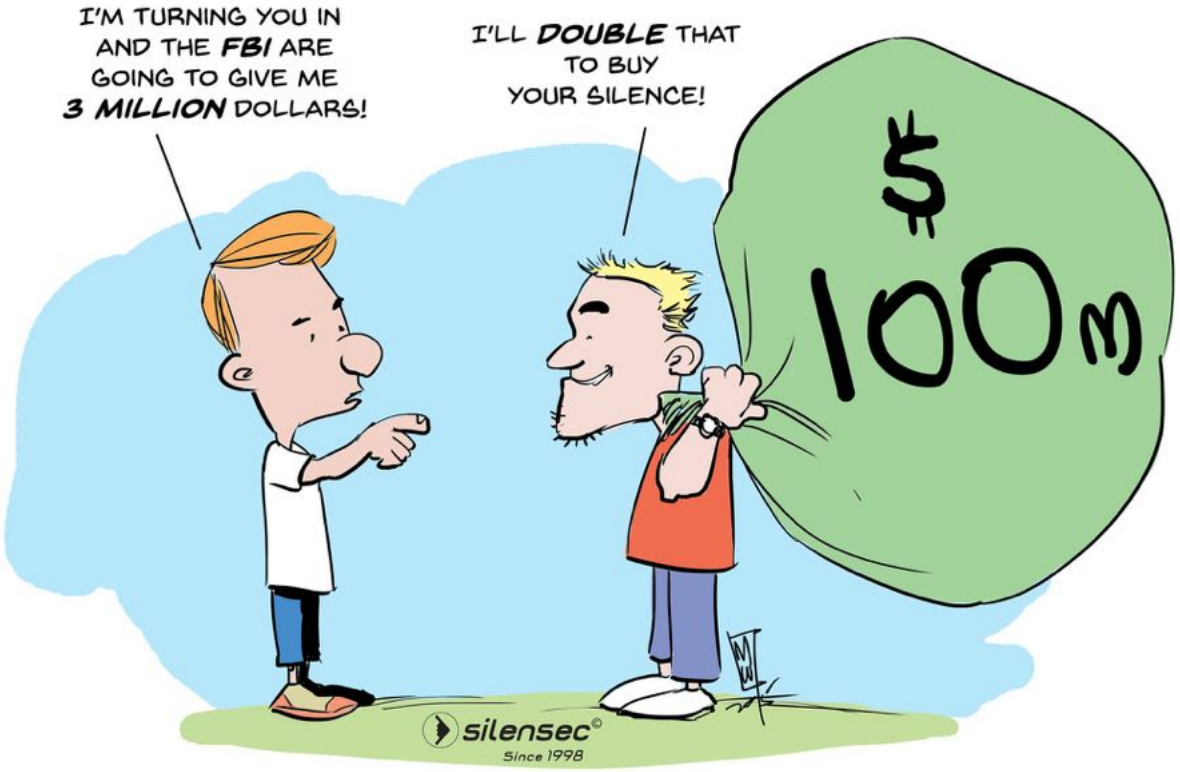
# Identifying, Investigating and Preventing Cyber Attacks to Financial Institutions

Almerindo Graziano, PhD
Silensec, CEO
al@silensec.com

silensec
Information Security Since 1998

# Crime Doesn't Pay…What about Cybercrime?




## FBI Issues $3 million Bounty for Russian Hacker

A $3 million reward for information on the FBI's most wanted cyber criminal was issued in Washington yesterday as his malware, GameOver ZeuS botnet, is alleged to have infected one million computers, and resulted in the theft of more than $100 million from businesses and consumers in the U.S. and worldwide

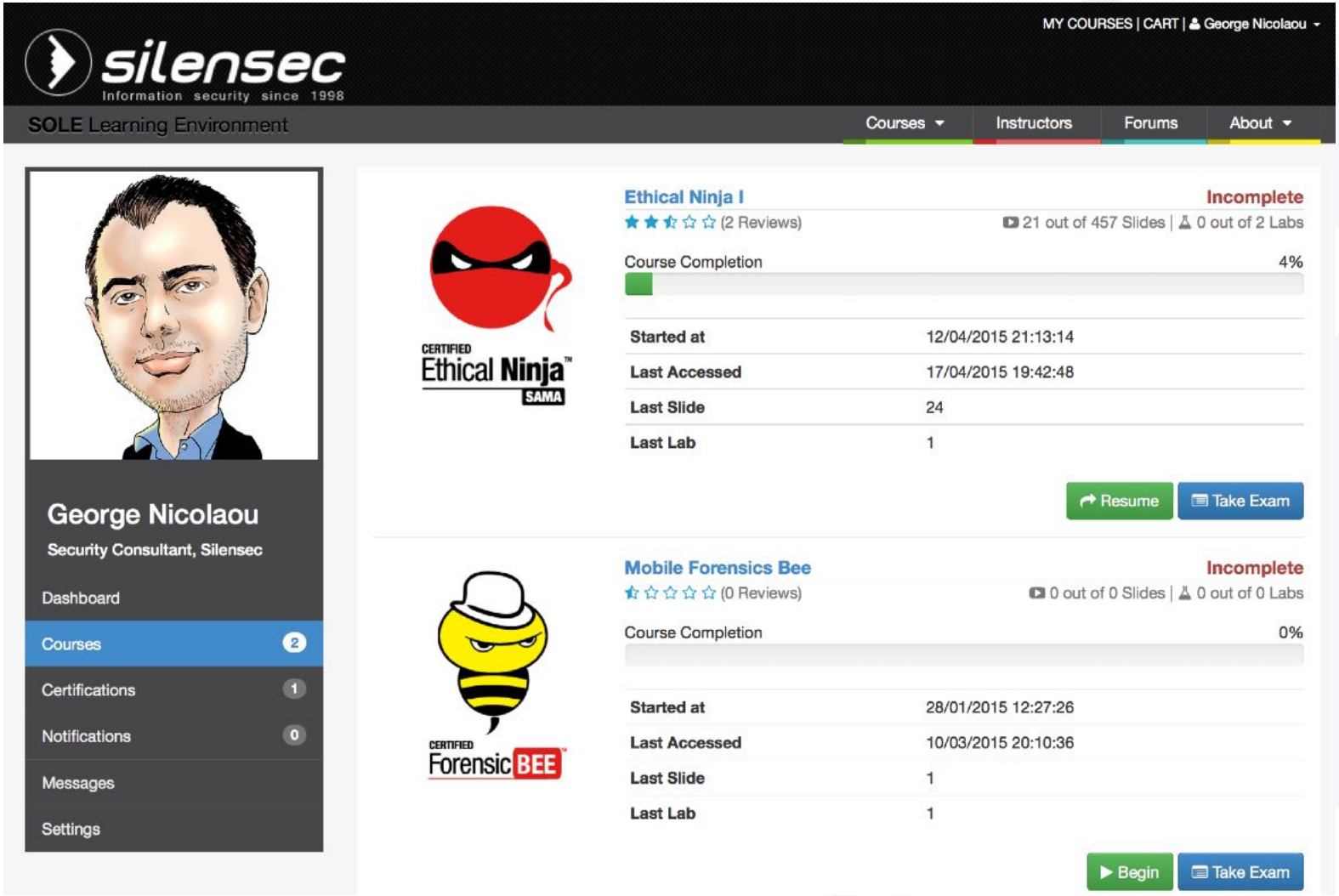
# About Silensec

- Information Security Management Consultancy Company (ISO27001 Certified)
  - IT Governance, Security Audits
  - Security System Integration (SIEM, LM, WAFs)
  - Managed Security Services
- Offices: England, Cyprus, Kenya,
- Independent Security Training Provider
  - ISO27001, Business Continuity, PCI DSS, CISSP, Ethical hacking, Computer Forensics, Mobile Forensics, Reverse Engineering, Intrusion Detection, Log Management


- Incident Response and Computer Forensics Services
- Research and Development
  - Nwuki Mobile Forensics Suite

# Silensec Online Learning Environment (SOLE)





# Competence Based Certifications



- Knowledge Assessment
  - Multiple choice
  - Multiple answer
  - True or false
  - Match nmap flag with the scan type
  - Drag and drop
- Competence Assessment through Virtual Labs
  - Perform task based on the certification track
    - Hacking
    - Investigating incidents
    - Performing computer forensics
    - Reverse engineering malware
    - Configuring and troubleshooting SIEM/Log Management Systems etc

# Introduction



- Africa Cyber Security Landscape
- Incident Investigation through Network Security Monitoring
- The Value of Log Management in Incident Response
- Log Management Maturity Model

