Raytheon

Customer Success Is Our Mission

LISA 2010

Enterprise Scale Employee Monitoring

(i.e. Information Protection via Employee Monitoring)

Mario Obejas

November 11, 2010

Agenda

1. Introduction and Problem Summary
2. General Considerations when contemplating *any* Employee Monitoring implementation
3. My Employee Monitoring deployment experience
4. Final thoughts
5. Q&A

Introduction and Problem Summary

Introduction/Disclaimers

- I'm only addressing electronic monitoring
  - i.e. not video surveillance
- I'm no expert
  - My field experience is solely with Raytheon Oakley Sureview
  - Aka DLP (Data Leak Protection)
- This is my first USENIX talk, so please be patient
- I walk a fine line ….
  - I'm in IT Security, not Marketing, despite the videos
  - This talk had to be approved – by a lot of people
- I assumed 50% of you are 1st timers at LISA

Introduction/Disclaimers

- Why I proposed this talk:
  - Outside of Marketing literature, I find little published about actual experience with employee monitoring infrastructures

- Let's gamble - Show of hands:
  - How many of you have had either direct experience with employee monitoring systems, or have seen a talk or presentation about an actual deployment?
  - (I'm not counting log correlation in the pool)

The Issue: Critical Data Leakage

- **Banking and credit companies**: Identity theft, account skimming, funds diversion
- **Financial firms**: Mergers and acquisition plans, non-public financial information, private research
- **Retail organizations**: Pricing information, personal information on credit card holders, CCVs on cards.
- **Public companies**: Earnings information not yet distributed to the market, new product information before release, intellectual property.
- **The government**: National secrets, classified and personal

How does the leakage occur?

- Exfiltration
  - Classified/Proprietary/PII data leaks
  - Classified and Proprietary Data spills
  - Employee computer policy violations
  - Espionage
    - Advanced Persistent Threat (APT) activity
  - Social Networking site leaks
  - Unencrypted removable media

- Insider Threat

INSIDER THREAT INSIDER THREAT INSIDER THREAT

Malicious Insider Definition:

- Current or former employee, contractor, or other business partner who
  - has or had authorized access to an organization's network, system or data and
  - intentionally exceeded or misused that access in a manner that
  - negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

(Definition Source : Software Engineering Institute, RSA Conference 2010)

- malicious insider

Trusted Malicious Insider:

- Why is it hard to spot Trusted Malicious Insiders?
  - Can insert code in systems
    - Code insertion is a normal activity of trusted users
    - How do you distinguish normal from abnormal?
  - Can override system controls designed to detect/deter such activity
    - Manual override is a normal activity of trusted users
    - How do you distinguish normal from abnormal?

Why do you care about data exfiltration?

Cost

- Liability
- Loss of R&D investments
- Loss of competitive advantages
- Brand degradation

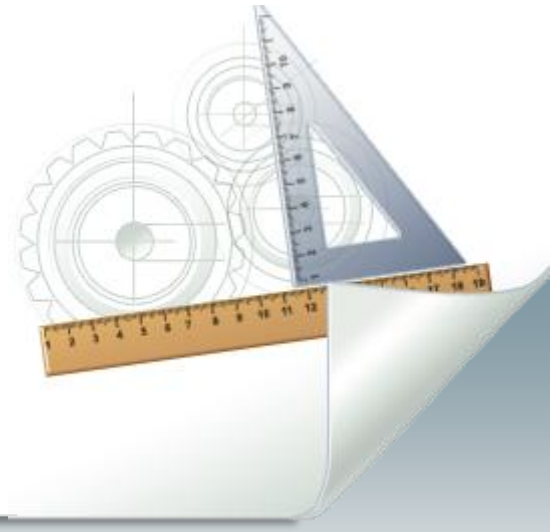
INSIDER THREAT INSIDER THREAT INSIDER THREAT

What can be done about the threat?

