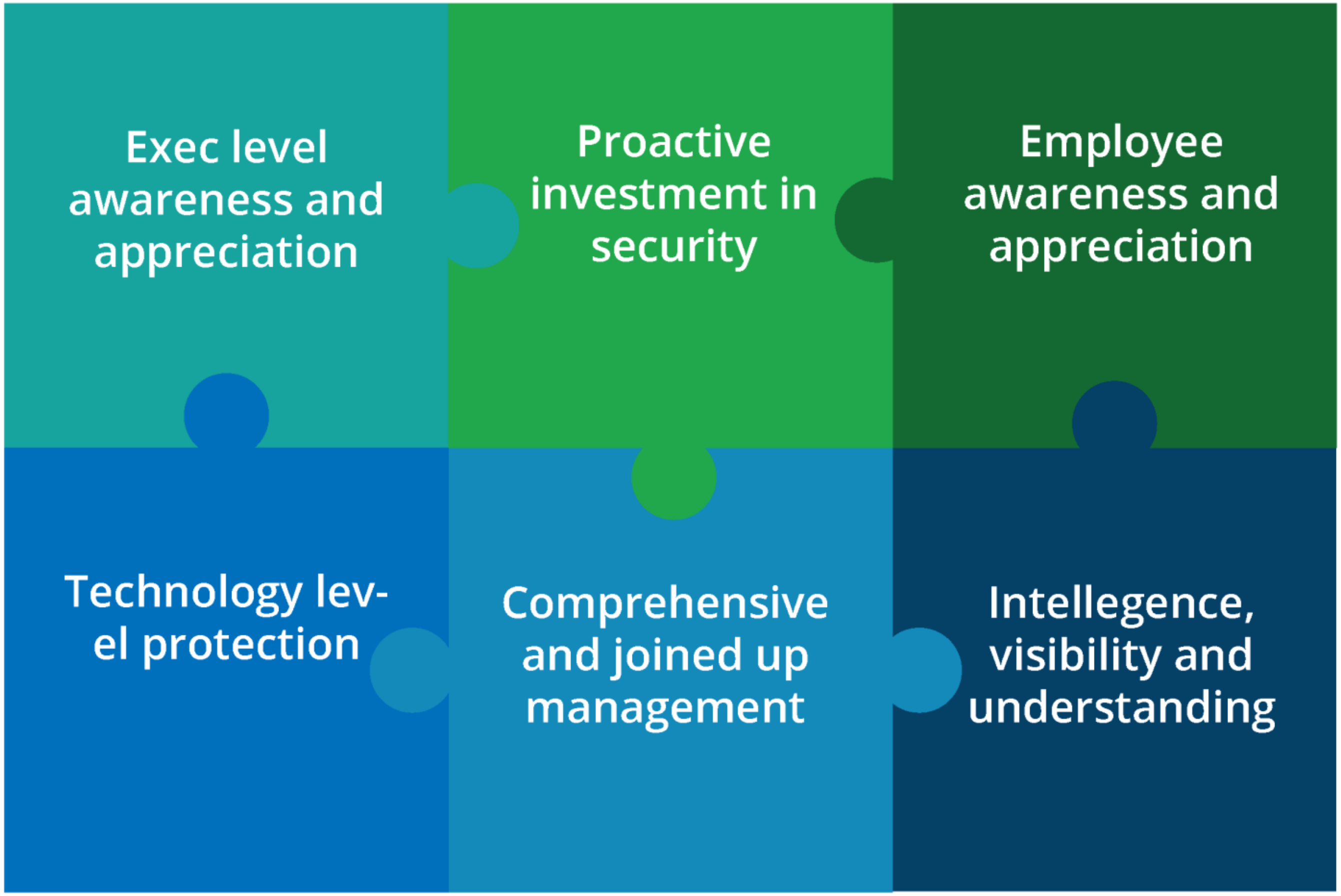


The McAfee agent logs all embedded control activity…these logs are collected by ePO and the ESMRCV

ePO dashboards enable rapid SA



Easy to read dashboards give the operator the SA required to take the appropriate action



Exec level awareness and appreciation

Proactive investment in security

Employee awareness and appreciation

Technology level protection

Comprehensive and joined up management

Intellegence, visibility and understanding

Online survey, 977 respondents
The End User Security Jigsaw (Research Report), August 2013

Further reading

Security Management 2.0	http://reg.cx/2cpk
Focus on 5 SIEM requirements	http://reg.cx/2cpm

Thanks for joining us

An archived version of today's event will be made available on The Register in the near future.