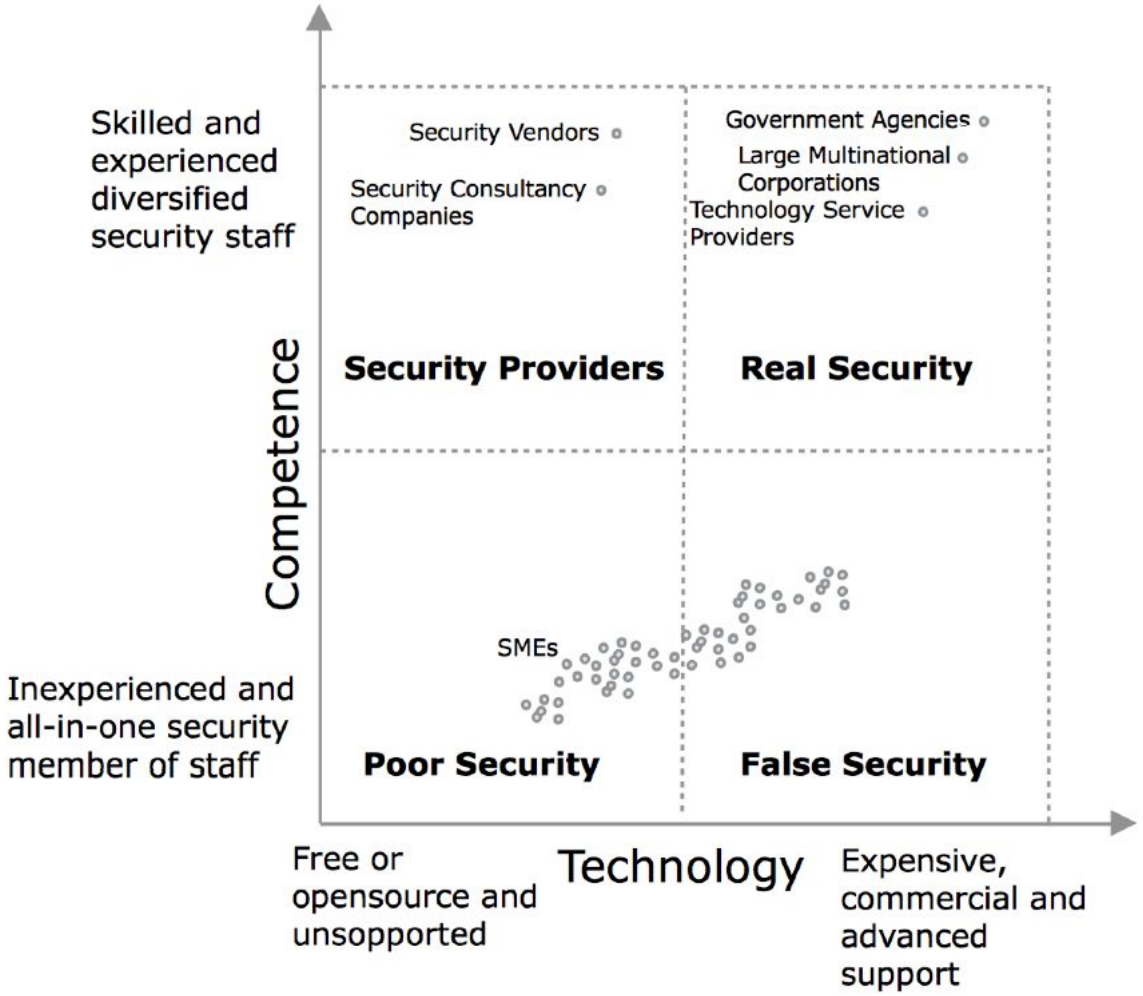
# Africa Cyber Security Landscape

silensec
Information Security Since 1998

# About Africa Cyber Security Research

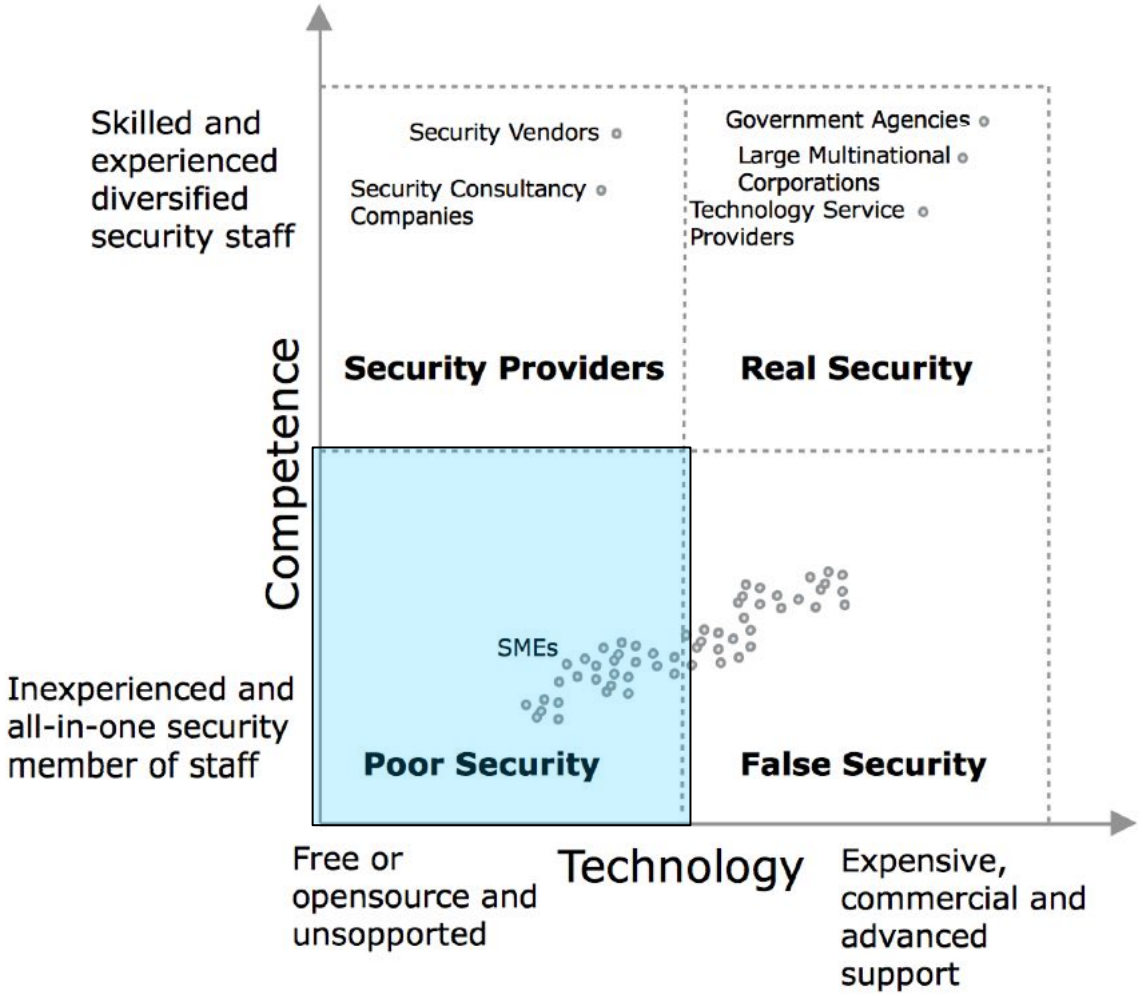
- Over 500 organizations across:
  - Kenya, Rwanda, Uganda, Tanzania, Ethiopia, Zambia, Burundi,
- Three main sectors
  - Banking/Financial
  - Telecommunication
  - Government
- Work in progress conducted by Silensec research related to Information Security Maturity models

# Silensec Security Quadrant



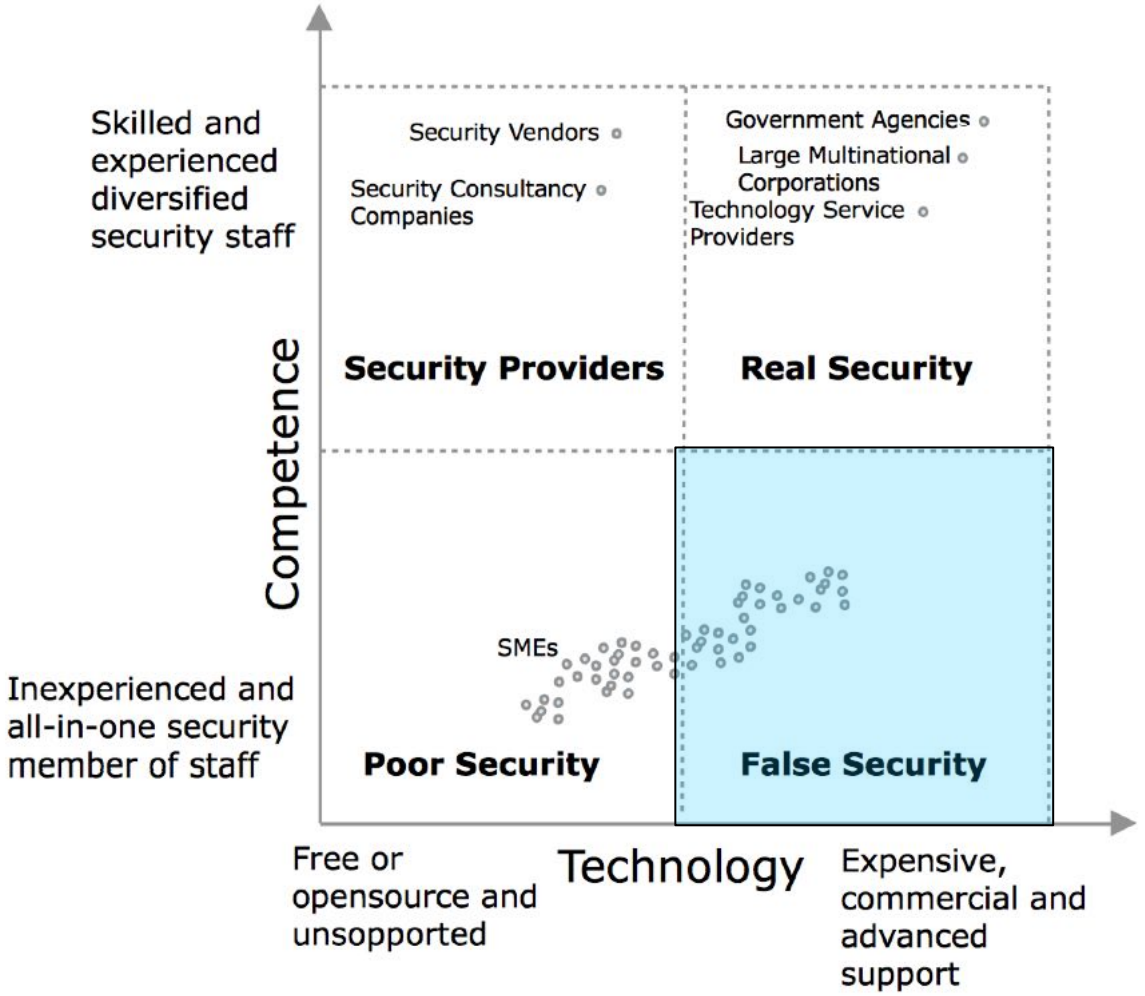

- Competence
  - Staff competence
  - Defined roles and responsibility
  - Management of Information Security
- Technology
  - Tools and systems and technologies to provide security controls

# Silensec Security Quadrant – Poor Security




- Competence
  - Weak Staff competence
  - Roles and responsibilities not clearly defined
  - No formal management of Information Security
- Technology
  - Little or no security technology
  - Mostly open source with some commercial tools

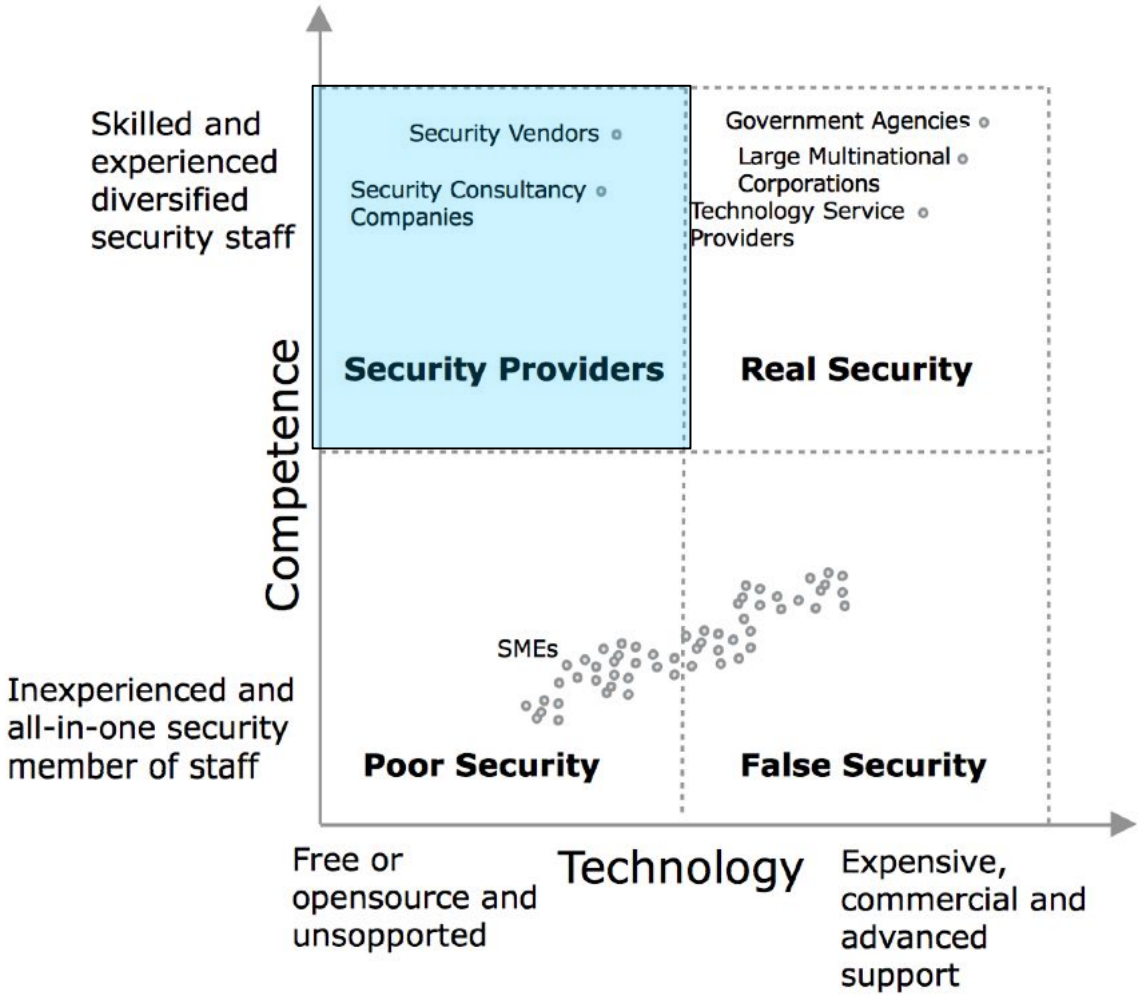
# Silensec Security Quadrant – False Security