- Employee Monitoring is **one way** to mitigate threat
  - A lot of Data Exfiltration is due to honest people cutting corners due to schedule pressure, lack of familiarity with “new” security procedures (especially encryption), avoiding inconvenience, etc.
  - Monitoring can be a critical component to policy enforcement
    - What good are speed limit signs if no one gets a ticket?
  - For Malicious Trusted User threat, Monitoring can
    - Alert on suspicious outbound traffic
    - Perform Continuous logging
    - Attribute individual actions of privileged users “on the HR radar”
    - Confirm failed physical access attempts

Food for thought: If you were designing it, what would be design considerations?

- Policy violations?
  - Will it catch “Proprietary” marking as well as “Proietary”?
- Threat triggers?
  - We happen to really care about APT activity
  - Agent tamper is a must
- Network connectivity reliance?
- Susceptibility to false positives?



Policy Violations

Threat Triggers

Network Connectivity

System Integrity

Enterprise Scale Employee Monitoring

General Considerations

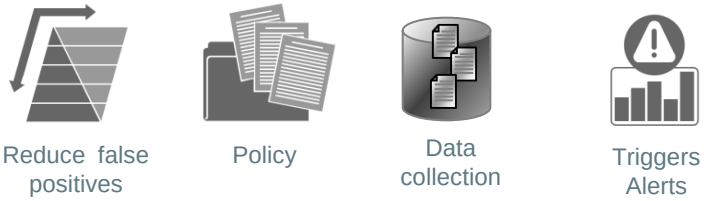
Employee Monitoring considerations

- **Step 1: Identify Assets at Risk**
  - **Banking and credit companies**: Identity theft, account skimming, funds diversion
  - **Financial firms**: Mergers and acquisition plans, non-public financial information, private research
  - **Retail organizations**: Pricing information, personal information on credit card holders, CCVs on cards.
  - **Public companies**: Earnings information not yet distributed to the market, new product information before release, intellectual property.
  - **The government**: National secrets, classified and personal

  - Yes, this is a repeat from a previous slide

Employee Monitoring considerations

- Think through and anticipate “Typical” investigations
- Intent is to
  - reduce false positives
  - create good policy
  - allow better data collection for timeline recreation
  - determine appropriate triggers and alerts



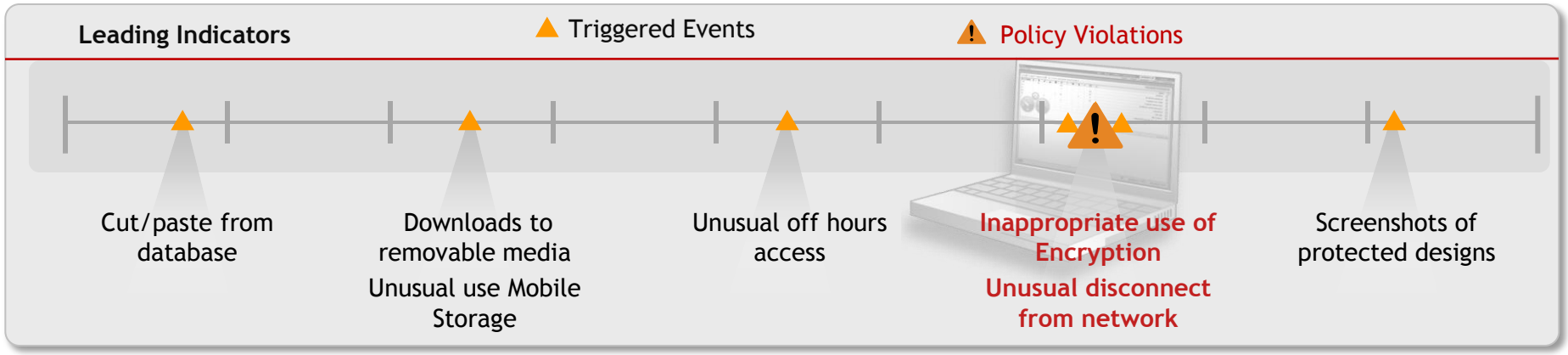
Let’s see how this works …

Employee Monitoring considerations

- Typical Customer data or IP loss investigations involve:
  - Thefts of customer lists or data for financial gain
  - Leaks of IP or customer data for revenge
  - Unintentional leaks (e.g., laptop theft)
- So to assist in those investigations:
  - Capturing certain activities (historical leading indicators) would give potential early warning of data loss, fraud activity
  - That “leading indicator event capture” is a focus of employee monitoring

