RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

A Human Factor Interface for SIEM

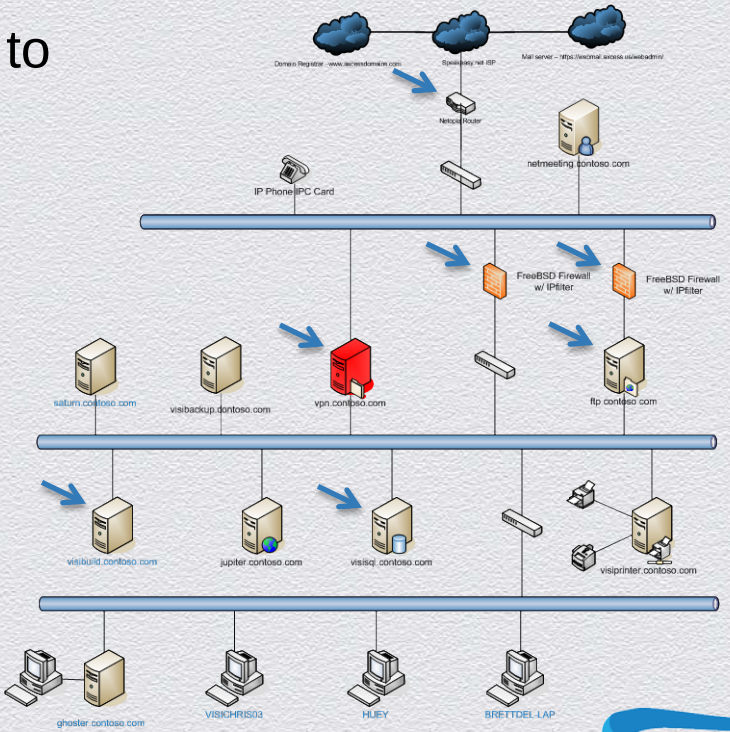
SESSION ID: ANF–R04A

Bettina Wesselmann
Information Security Communications Consultant

Johannes Wiele
Senior Information Security Consultant
Trustwave Germany GmbH

Security Information and Event Management

- SIEM systems are powerful tools to achieve security and compliance by correlating log data from disparate network sources.
- They automate information analysis tasks required by several industry security standards.



↘ Sensor / Log Source

Bettina Wesselmann
Johannes Wiele

Security Information and Event Management

- But are you really sure that SIEM technology covers all attack vectors targeting your assets?

All Photographs in this presentation:
Fotolia.com

Security Information and Event Management

- Serious attackers rely on blended threats combining hacking with social engineering and physical access...

- whereas -

- …SIEM systems correlate event logs only from IT sources!
  - Non-technical attack vectors remain unnoticed.
  - SIEM systems do not make use of human observations/intelligence.
  - Few exceptions: Laptops, mobile phones or badges reported lost or stolen.

Security Information and Event Management

- Industry information security and data privacy standards and laws require full coverage of all threats to information assets.
- ISO/IEC 27001 for example covers Human Resources, Records Management, Business Continuity, Physical Security and Risk Management.

A.13.1 Reporting information security events and weaknesses
Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

A.13.1.1 Reporting information security events
Control - Information security events shall be reported through appropriate management channels as quickly as possible.

A.13.1.2 Reporting security weaknesses
Control - All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

The Idea

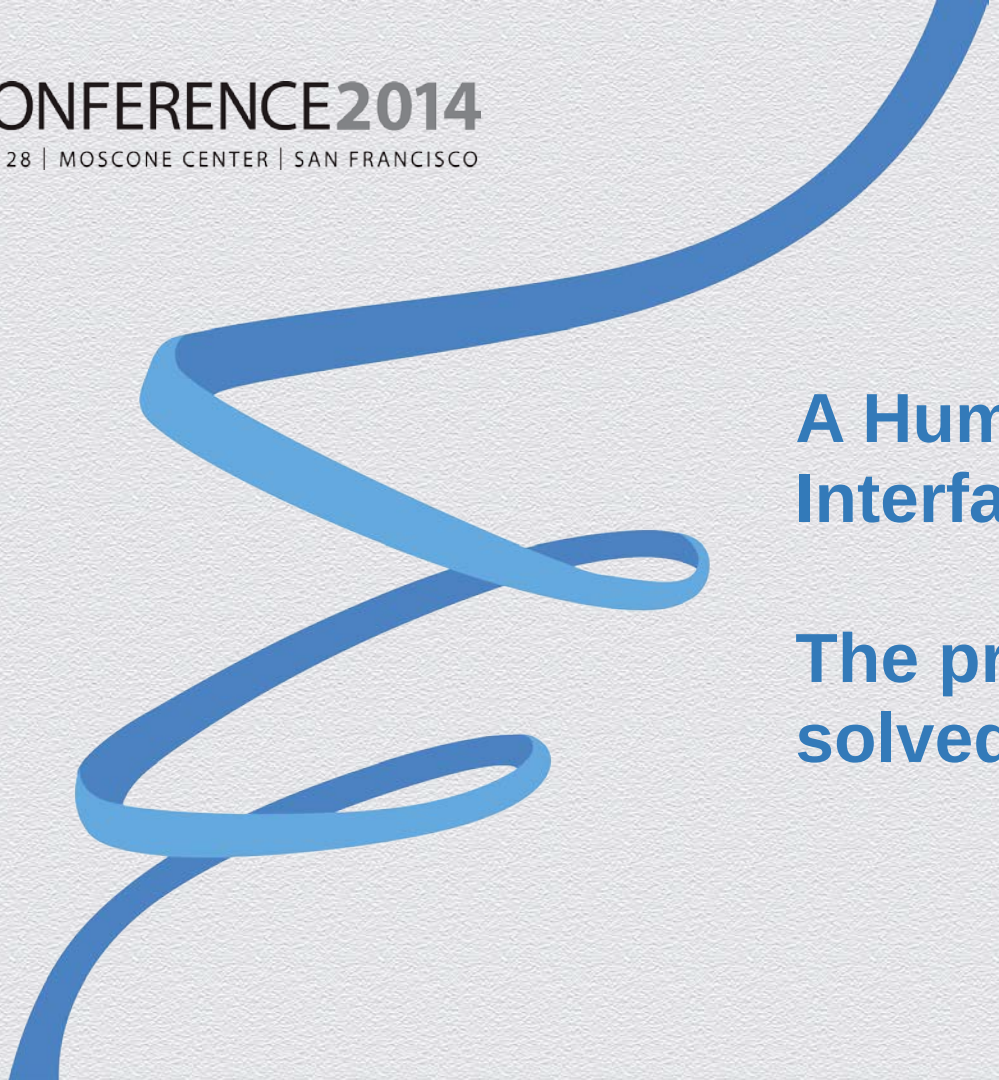
- Feed non-technical events into the correlation engines of SIEM systems.