- **Competence**
  - Some level of staff competence
  - Some roles and responsibilities
  - Some (often formal) Management of Information Security
- **Technology**
  - More investment in security tools and technologies
  - Over reliance on technology

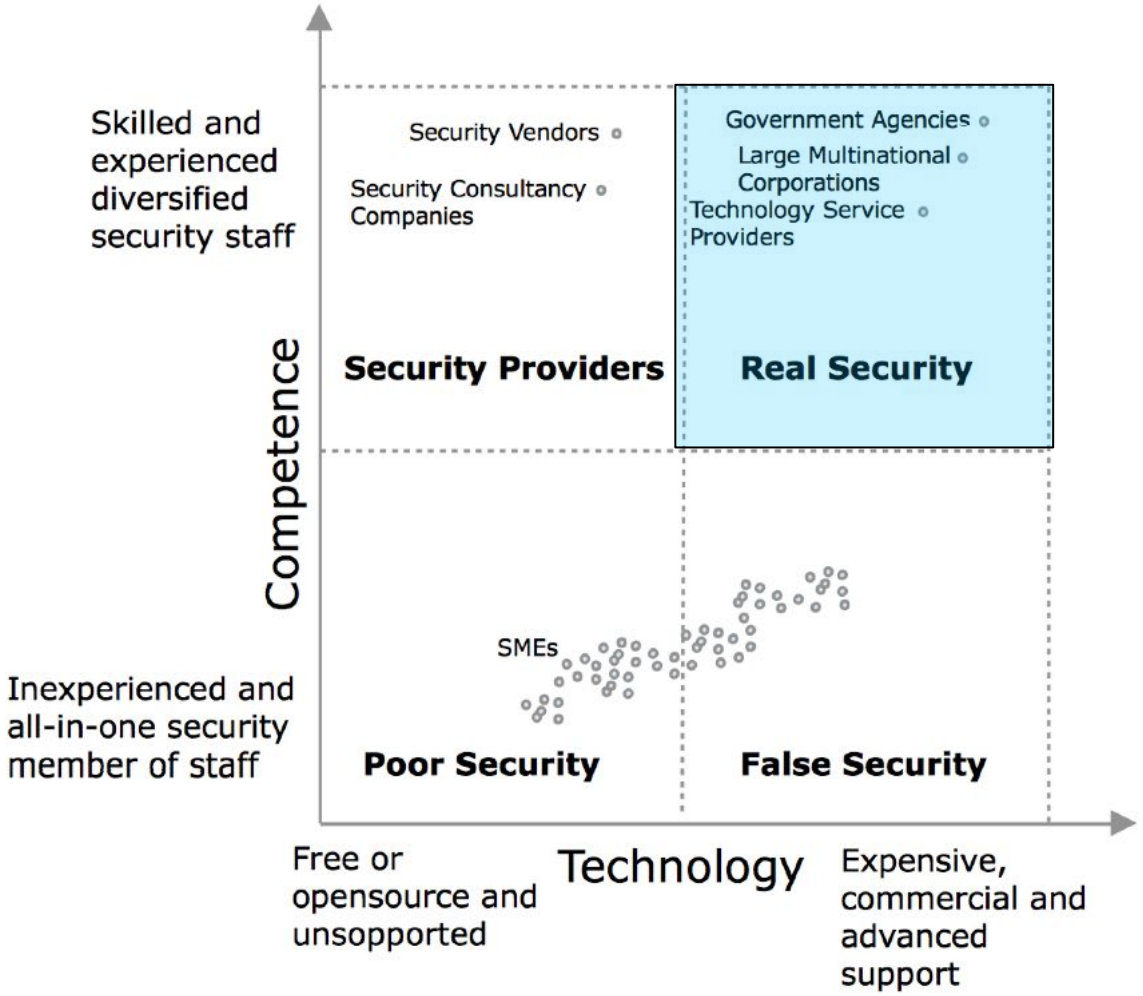
# Silensec Security Quadrant – Security Providers






- Competence
  - High level of staff competence
  - Clear roles and responsibility
  - Strong management of Information Security
- Technology
  - Strong use of “free” technology
  - Use of commercial tools to the extent needed

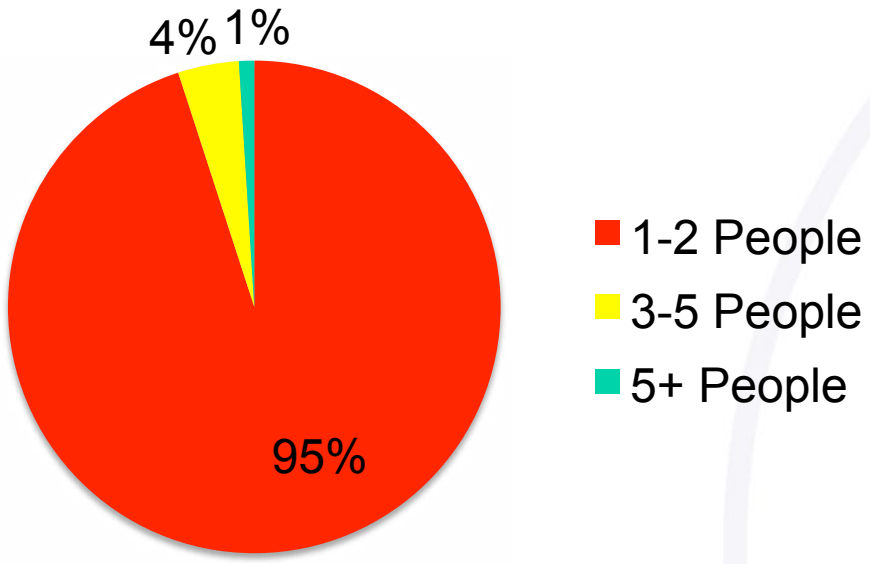
# Silensec Security Quadrant – Real Security




- Competence
  - High level of staff competence
  - Clear roles and responsibility
  - Strong management of Information Security
- Technology
  - Strong use of comemrcial security products and services
  - “free” technology

# Organization of information security

- Size of the security department




- No Information Security Role and very little decision power

# Poor Risk Management

- Very little focus on Risk Management
- Little or no risk ownership
- Little or no input into risk criteria
- Poor process documentation
- Choice of controls based on best practice rather than focused on risk mitigation

# Security Competence

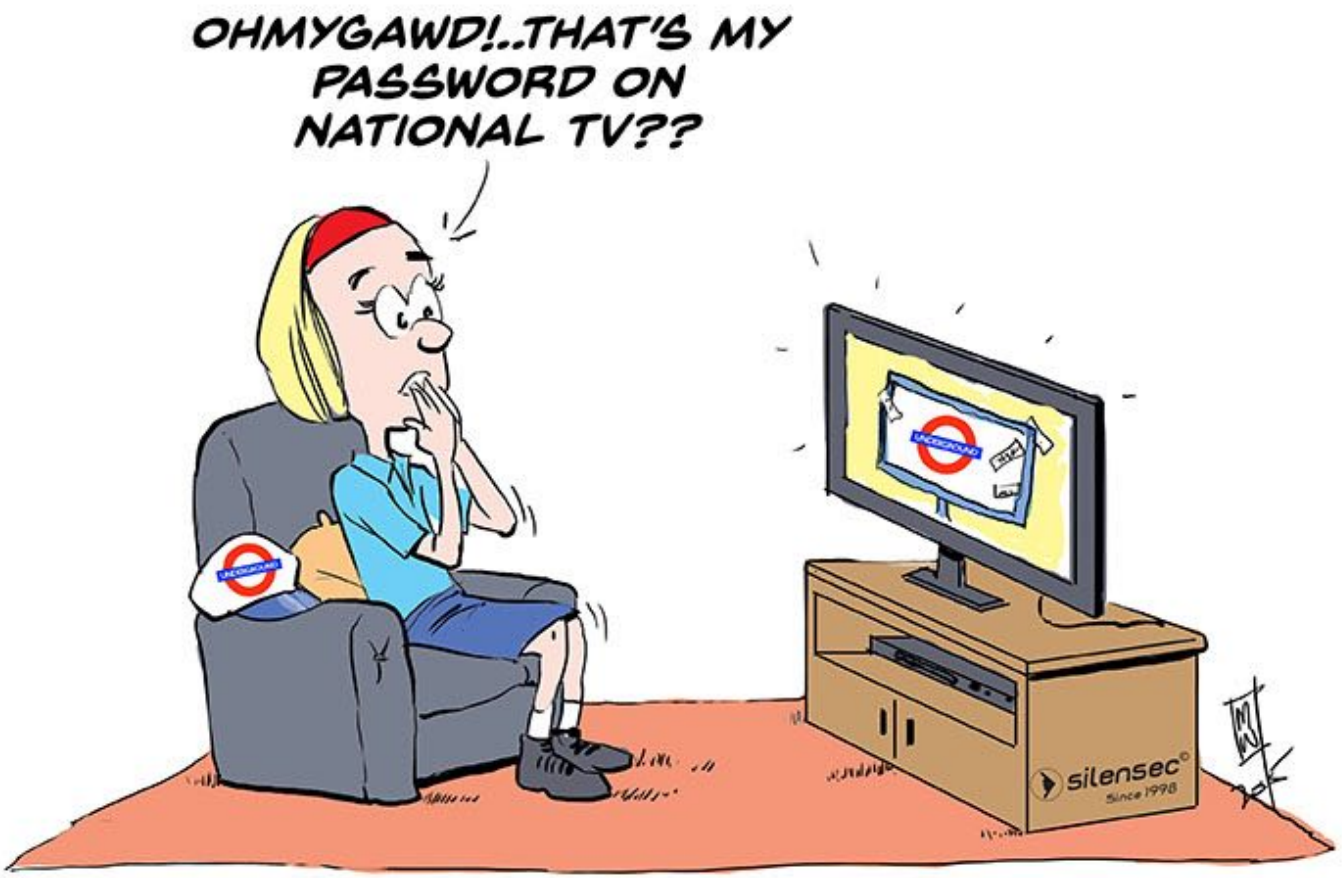
- Key missing competences
  - Secure software development
  - Web Security
  - Hacking techniques
  - Intrusion Detection and monitoring
  - Log Analysis
- Typical focus is on Vendor training, which assumes all the above is already in place!

# Security Awareness

- Mainly a tick box exercise and no effectiveness measurements

# London Railway System Passwords exposed by BBC Documentary






http://thehackernews.com/2015/05/railway-system-password.html

# Security Audits

- Short engagements
  - Ad hoc, driven by security incidents
  - No consistent budget allocation
  - Choice made primarily on cost
- Almost never included
  - Social Engineering
  - Physical Security Assessment
  - Source code review
  - Process Review
- Long periods of remediation
- Little or no learning
  - Misconfiguration, lack of patches, poor passwords

# Security Monitoring

- Intrusion Detection Systems
  - Some end point detection
  - Little or no NIDS and limited to edge network
- Log Management
  - No log collection (Critical applications not integrated)
  - Little or weak competence in logs review
- SIEM technologies
  - Still in early stages
  - Weak implementations
  - Weak core competences for monitoring and investigations
  - Weak integrations

If you bought a brand new car and soon after the purchase you discovered faulty breaks, faulty lights or faulty safety belts, who would you expect to pay for those faults?