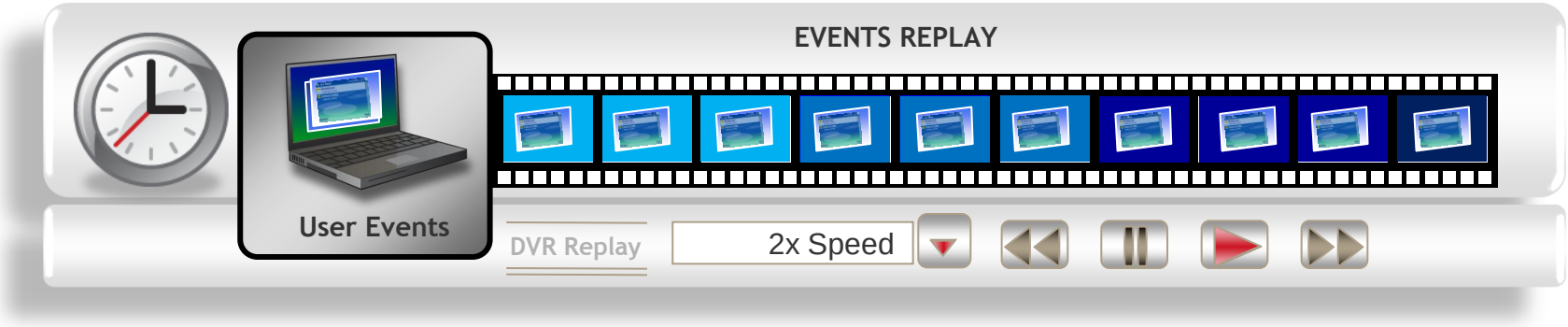
Log leading indicators (potential triggers)

- **IP/Customer Data Loss countermeasures**
  - Cut/paste from databases
  - Downloads to removable media (CD, USB drive, etc)
  - Unusual off hours access
  - Unusual mobile storage use (e.g., Gigs, not MBs)
  - Screenshots (e.g., from Sensitive drawings)
- **Fraud countermeasures**
  - Manual disconnects from the network
  - Inappropriate/unusual use of encryption



Log leading indicators (potential triggers)

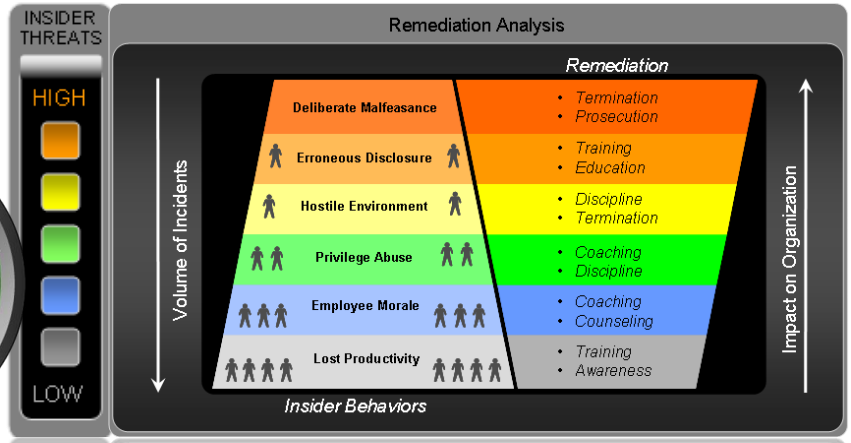
- Compliance investigations
  - The reverse of a loss investigation: rather than logging policy violations, you benefit from logging compliance events
  - Time stamp or video replay shows proper sequence followed