- *Design a human factor interface for SIEM systems to acquire and process security related input provided by human beings.*

Human Intelligence & SIEM – Micro Case Study

- A seemingly harmless telephone call of an unidentified person asking for a password in order to gain access to a certain system could be a good reason for a SIEM system to take notice, if at the same day a similar call is observed at an overseas office.
- If, in addition to that, at the same time intrusion detection and firewalls show increasing hacking activities targeting the same asset, an alarm should be raised.

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



A Human Factor Interface for SIEM:

The problems to be solved in detail

Undiscovered Blended Threats

- Non-technical attack vectors include manipulative phone calls and other communicational approaches, identity theft, onsite visits, burglary and dumpster diving.
- Everyone with access to promising assets can be a target – executives, their secretaries, developers, cleaning workers, call center employees, IT specialists, human resources employees.
- Each single step is kept inconspicuous. If recognized at all, the steps are recorded at different security or business departments. There is no correlation with IT event logs.

Insufficient Security Communication Practices

- IT security, compliance management, physical security and personal security belong to different business and communication cultures.
- If organizations succeed in building an internal security communication framework involving all different security departments, in most cases this framework relies on scheduled meetings.
- Timely correlation, interdisciplinary alerting and fast reactions to blended threats have been put into practice manually only at a small number of organizations.

The Psychology of Incident Reporting

- Human beings usually are perfect anomaly detectors, but often they hesitate to report.
  - I feel uneasy about that phone call or that open window – but is it really important?
  - Will those IT people / security guys laugh at me?
  - How shall I find the right words? It's just a feeling…
  - Perhaps it was my fault and I get punished!
  - Perhaps I blame an innocent person…
  - And who after all is the one in charge?

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

How to Build a Human Factor Interface for SIEM

1. Start with a Risk Assessment

- Human Factor Risk Assessment
  - What kind of human behavior may have what influence on information security?
  - Which employees/managers would you try to manipulate to obtain access to what assets by fraud?
- How can information assets be accessed unauthorized physically?
- What information about what assets can be found on the internet?
- Define a set of communicational and physical attack vectors to be watched.
- Define critical events and corresponding threshold values.

2. Relate Non-Technical Attack Vectors to the Known Technical Ones

- Think about blended threats.
  - How could technical and non-technical attack vectors be combined to get access to critical assets?
  - What assets may provide access to other, even more critical ones?
  - Would the single steps already be recognized or fly under the existing security radar?
- As a result, define additional correlation rules.

3. Design a Web Interface

- Provide a list/menu of important assets.
- Provide a list of well-known attack methodologies.
- Alternatively allow free form entries (to learn and to cover creative attacks).
- Provide fields for time, location, role of the reporting person and an individual risk estimation.
- Program correlation rules into the interface or the SIEM system.
- Let the interface produce a log.

4. Use the Web Interface

- First step: Choose an asset (e.g. customer database, lab or credit card holder data).
- Second step: Choose or describe type of suspected attack/weakness observed (e.g. suspicious phone call, suspicious discussion at hotel bar or visitor trying to open server room door).
- Third step: Indicate own risk estimation.
- Add notes – for forensic use or further improvement (new correlation rules) of the PDCA cycle.
- Entries result in a log automatically sent to the SIEM system.

Who should use the Interface?

- Security personnel of different departments.
- For most employees: A specialized security help desk.
  - Security Help desk employees should train their communicational and psychological skills.
  - An all-hands awareness training should explicitly cover human factors. It should also introduce the use of the interface.
- Individuals who are preferred targets of social engineers may be granted direct access.

Should anonymous entries be allowed?

The Benefits

A Human Factor Interface for SIEM

- Make use of human intelligence.
- Formalized process and well-defined point of contact encourage employees to report security observations.
- With the interface added, SIEM systems cover all incident and event management requirements of industry security standards and laws.
- With the interface added, SIEM systems may help to overcome communicational barriers between different security departments.

Thank You!
johannes@wiele.com, bettina@wesselmann.com