Let's Talk About Software Security!

# Secure Software Development



- Local Software Vendors do not have/follow Secure Software Development Methodology
  - Software is developed to meet functionality requirements
  - Security Requirements are limited to authentication, access control and encryption, all of which are weakly implemented
  - Only UAT performed and no evidence of security testing performed, either internally or by a Third party
- Financial applications, like cars, are not built to just work. As cars, they have to guarantee safety

# Building Secure Software

- Answer the following questions:
  - Which university teaches courses on secure software development?
  - Which security training provider offer professional competence building courses in secure development
  - Where did the vendor's developers learn to develop secure applications?
  - How does the vendor ensure that its applications are developed to meet and exceed best practice security standards?

# Building Secure Software – The Challenge



- Many financial institutions, including telecom, partner with software vendors to provide (microfinance) financial services
- Sample model
  - Bank A partners with Vendor B to provide Service C
  - Revenue from financial transaction made through Service C are share between the Bank and the Vendor
  - Vendor takes care of support and availability of service
- The Challenge
  - The bank is still affected by fraud both financially and in terms of reputation

# Building Secure Software – The Remedy



- Software vendors must be pushed to take ownership of the responsibility to develop Secure Software
- Sample approach

1) Demand
   - Proof of Developer's competence in secure software development
   - A copy of the vendor's Secure Software Development methodology
   - Proof that the methodology has been followed (not just paper policy). Examples include: threat modeling, source code review, security testing plan and results etc
2) Obtain signed commitment to pay for third party penetration testing and/or penalties should a test by the Bank reveal critical vulnerabilities

# Source Code Review

- Manual, labour-intensive assessment
- It requires competences in
  - Secure Software Development Methodology
  - Application-specific programming language
  - Hacking techniques
- Many Systems are developed multiple technologies
- Example: Mobile banking
  - Java, C, .Net etc

# Source Code Review – The Challenge



- Vendors refuse to make source code available and do not provide evidence of any source code review performed.
- Irony: Many vendors take very little care of their source code
  - Copies deployed on client infrastructure with poor security and protection of the same
- More expensive than standard penetration testing
  - Most professional companies will charge $2500 per day
- Including source code review is likely to increase
  - Testing time unless multiple testers are employed
  - Release date of the application (more vulnerabilities will be found, which need to be remediated

# Typical Distribution of Web Vulnerabilities



| Threat Classification | N of Vulns | N of Sites | Vulns% | Sites% |
|---|---|---|---|---|
| Information leakage | 31527 | 7942 | 32.32% | 65.17% |
| Cross-Site Scripting | 37624 | 4686 | 38.57% | 38.45% |
| Insufficient Transport Layer Protection | 4317 | 4195 | 4.43% | 34.42% |
| Fingerprinting | 3663 | 3604 | 3.75% | 29.57% |
| SQL Injection | 6345 | 1555 | 6.50% | 12.76% |
| Improper Parsing | 1464 | 524 | 1.50% | 4.30% |
| Insufficient Authentication | 806 | 304 | 0.83% | 2.49% |
| Content Spoofing | 1564 | 304 | 1.60% | 2.49% |
| Predictable Resource Location | 1507 | 295 | 1.54% | 2.42% |
| Insufficient Authorization | 615 | 286 | 0.63% | 2.35% |
| Directory Indexing | 370 | 184 | 0.38% | 1.51% |
| HTTP Request Splitting | 311 | 162 | 0.32% | 1.33% |
| HTTP Response Splitting | 2592 | 161 | 2.66% | 1.32% |
| Cross-Site Request Forgery | 285 | 161 | 0.29% | 1.32% |
| Credential/Session Prediction | 794 | 147 | 0.81% | 1.21% |
| Path Traversal | 1563 | 139 | 1.60% | 1.14% |
| Session Fixation | 137 | 123 | 0.14% | 1.01% |

**[*] http://www.webappsec.org/projects/statistics/**

# The Importance of Source Code Review

| Finding | Percentage |
|---|---|
| Sites that can be compromised completely automatically | >13% |
| Web applications containing vulnerabilities of high risk level (Urgent and Critical) detected during automatic scanning | 49% |
| Web applications containing vulnerabilities of high risk level (Urgent and Critical) detected through detailed manual and automated assessment by white box method | >86% |

# Source Code Review – The Remedy



- Engage the vendor to demand:
  - proof of source code review by a trusted third party, or (if not available)
  - Access to source code (may consider using escrow service for source code release) and
  - Vendor to sustain the charges for source code review (due diligence)
- Ensure the above is repeated for every single software update and changes made to the applications provided

# Web Application Firewalls (WAF)



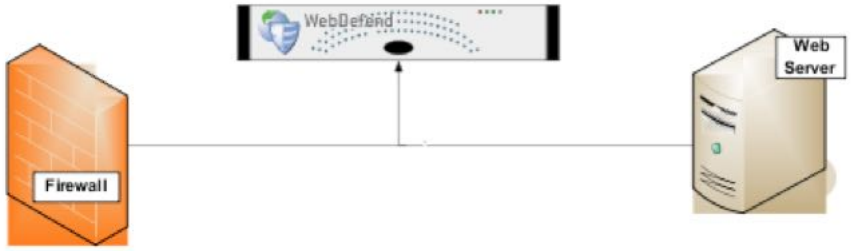
- Many organizations still rely on Network Firewalls and network IDS/IPS
  - Not designed to understand web applications and attacks against them (although not useless!)
  - Most of the web application are unique and need custom rules
- Several options
  - Commercial
    - FortiWeb by Fortinet, Defender by Fortify Software, SecureSphere by Imperva
  - Open source
    - ModSecurity, WebKnight by AQTronix, IronBee by Qualys, OpenWAF by Art of Defence

# WAF – Sample Deployments

**In-Line mode**


**Embedded mode**


**Out of line mode**



# WAF – The Challenge

- Much more complex to manage than traditional network firewall
  - Wider range regular monitoring and configuration update
  - WAF log review is more complex and requires knowledge of a wide range of Web Attacks and Web technologies
- More WAF to deploy
  - Modern OS come with built-in network firewall
  - Web servers and Web applications DO NOT

# WAF – The Remedy



- Deploy a WAF to protect critical Web Applications
- Adopt freely available and robust WAFs such as ModSecurity
  - License free
  - Easy to deploy
  - Less easy to manage
  - Invest in competence building (Web Attacks and WAF deployment and configuration)
- Invest in commercial WAF when budget becomes available

# Security Process Review



- Many companies suffer incidents because of flaws in security processes
- Examples
  - Not documented segregation of duties
  - Biased Log Review
  - Shared passwords among administrators
  - Poor review of user access rights
  - No separation of operational and development environment
- Penetration tests and vulnerability assessments are not likely to unveil such vulnerabilities
  - Yet…many company do not ask for it

# Security Process Review – The Challenge



- Security is seen as a technical problem
  - Technology-based approach
- Many consultants/companies misunderstand best practice requirements (e.g. ISO27001)
- Many companies do not maintain accurate Asset Registry
  - IT assets and Information Assets
- Many companies have weakly defined and undocumented processes
  - ISO9001 still not widely adopted

# Security Process Review – The Remedy

- Perform business process analysis and document key business processes and information security processes
- Adopt best practice standards such as ISO27001
  - Annex A provides a good checklist of 114 security controls
  - Get audited against ISO27001 requirments
- Adopt a risk approach to security
  - Prioritize risk treament based on what is important for the organization (risk evaluation criteria)
  - Document accepted risks

# Incident Management Process

Preparation

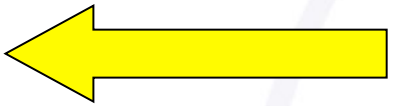
Identification

Containment

Eradication

Recovery

Learning



Many Organizations operate there

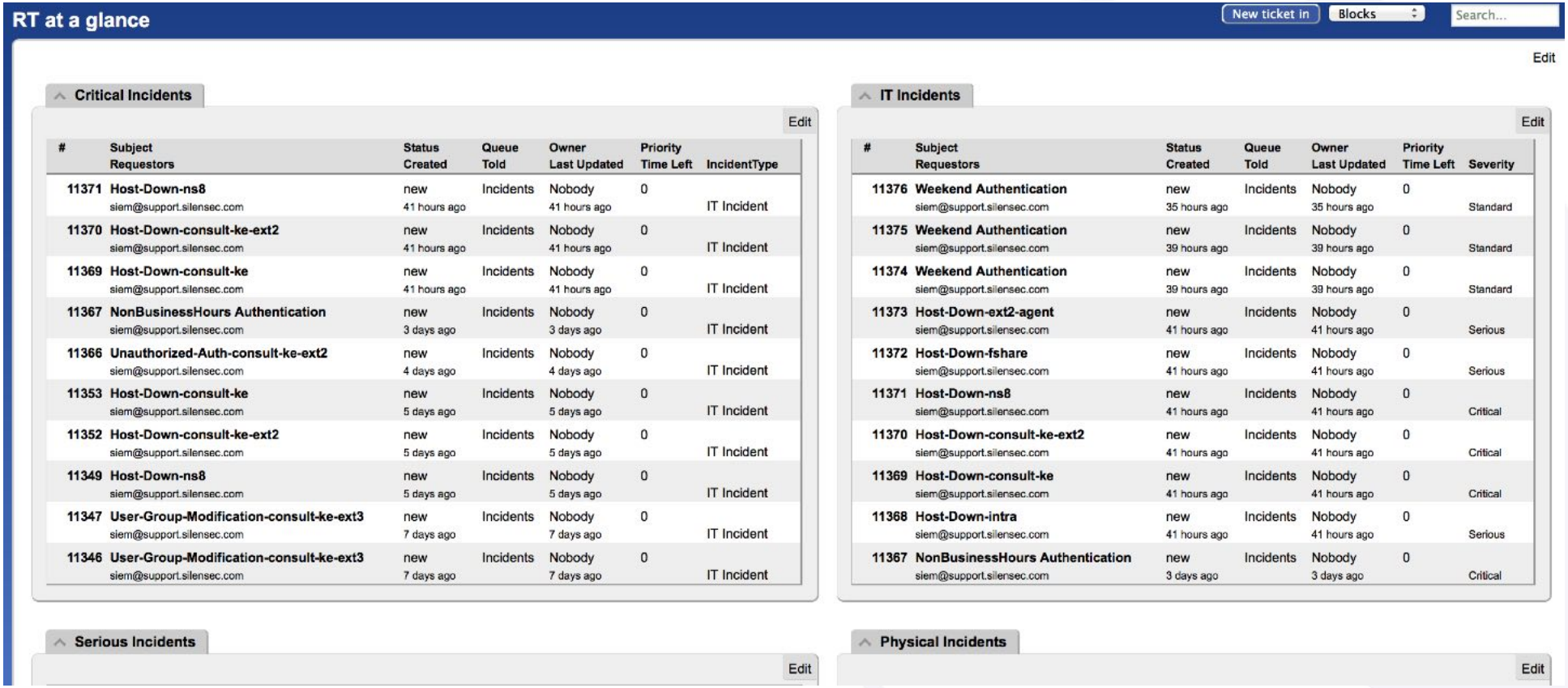
..and adopt a technology-based approach

# No Incident Management

- Many organization confuse Helpdesk with Incident Management
  - No integration with security events sources
  - No preparation
  - No review of the incident management process
- Incident Management is about
  - Identify and handling incidents
  - Learning from past mistakes
  - Reducing Impact of future incidents

# Incident Management





RT at a glance

New ticket in | Blocks | Search...

