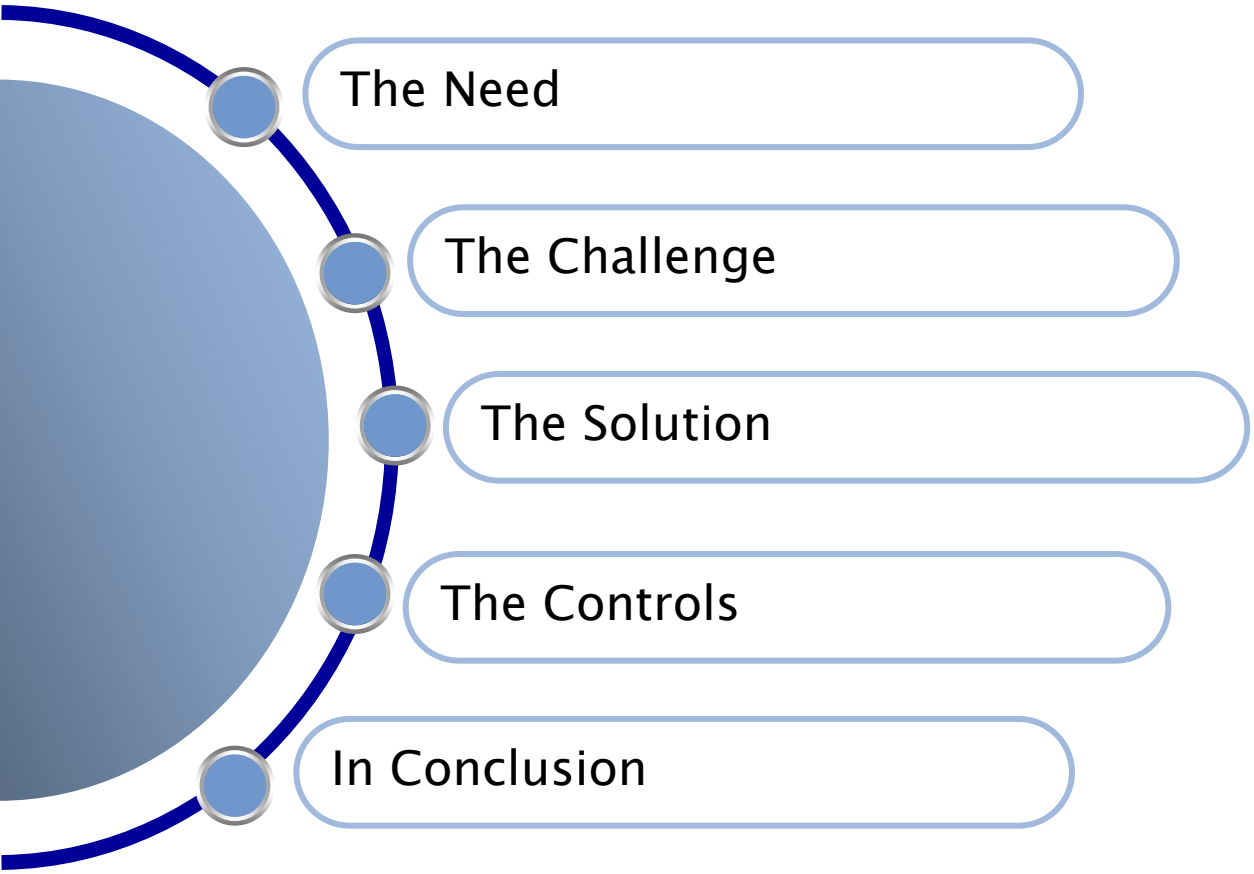
Watching the *"Watchers"*

3rd InfoCom Security, Athens, 10 Arpil 2013

Kostas Kolokotronis
Manager, Security Architecture Services
CISSP, PCI DSS QSA

Table of Contents



encode
Information Risk Management

Watching the *"Watchers"*

- The Need

encode
Information Risk Management

The Need for Privileged Users Monitoring

- **Insider Threat**
  - 57% of insider security attacks were carried out by employees who at one time had privileged user status – "Insider Threat Survey", CERT
- **External Threat**
  - In 100% of APT-type of attacks there is a case of Account Hijacking and misuse of Privileged User credentials
- **Today's Social & Economical conditions**
  - Disappointed & disgruntled employees losing their jobs
  - Tremendous increase in privileged access abuse incidents
  - Organizations have already started taking measures
- **Compliance Mandate**
  - Global security standards (such as PCI DSS, SOX etc.) explicitly require that administrative actions are fully audited

encode
Information Risk Management

Watching the *"Watchers"*

- The Challenge

encode
Information Risk Management

The Challenge of Privileged Users Monitoring

- **They are the "watchers"**
  - In most cases security monitoring is assigned to IT admins
  - Lack of a distinct role
  - So actually they are watching themselves!
- **User Access & Activity Monitoring relies on systems' native audit mechanisms**
  - Privileged users can bypass / tamper with them
- **Lack of necessary user accountability**
  - In many cases activities are performed using shared, application or generic system accounts that provide no accountability
- **Lack of centralized log management system**
  - Privileged users can harm the integrity of log records
  - Privileged users can "hide" illegal activity log records within mass volumes of not important log data