Employee Monitoring considerations

- Create Profile(s), those most likely to put assets at risk,
  - Employees who have resigned or about to resign
  - Contractors, outsourced call or service center employees
  - Former employees given access for any reason
  - Technically sophisticated users
  - Employees w/privileged access, e.g. sysadmins
- Employees on HR radar should be subject to stricter policies.
- Leading indicators:
  - Conflicts with coworkers (especially angry/violent)
  - Sudden performance drops
  - Unusual tardiness, absenteeism

HR RADAR



"Past performance is no guarantee of future results …. But it's all you have to go on"

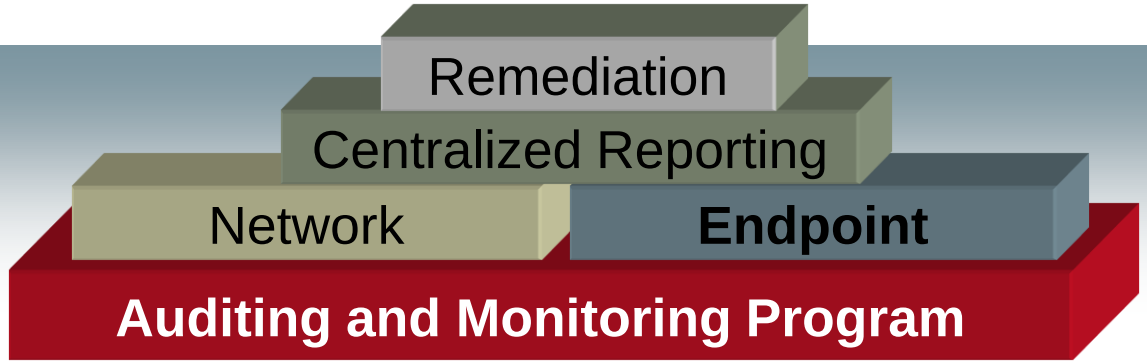
Raytheon

- 2009 Carnegie Melon data on malicious insiders:
  - 50% of insiders who stole for financial gain were recruited by outsiders
  - 50% were disgruntled; most of the disgruntled were motivated by revenge
  - Only 30%% used their personal account for the attack; 34% used a shared account (including sysadmin and DBA accounts)
  - Most used remote access for the attack
  - Most attacked during off hours
- On the other hand:
  - 80% were male; but 75% of IT and math field is male.
    - My conclusion: don't just focus on males
- (Source: http://www.cert.org/archive/pdf/CSG-V3.pdf)

Raytheon

Employee Monitoring considerations

- **Three typical Foundation Components for Investigations:**
  - **Endpoint device monitoring**
    - **Need: something that profiles normal behavior; look for abnormal patterns**
    - **A monitoring solution that does not require network connection is better than one that does.**
  - **Network device monitoring**
    - **Traffic analysis looking for abnormal patterns**
  - **Enterprise reporting=Centralized reporting**