Edit

**Critical Incidents**

Edit

| # | Subject<br>Requestors | Status<br>Created | Queue<br>Told | Owner<br>Last Updated | Priority<br>Time Left | IncidentType |
|---|---|---|---|---|---|---|
| 11371 | Host-Down-ns8<br>siem@support.silensec.com | new<br>41 hours ago | Incidents | Nobody<br>41 hours ago | 0 | IT Incident |
| 11370 | Host-Down-consult-ke-ext2<br>siem@support.silensec.com | new<br>41 hours ago | Incidents | Nobody<br>41 hours ago | 0 | IT Incident |
| 11369 | Host-Down-consult-ke<br>siem@support.silensec.com | new<br>41 hours ago | Incidents | Nobody<br>41 hours ago | 0 | IT Incident |
| 11367 | NonBusinessHours Authentication<br>siem@support.silensec.com | new<br>3 days ago | Incidents | Nobody<br>3 days ago | 0 | IT Incident |
| 11366 | Unauthorized-Auth-consult-ke-ext2<br>siem@support.silensec.com | new<br>4 days ago | Incidents | Nobody<br>4 days ago | 0 | IT Incident |
| 11353 | Host-Down-consult-ke<br>siem@support.silensec.com | new<br>5 days ago | Incidents | Nobody<br>5 days ago | 0 | IT Incident |
| 11352 | Host-Down-consult-ke-ext2<br>siem@support.silensec.com | new<br>5 days ago | Incidents | Nobody<br>5 days ago | 0 | IT Incident |
| 11349 | Host-Down-ns8<br>siem@support.silensec.com | new<br>5 days ago | Incidents | Nobody<br>5 days ago | 0 | IT Incident |
| 11347 | User-Group-Modification-consult-ke-ext3<br>siem@support.silensec.com | new<br>7 days ago | Incidents | Nobody<br>7 days ago | 0 | IT Incident |
| 11346 | User-Group-Modification-consult-ke-ext3<br>siem@support.silensec.com | new<br>7 days ago | Incidents | Nobody<br>7 days ago | 0 | IT Incident |

**IT Incidents**

Edit

| # | Subject<br>Requestors | Status<br>Created | Queue<br>Told | Owner<br>Last Updated | Priority<br>Time Left | Severity |
|---|---|---|---|---|---|---|
| 11376 | Weekend Authentication<br>siem@support.silensec.com | new<br>35 hours ago | Incidents | Nobody<br>35 hours ago | 0 | Standard |
| 11375 | Weekend Authentication<br>siem@support.silensec.com | new<br>39 hours ago | Incidents | Nobody<br>39 hours ago | 0 | Standard |
| 11374 | Weekend Authentication<br>siem@support.silensec.com | new<br>39 hours ago | Incidents | Nobody<br>39 hours ago | 0 | Standard |
| 11373 | Host-Down-ext2-agent<br>siem@support.silensec.com | new<br>41 hours ago | Incidents | Nobody<br>41 hours ago | 0 | Serious |
| 11372 | Host-Down-fshare<br>siem@support.silensec.com | new<br>41 hours ago | Incidents | Nobody<br>41 hours ago | 0 | Serious |
| 11371 | Host-Down-ns8<br>siem@support.silensec.com | new<br>41 hours ago | Incidents | Nobody<br>41 hours ago | 0 | Critical |
| 11370 | Host-Down-consult-ke-ext2<br>siem@support.silensec.com | new<br>41 hours ago | Incidents | Nobody<br>41 hours ago | 0 | Critical |
| 11369 | Host-Down-consult-ke<br>siem@support.silensec.com | new<br>41 hours ago | Incidents | Nobody<br>41 hours ago | 0 | Critical |
| 11368 | Host-Down-intra<br>siem@support.silensec.com | new<br>41 hours ago | Incidents | Nobody<br>41 hours ago | 0 | Serious |
| 11367 | NonBusinessHours Authentication<br>siem@support.silensec.com | new<br>3 days ago | Incidents | Nobody<br>3 days ago | 0 | Critical |

**Serious Incidents**

Edit

**Physical Incidents**

Edit

# Learning From Incidents

## Critical Incident Management Form

| | |
|---|---|
| **CRITICAL Incident Num.** | |
| **Date the incident was reported** | |
| **Incident Reported by** | |
| **Incident Handler** | |
| **Initial Assessment** | |
| How was the incident discovered?<br><br>Which Assets where affected? | |
| **Containment** | |
| How was the incident contained? | |
| **Eradication** | |
| How was the incident eradicated? | |
| **Recovery** | |
| How was the recovery executed? | |
| **Learning** | |
| 1) Root Cause Analysis – What caused the incident?<br><br>2) What corrective action can be put in place?<br><br>3) What preventive action can be put in place?<br><br>4) What Improvements can be suggested with regards to:<br>• How to identify the incident:<br>• How to contain the incident:<br>• How to eradicate the incident:<br>• How to recover: | |

# Investigation Incidents through Network Security Monitoring



# Network Security Monitoring

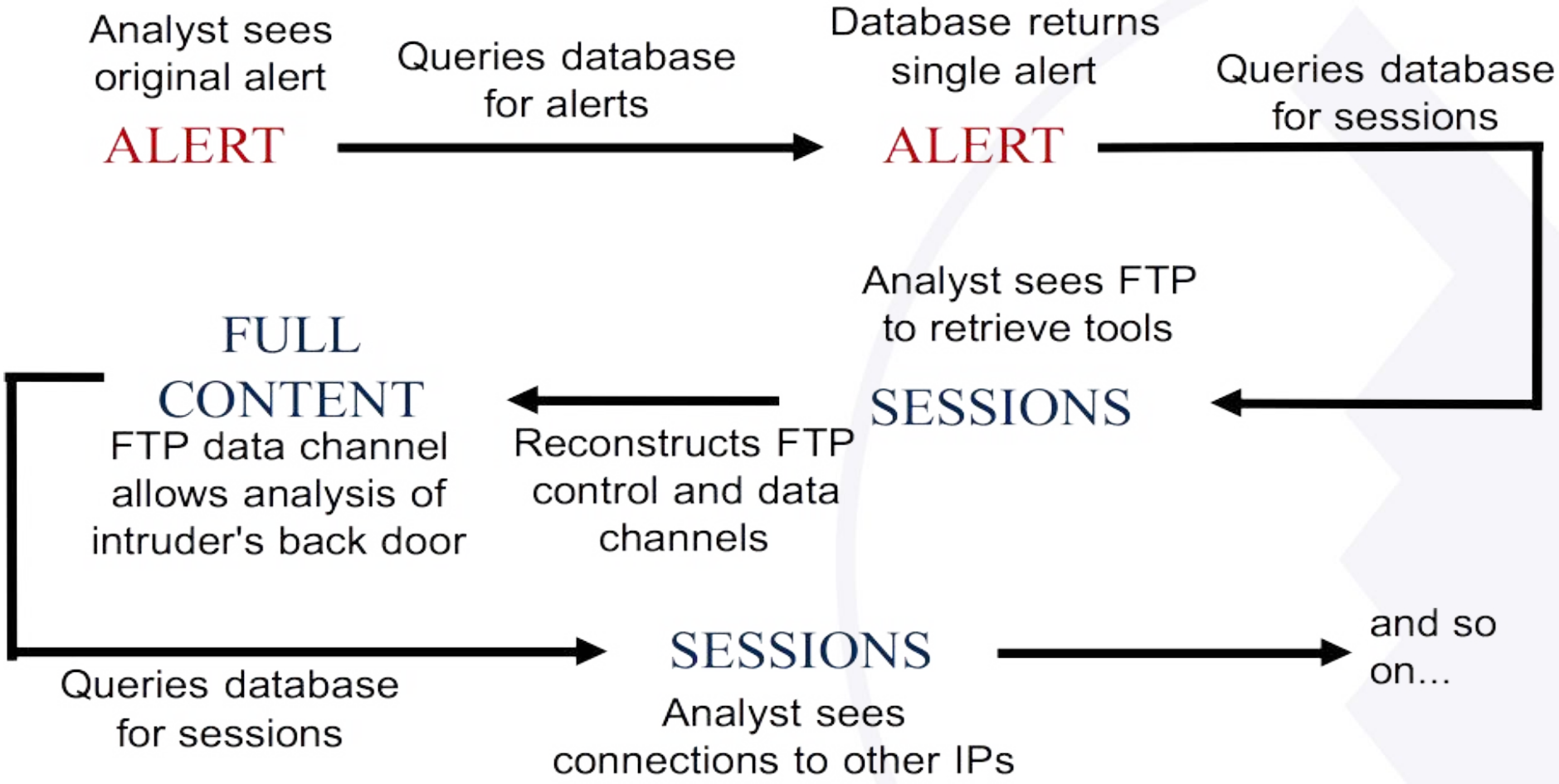


- Network Security Monitoring is:
  - *"the collection, analysis and escalation of indications and warning (I&W) to detect and respond to intrusions"* (2002, Bamm Visscher & Richard Bejtlich)
- It includes
  - Data Collection
  - Data Analysis
  - Escalation
- Misleading name
  - Not really just about "network security

# NSM Data Collection

- **Alert data**
  - Traditional IDS alerts (e.g. Snort alerts)
  - Context-sensitive, either by signature or anomaly
- **Statistical data**
  - Descriptive, high-level view of aggregated events
  - Example: Capinfos, Tcpdstat
- **Session data**
  - Summaries of conversations between systems
  - Content-neutral, compact; encryption no problem
  - Example: SANCP, NetFlow, Argus
- **Full content data**
  - All packet details, including application layer
  - Example: traffic captured with Tcpdump, Wireshark

# Investigation Using NSM



# Implementing NSM

- Not easy but accessible
- NSM is about having centralized access to all layers
- Challenge
  - Each layer served by different technologies
  - Must integrate technologies
- Many companies focus only on the Alert layer
- Incident investigation requires accessing different systems
  - Slow investigation
  - Manual correlation (effectiveness relies heavily on investigator's competence)
  - Lots of false negatives (investigation focuses on symptoms or visible alerts)

# Lessons Learned

- NSM approach allows quick and efficient investigations
- However, not technology works by itself
  - Some logs are missing from the SIEM
    - Misconfiguration
    - Incorrect requirements analysis
  - Investigation requires diverse set of skills to address attacks and anomalies to
    - Operating systems
    - Databases
    - Web Applications
    - Network Infrastructure

# The Value of Log Management in Incident Response



# The Value of Log Management in Incident Management

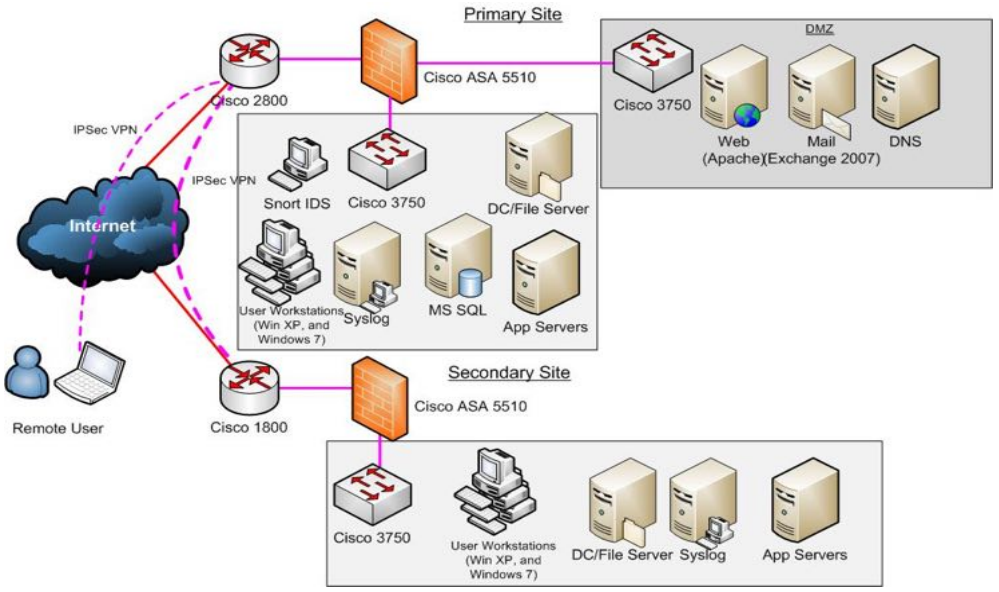


- Logs and the importance of logging
- Developing a Log Management System using the PDCA Model
- Log Management Maturity Models
- Common Mistakes
- Final Recommendations