encode
Information Risk Management

Watching the *"Watchers"*

- The Solution

encode
Information Risk Management

The Solution for Privileged Users Monitoring

- **Segregation of Duties**
  - At the organization level – Creation of a distinct role for security monitoring assigned to a person/team no related with IT admin
- **Security audit tools beyond IT admins' control**
  - Use of audit tools independent to native audit mechanisms
- **Centralized monitoring solution**
  - Security audit data are promptly (near real-time) sent to centralized log management/SIEM system (in-house or MSS provider)
  - Centralized collection, processing and secure retention of log data from all critical parts of the IT environment

encode
Information Risk Management

Watching the *"Watchers"*

- The Controls

encode
Information Risk Management

The Controls for Privileged Users Monitoring – Part 1

- **Database Activity Monitoring solutions**
  - Full audit of DB users accesses and activities (including DB admins)
  - Totally independent to native DB audit mechanism
  - Minimum performance impact
  - Out of IT admins' control

- **System Configuration Audit & File Integrity Monitoring Solutions**
  - Full audit of changes performed at system configuration settings and critical files
  - Independent to native system audit mechanisms
  - Out of IT admins' control

encode
Information Risk Management

The Controls for Privileged Users Monitoring – Part 2

- **Terminal Services or VDI Infrastructure**
  - Security controlled environment – best practice for administrative and remote accesses
  - Data/Application/Network activity monitoring
  - Session Recording (best practice for forensic investigations)

- **Privileged Accounts Password Management solution**
  - Enforce strong authentication on all privileged user accesses
  - Maintain user accountability over shared or generic system accounts
  - Enforce authorization workflow for access to very critical systems

encode
Information Risk Management

The Controls for Privileged Users Monitoring – Part 3

- **Security Information & Event Management System**
  - Centralized log aggregation, processing (filtering, normalization, correlation) and secure retention
  - Real-time monitoring & alerting
  - Cross-device correlation
  - Compliance reporting
  - Enables early detection, warning & response to security incidents
  - The only effective way of security monitoring

encode
Information Risk Management

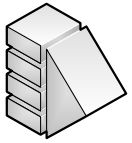
Privileged Users Monitoring – Controls/Effectiveness

Baseline
- Segregation of duties – Distinct Role
- Security logs are promptly sent to centralized log management system

Good
- + Database Activity Monitoring solution
- + System Configuration & File Integrity Monitoring solution