Deciding Where, What, and Whom to Monitor

Raytheon

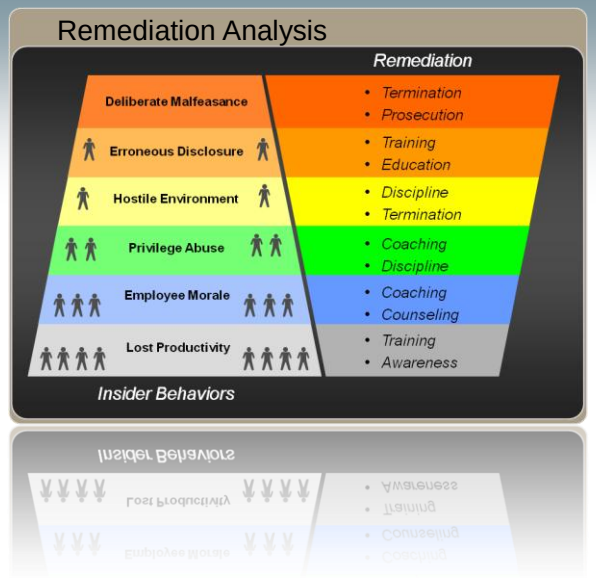
- **Assets, IP can/should be prioritized**
- **USB/mobile storage use profiling** (possibly focused on certain employee segments, e.g., Engineering)
- **Outsourced call center representatives**
  - Defcon 18 Capture The Flag event:
    - "Very often, call center employees are overlooked in various employee awareness programs. However, this weak link, at least in the context of this contest, led to the vast majority of the captured flags."
- **SysAdmins/DBAs**
  - high levels of non-business related activities (a leading indicator of job discontent).

Employee Monitoring considerations

- Disclosure decision
  - A. Inform employees, deter bad behaviors
  - B. Don't inform Employees
  - C. Do whatever is mandated by Law

- My personal $0.02 (which I'll repeat):
  - Inform employees that monitoring is going on
  - Don't disclose details like specific triggers
    - Except one: if there is a specific agent visible to the user, inform the user that it is an offense to tamper with the agent
    - Like on airplanes: you are told not too muck w/smoke detector
  - Periodically and broadly report the types of violations found

Employee Monitoring Considerations



Analyze/measure vulnerabilities and areas of concern, leading indicators

- **Analyze/measure vulnerabilities and areas of concern, leading indicators, and get an as-is profile**
  - Unusual network traffic spikes (off-hours, unusual protocols, non-business applications such as webmail, etc.)
  - Traffic going to unauthorized geographic destinations (e.g., FTP site in <unexpected country>)
  - Unauthorized or harmful content (hate sites, pornography, job search sites) that indicate low productivity, job discontent and potential legal liabilities
  - High volumes of unexpected USB/mobile storage use
  - Inappropriate use of encryption
  - Unusual offline activities
  - High printing volumes off-hours