# What is a Log?

- A log is a trace generated by an application, a system or a device capturing information about a specific event that has occurred.
- Electronic
  - E.g. Webserver logs
- Physical logs
  - E.g. Visitors Log

# Modern IT Infrastructures




**A typical company will produce tens of thousand of logs daily**

- IT/Telco Infrastructure
  - Routers, switches, Wireless APs, VoIP etc.
- Services and Applications
  - Mail, Web, Internet banking, e-commerce etc.
- Operating Systems
  - Unix/Linux, Windows, Apple etc.
- Mobile Devices
  - Mobile phones, Laptops, Pads etc.
- Security appliances and products
  - Network/Web firewalls, HIDS, IDS/IPS, Vulnerability Scanners, Antivirus, DLP etc.

# What is Log Management



- Log Management is a key process aimed at the management of logs and associated information security risks
- Log Management is NOT:
  - A technology solution or something that can be addressed by technology alone
  - Just about security

# Why Log Management



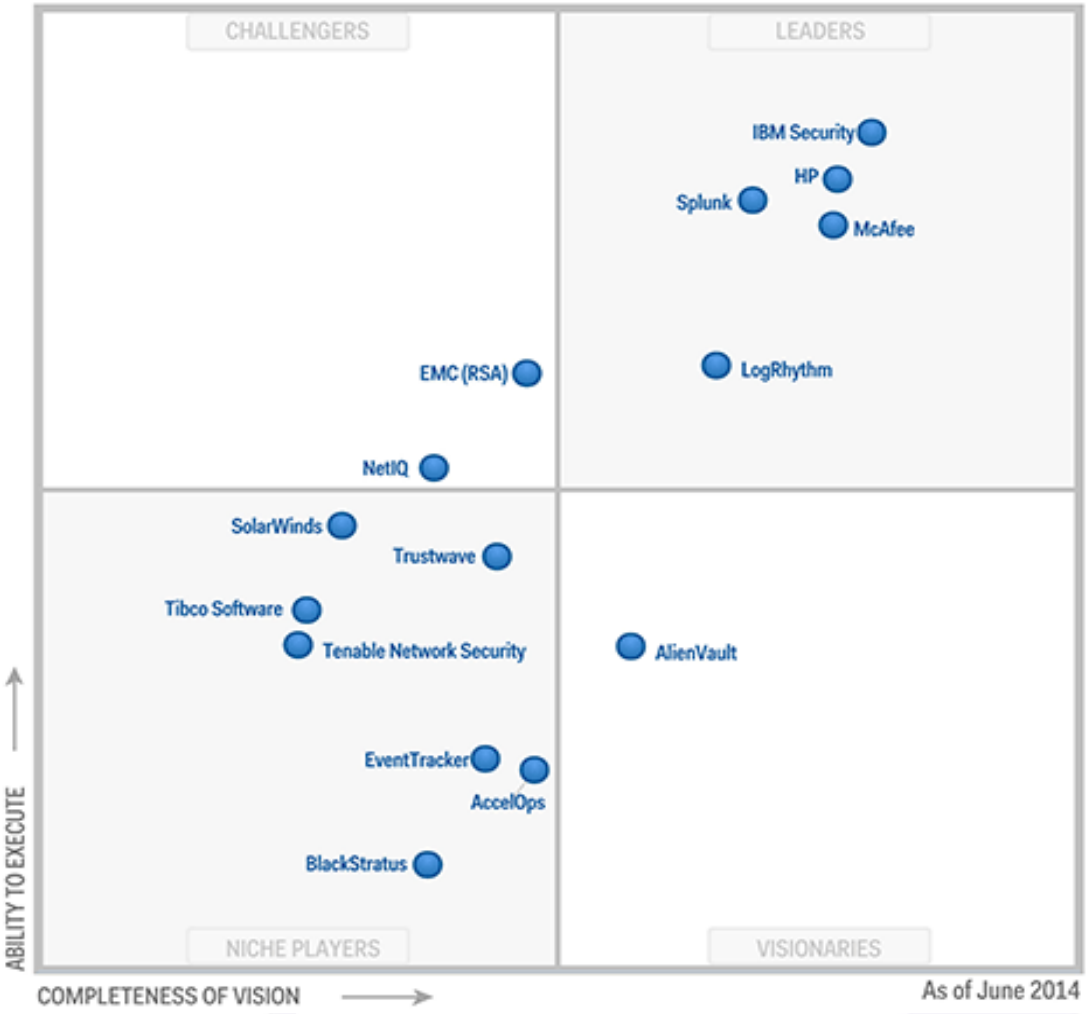
- Compliance
  - Complying with legal, regulatory and contractual obligations
- Security
  - Effectively monitoring both internal and external threats
  - Performing effective investigations of information security incidents
  - Improving overall security
- Business
  - Business analytics, measurement of process performance and achievement of objectives

# Log Management Systems Common Features

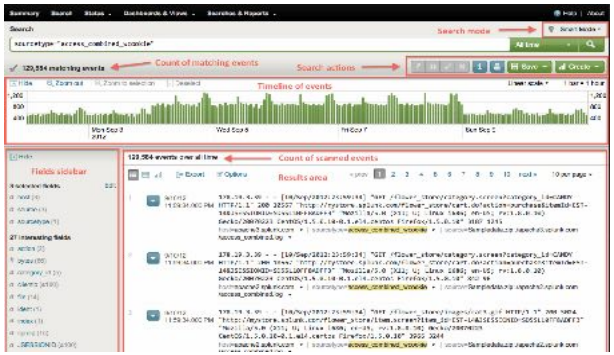
- Collection (from different sources)
- Aggregation
- Normalization
- Compression and storage
- Correlation
- Alerting
- Reporting

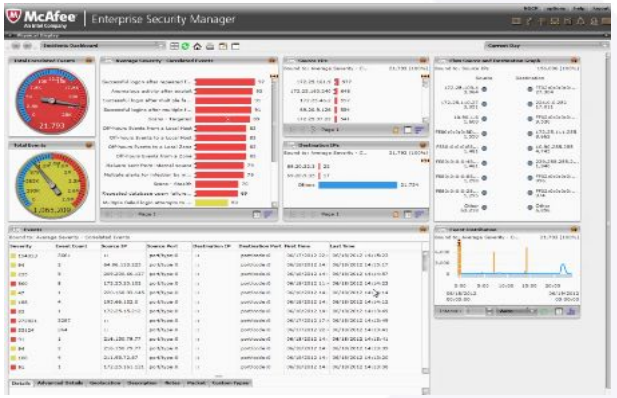
# Gartner Magic Quadrant for Security Information and Event Management 2014

Which Solution would you buy for Log Management?

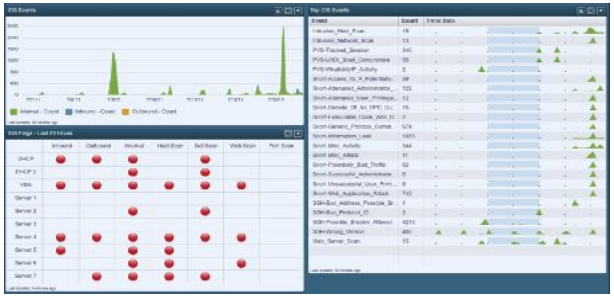


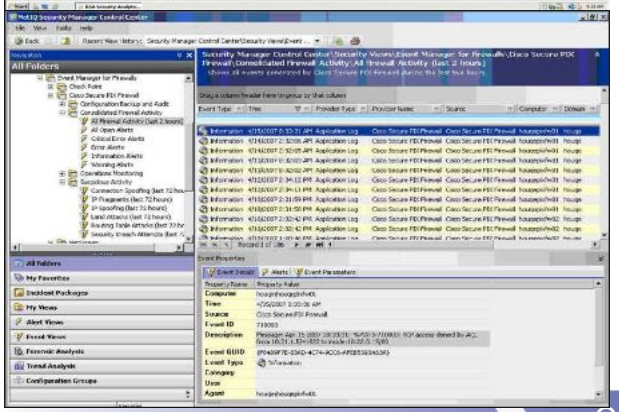
# What Would you Choose?










silensec
Information Security Since 1998

Cyberdrill for Africa
5-7 May 2015
Kigali, Rwanda



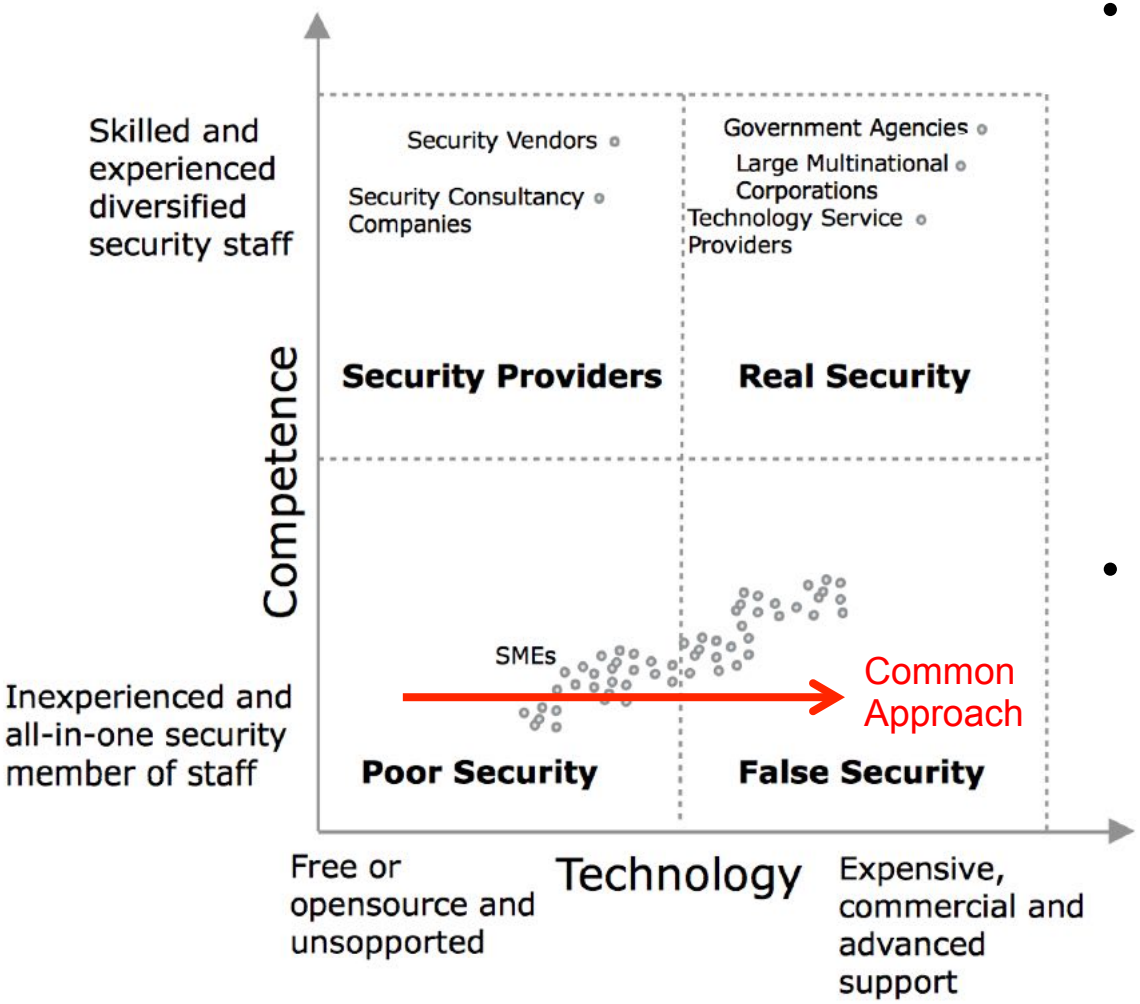

Version 1

# SIEM vs. Log Management



- Much confusion around SIEM
  - Log Management is about logs not just security logs
  - SIEM is about security
- Vendor convergence
  - LM roots vs. SIEM roots