Advanced
- + Privileged Accounts Password Management system

DiD
- + Terminal Service or VDI infrastructure with Session Recording

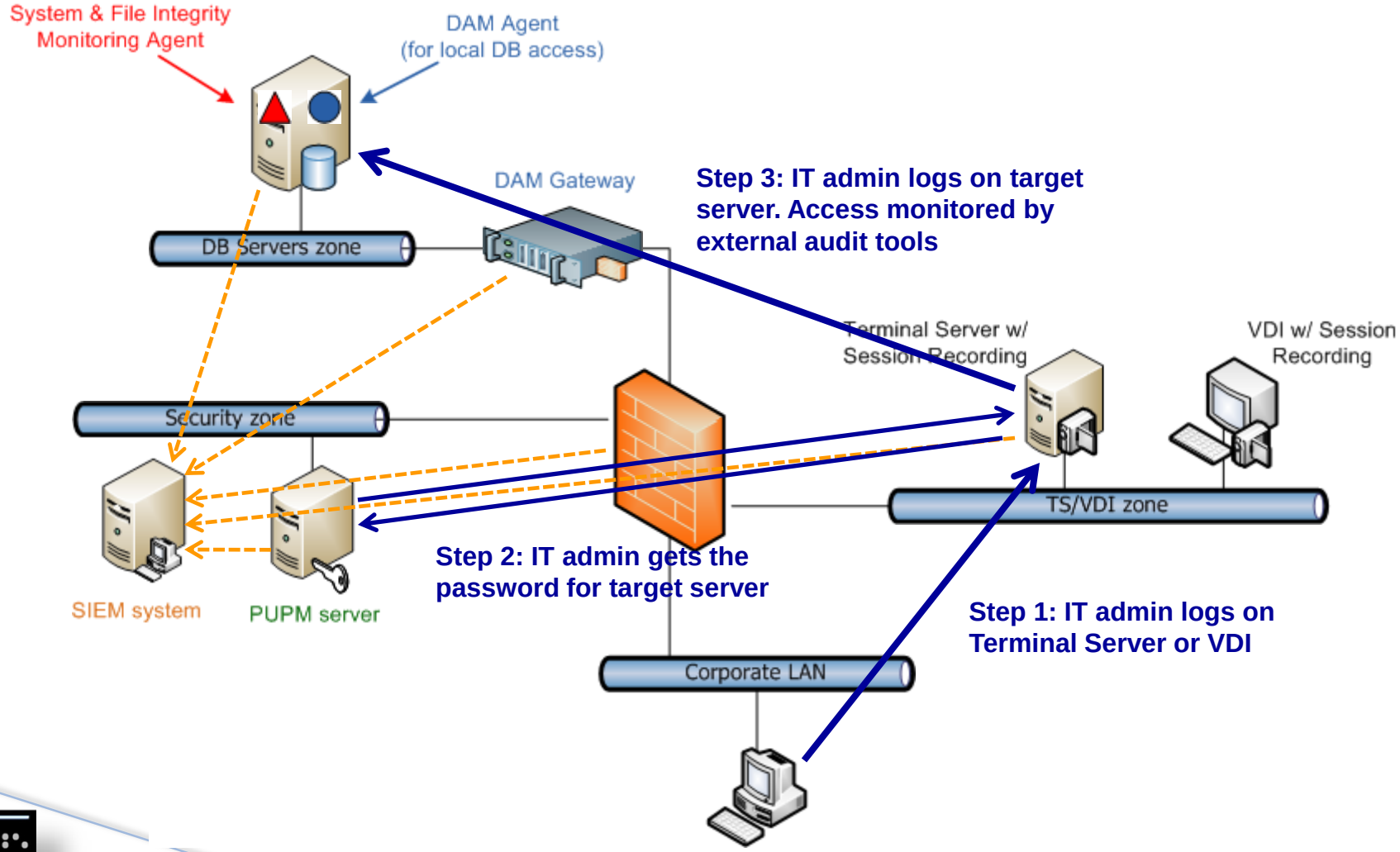


Optimized
- + Security Information & Event Management (in-house or through MSS provider)

Baseline | Good | Advanced | Defense in Depth | Optimized /effective

encode
Information Risk Management

Privileged Users Monitoring – The Complete Picture



Watching the *"Watchers"*

- In Conclusion

encode
Information Risk Management

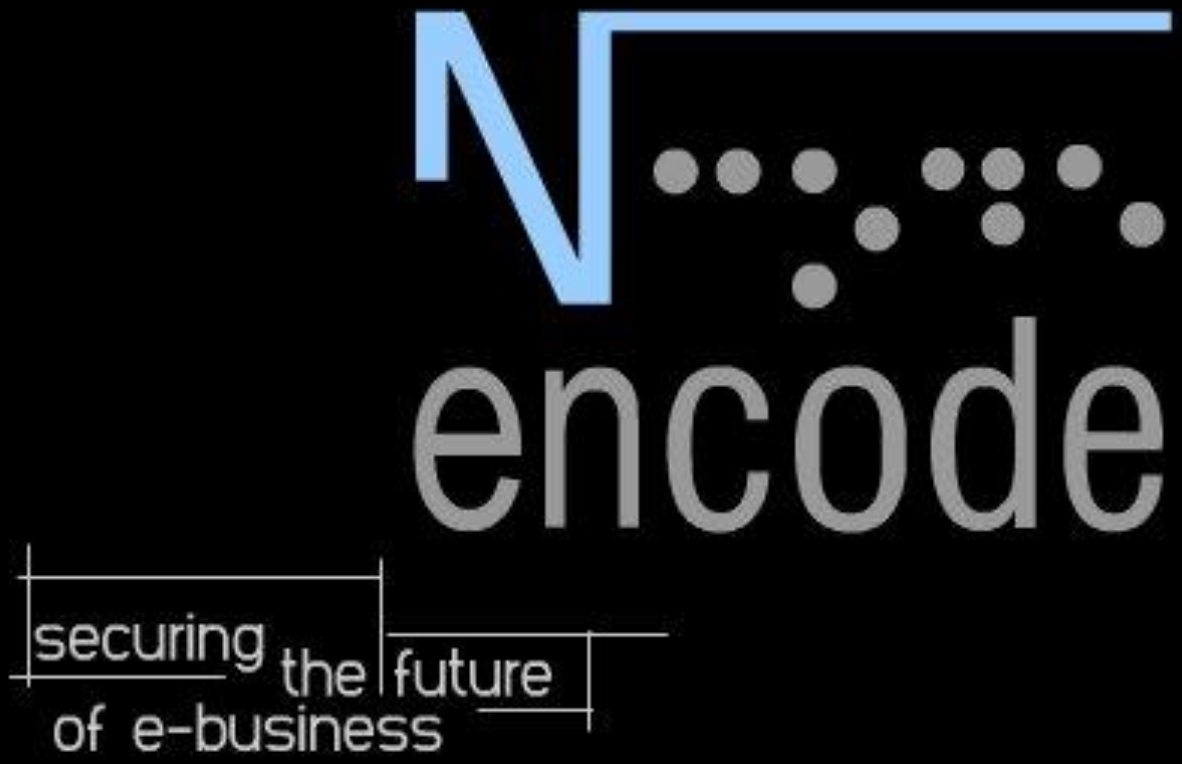
Privileged Users Monitoring In Conclusion

- **IT admins**
  - We cannot live without them
  - We cannot restrict them greatly

  however
  - We must closely monitor them!

- **This is not just a best practice, this is a major security & compliance mandate**

encode
Information Risk Management



www.encodegroup.com_