Employee Monitoring Considerations

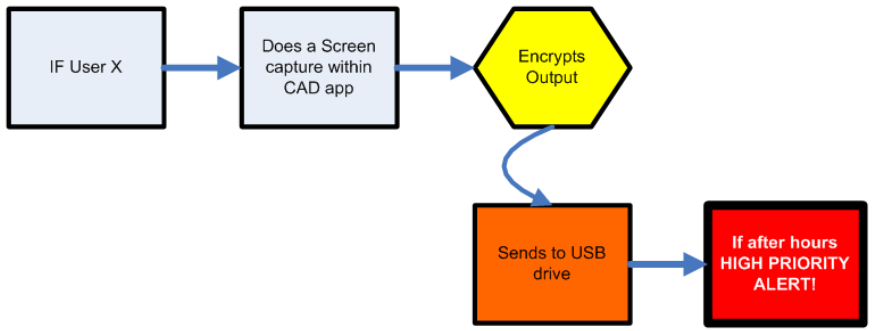
Avoids false positives

Positive behaviors

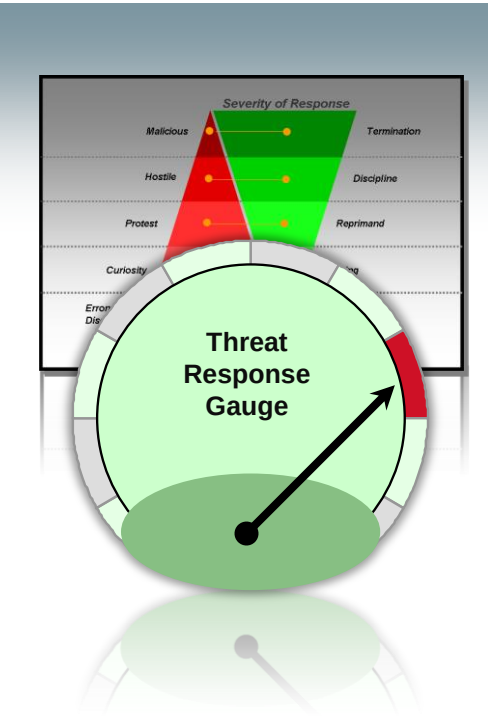
Prompts users

Prevent unwanted behaviors

- Create automated processes to investigate and remediate non-critical violations with automatic or guided course correction
  - Avoids false positive inundation
  - Enforces positive behavior change
  - Confirms that yes, “somebody’s watching”
  - Stop some behaviors automatically
    - “We stopped your unencrypted outbound email; please encrypt and resend”



Employee Monitoring Considerations



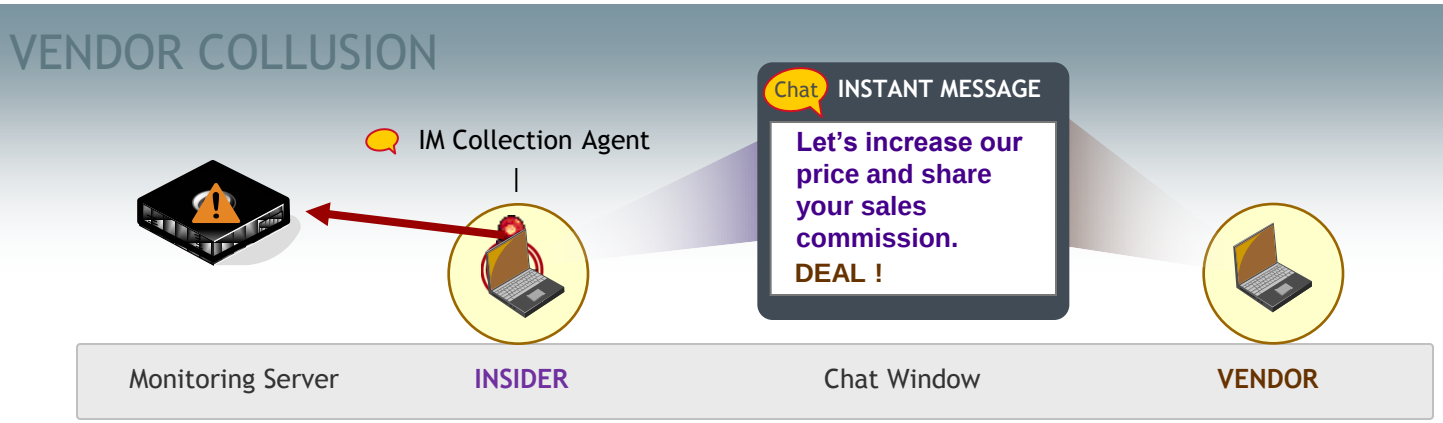
- Identify incidents for investigation (i.e., what makes an incident “investigation worthy”?)
  - E.g., Copies to USB portable drive
    - 2 documents within 5 minutes, normal business hours: probably benign
    - 20 docs within 10 minutes, during off hours or via remote access: probably not benign?
    - 20 docs within 10 minutes, during off hours or via remote access, by an employee who has given notice: investigation worthy
  - IMs from Security office to employee under active investigation: *very* odd
- But only you know what makes sense in your world

Employee Monitoring considerations

- Resource commitment
  - My company has internal investigation folks; do you?
  - Employee monitoring requires that infrastructure, in one form or another (in-house or outsource)
  - Prosecutions require proper chain of custody handling, etc.