# Common Approach to Log Management



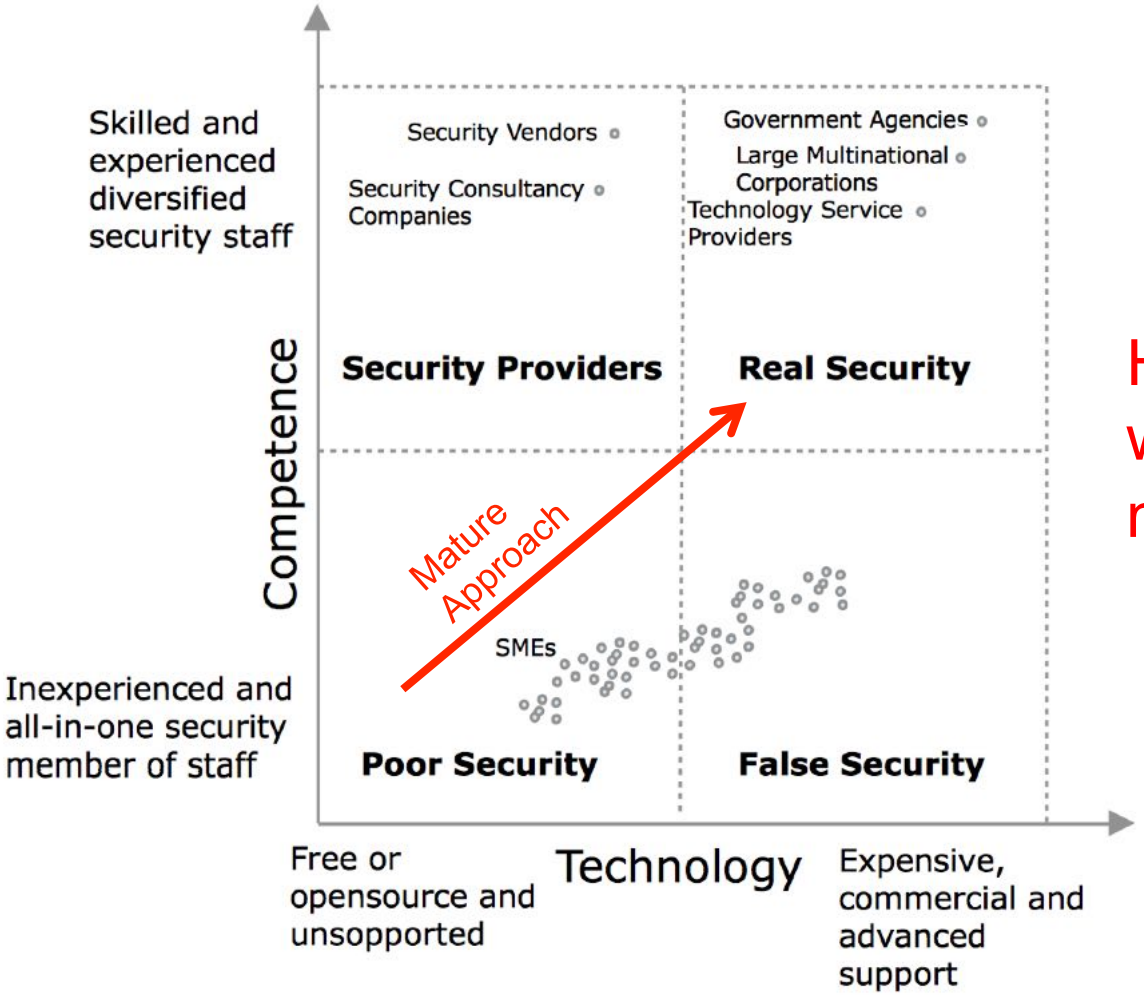

- Competence
  - No focus on people, competence and supporting controls
  - Weak or no defined processes
    - Requirements analysis
    - Log review and analysis
    - Improvements
  - Log everything and store it for as long as we can
  - Alert on anything and everything
- Technology
  - Looking for the safe choice rather than the right one!
  - Limited integration
    - No bespoke systems and applications
  - Not fully utilized
    - Default correlation rules and reporting

# Achieving Maturity

- Physical
- Mental
- Spiritual
- Social
- Sentimental
- Professional

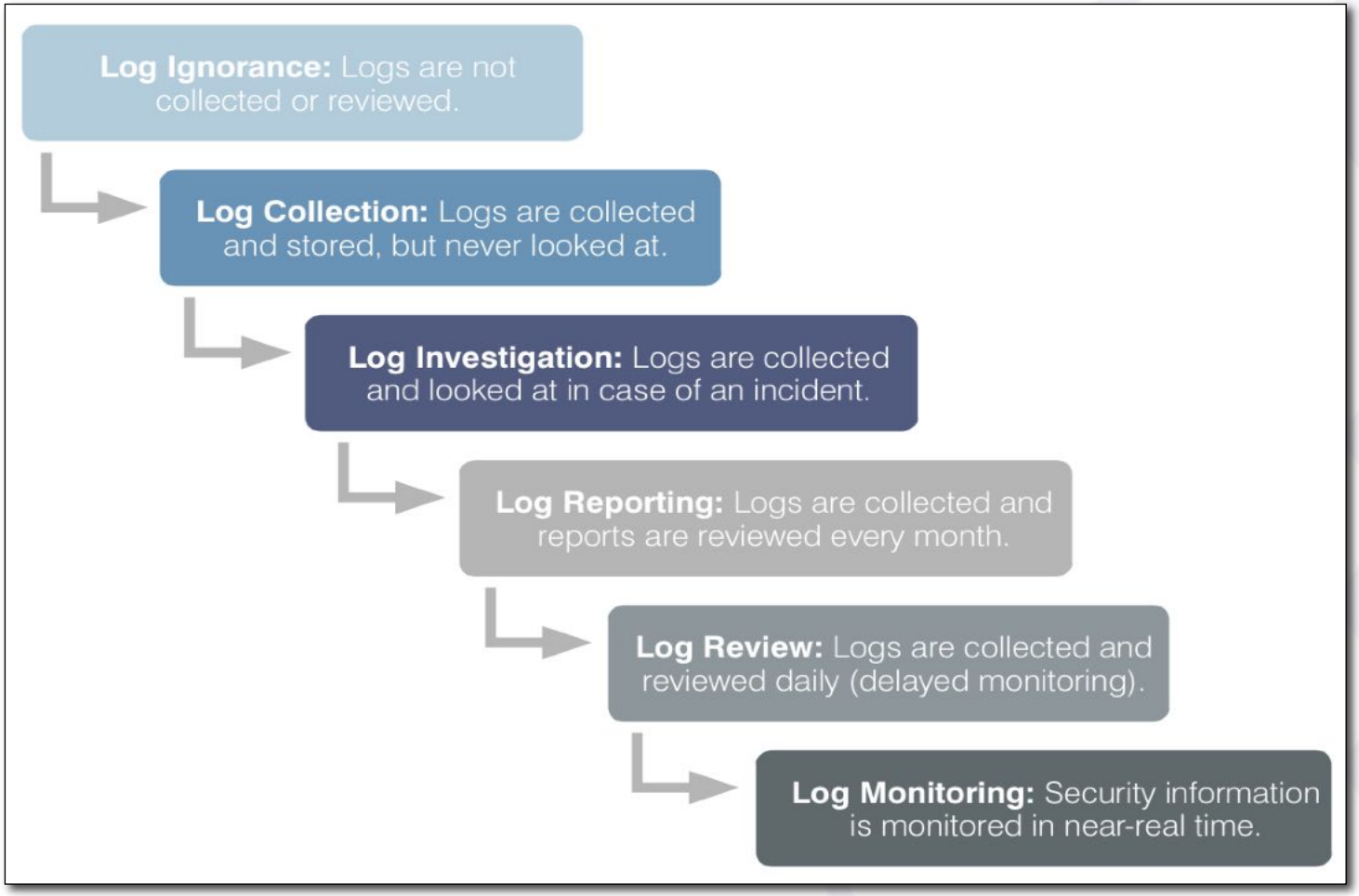
Achieving Maturity means achieving a conscious and accepted balance of maturity across all levels against one's stated objectives

# Mature Approach to Log Management



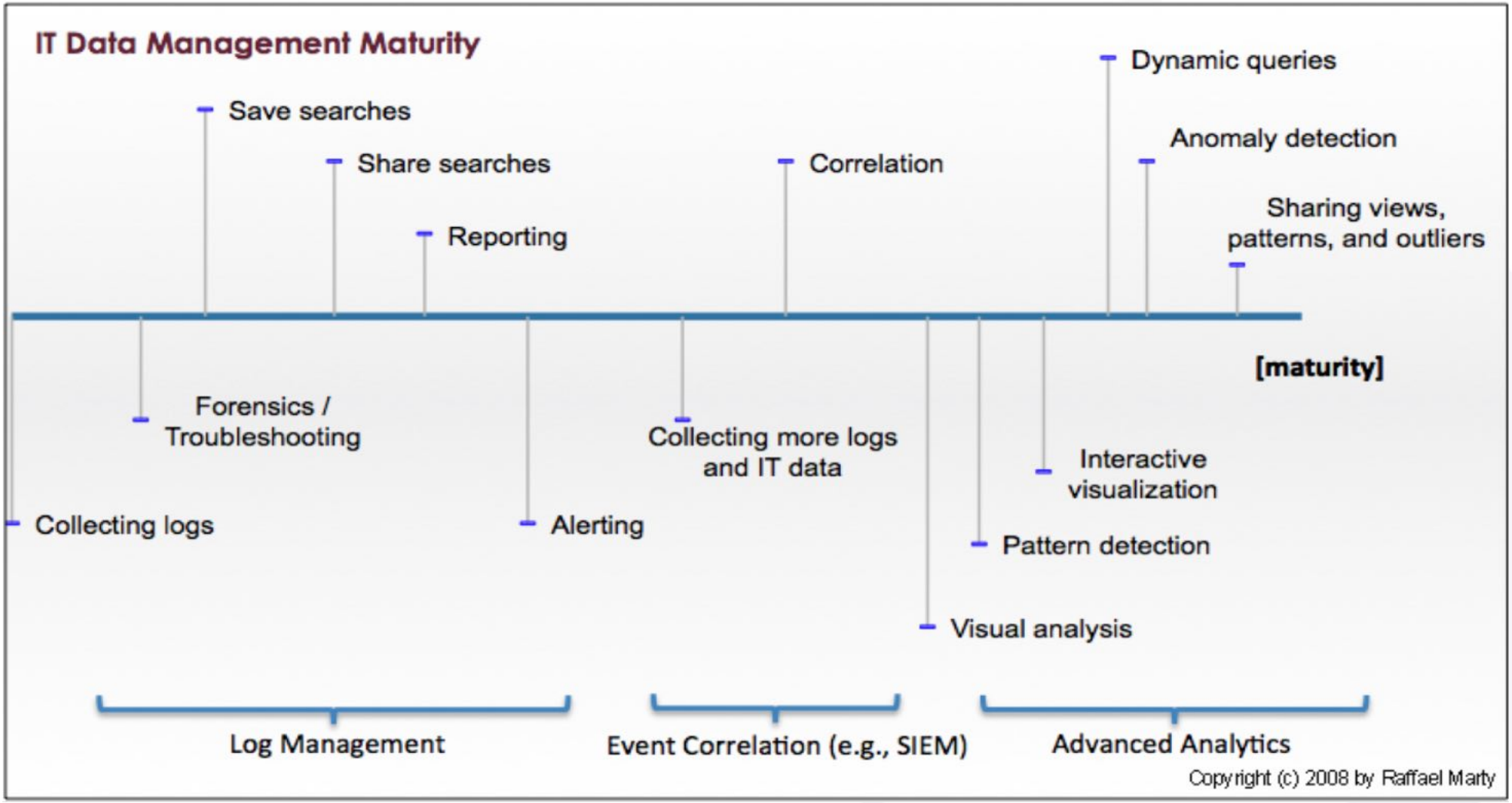

How do we achieve maturity when talking about log management?

# Log Management Maturity – Example 1



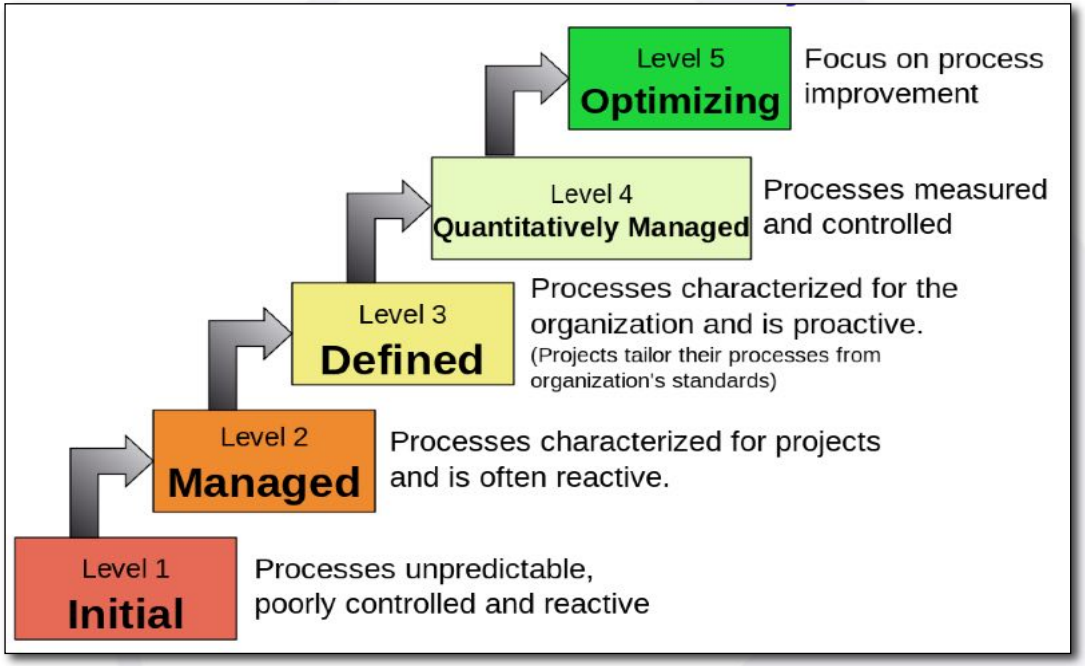

**[*] Anton Chuvakin (Gartner)**

# Log Management Maturity – Example 2



# Capability Maturity Model Integration (CMMI)

- Developed and maintained by Carnegie Mellon University
  - Process improvement training and appraisal program and service
- Required by many DoD and U.S. Government contracts (especially in software development)



# Developing A Log Management System (LMS)


- PDCA Model
  - Widely adopted across a number of international standards
  - ISO9001, ISO27001, ISO22301 etc.
- Four Phases
  - **Plan** – Scoping, Requirement analysis, Risk Assessment, selection of controls
  - **Do** – Implementation of controls and key processes
  - **Check** – Execution of monitoring processes and identification of improvements
  - **Act** – Implementation of improvements

# Applying the PDCA Model


**Plan**

- Organizational Context
  - Why are we logging and what are we trying to achieve
  - Scope
- Roles and Responsibilities
- Requirements Analysis
  - Log and Alerts Schedules, Retention Schedule
  - Logs Security Requirements
- Risk Assessment
- Choice of Log Management solution

Drives

**Do**

- Competence Building
- Implementation of supporting controls
- Development of Log Management processes
- Deployment and integration of Log Management solution

**Check**

- Log review and analysis
- Log Reporting

**Act**

- Implementation of improvements

# Log Management Foundation



- For Log Management to work and deliver on its promises we must be able to trust the logs being generated and ensure those logs are generated in the first place
- Key Supporting Controls
  - Segregation of duties
  - Password Management
  - Patch Management
  - Vulnerability Management

# CMMI-Based Log Management Maturity Model

| Level | Description |
|---|---|
| Level 0<br>Non Existent | Logs are generated based on default settings and not centrally collected. Staff has little or no competence in log analysis with no log review being carried out. |
| Level 1<br>Initial | The organization has an ad hoc and inconsistent approach to log management, with log collection and based on default settings and mainly for some important assets. There is no established log management process and no log review or analysis is being carried out. Any log management activity is down to the specific competence of staff. |
| Level 2<br>Managed | The organization has a consistent overall approach, but it is mostly undocumented, including roles and responsibilities. The log management process has been established from requirement analysis up to monitoring and improvement and it is somehow repeatable, possibly with consistent results. The organization is also capable of ensuring a correct execution of the log management activities during times of stress such as during an incident investigation although the process may lack in effectiveness and efficiency. |
| Level 3<br>Defined | The log management process is more thoroughly documented and in much more detail, defining clear roles and responsibilities and tools and techniques for log management activities. The organization is able to take full advantage of the log management process in a consistent and much more proactive way, through well documented reviewing activities. However, at this level there is not a strong emphasis on improvements. |
| Level 4<br>Quantifiable Managed | On top of the documented log management process, the organization has a documented approach for monitoring and measuring effectiveness and improvements. The log management process is quantitatively managed in accordance with defined metrics. |
| Level 5<br>Optimizing | This final phase is characterized by a strong emphasis on improvement and proactivity through a range of documented processes. Examples include algorithms for the analysis of large volumes of log to identify anomalies and patterns of interest that drive the implementation of changes. |

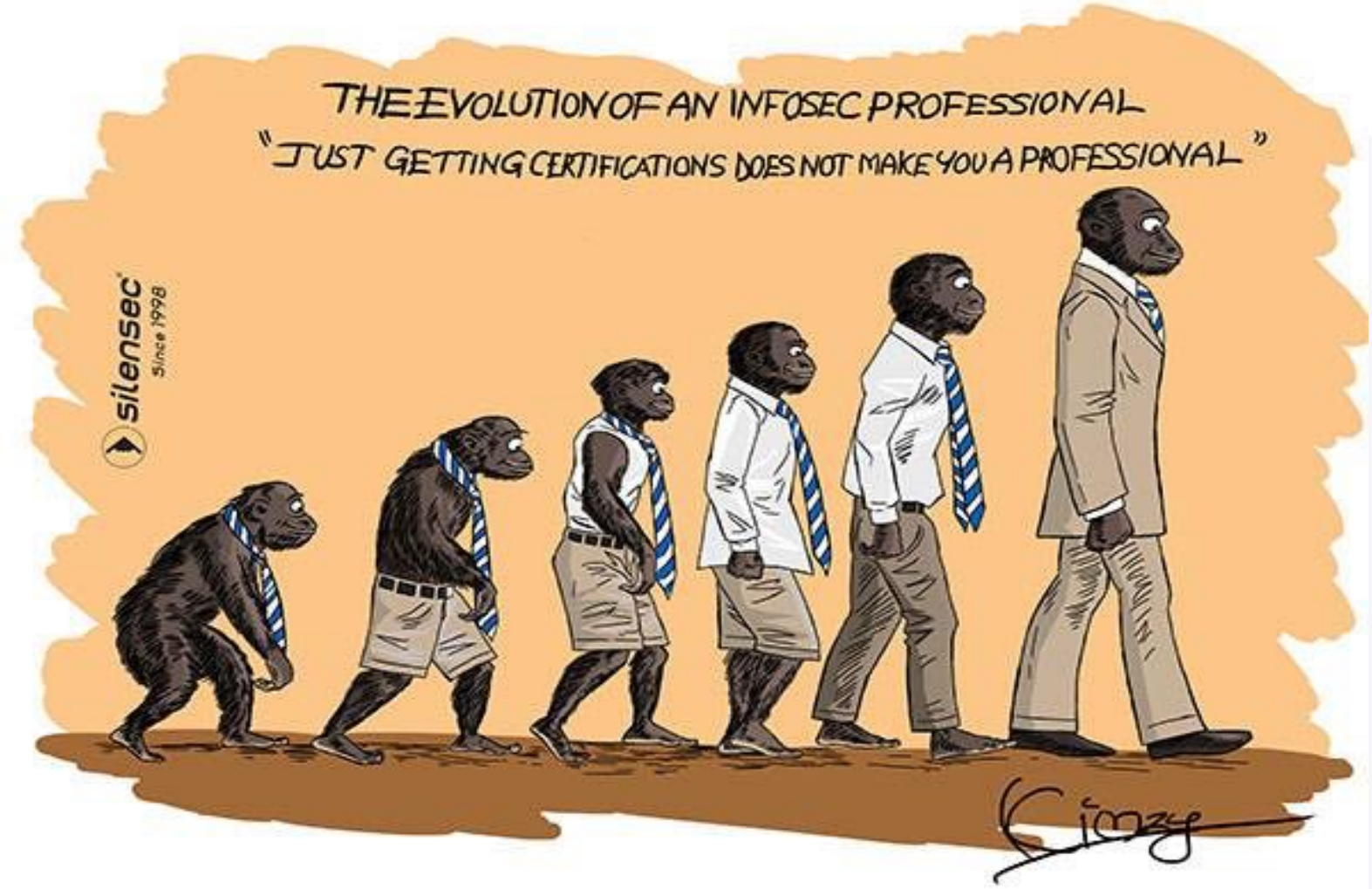
# Common Mistakes

- Buying what others are buying
- No requirements analysis
- No PoC Done
- Not Valuing Competence Building
- Only budgeting for installation and integration
- No process development
- Not buying value-added support
- Badly written RFPs

# Final Recommendations

- Focus on the processes NOT on the technology
- Spend time to understand what needs to be logged and what can be left out
- Focus on building staff competences and less on on product specific training
- Make sure supporting controls are in place

# Take your time to reach maturity!



Thank You

Questions?