Employee Monitoring Considerations

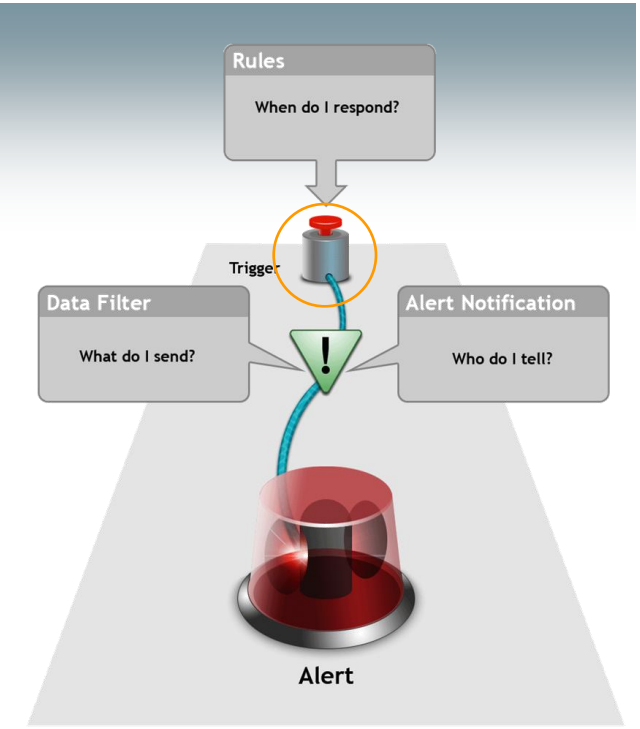
- **Incident logs and historical user activity**
  - The best leading indicator of bad behavior is other bad behavior
  - E.g.: an encryption history log might show files encrypted with innocuous non-business names like “Vacation Photos”
  - The policy violation trigger (e.g., email to unfamiliar domain) is likely preceded by leading indicators, e.g.:
    - Visits to competitor job sites
    - Collusion with peers



Employee Monitoring Considerations

- **Can you Evaluate Incidents in Full Context?**
  - Visual replay of an incident can confirm an incident better than correlation of discrete log events
  - Often, non technical people must evaluate evidence (e.g., management, juries, etc)
  - Replay can also exonerate clearly accidental behaviors

Employee Monitoring considerations



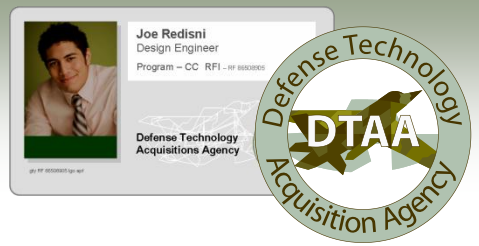
? > = <

- Isolate/Refine True "Trigger" Events That Lead to This Behavior
  - Analysis of a sequence of events may show that an earlier event is a better indicator of actionable behavior
  - Any infrastructure must deal with removing the noise – false positives – from actionable events
- Recycle Lessons Learned Back "Upstream" into Enterprise Monitoring
  - Don't be surprised if "version 1.0" of your trigger set has an unmanageable volume of false positives

Enterprise Scale Employee Monitoring

My Employee Monitoring Deployment Experience

Sensitive Data Violation



Problem

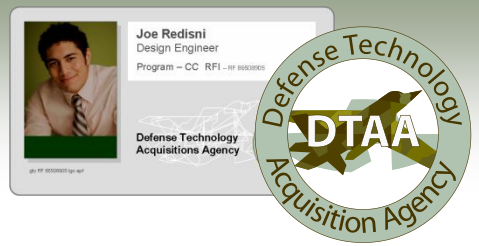
Joe Redisni, Design Engineer has sent sensitive Information outside the organization.

Raytheon Solution

- **SureView monitors sensitive documents using "document fingerprinting" policies**
  - fingerprinting is able to detect if sections of text match sections from the protected document
  - SureView policy can be set to alert an investigator if sensitive information is mishandled even if encrypted
- **Even though Joe was "offline" SureView continued to monitor**
- **The Investigator viewed the incident in full context with SureView's DVR-like replay revealing**:
  - Joe tried to hide his actions
  - Joe stole proprietary company information
  - Joe is an insider threat

SureView enables investigators to make quick and accurate assessments of a target's intent.

SureView Use Case



SureView

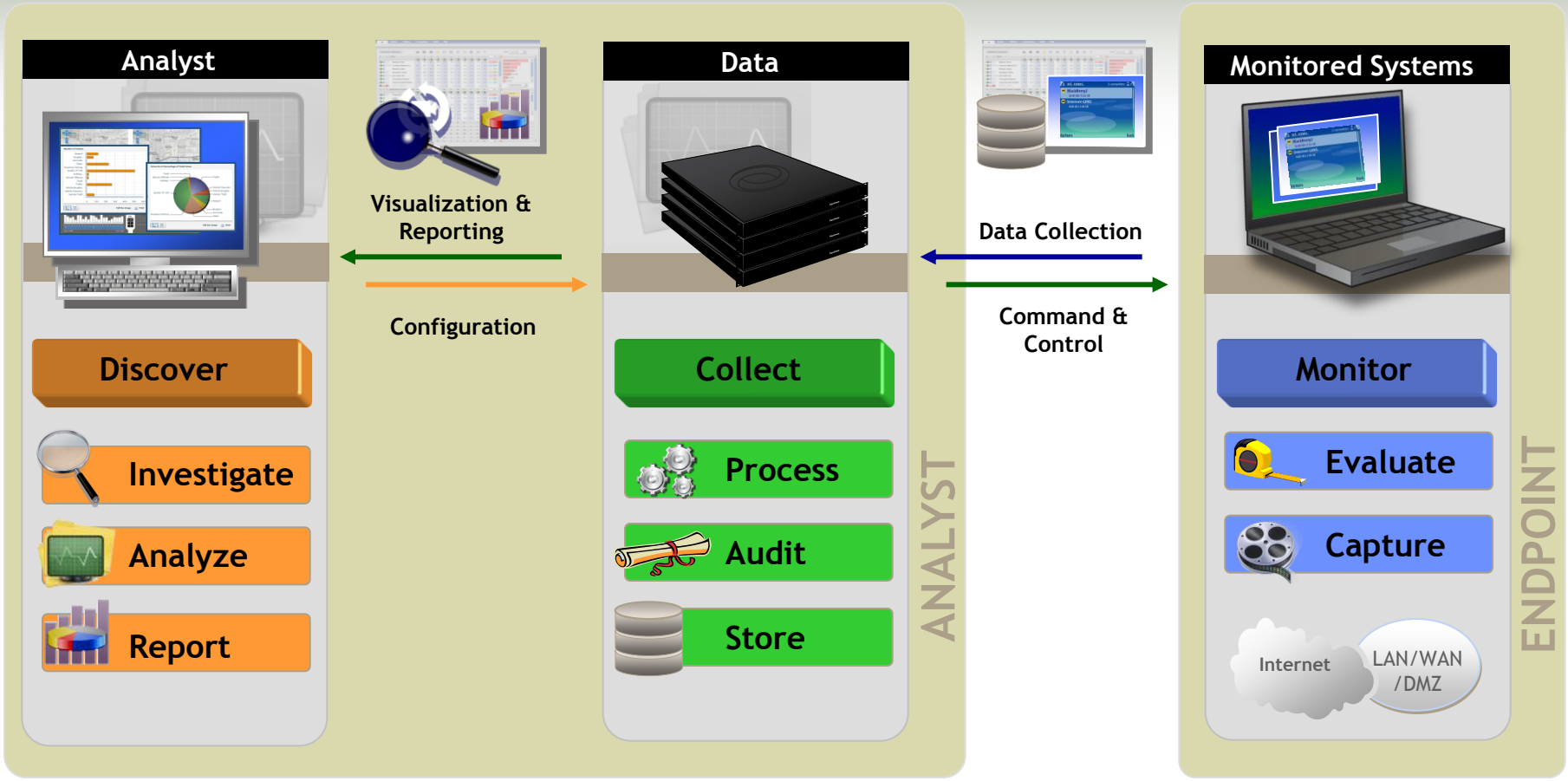
Has detected Joe Redisni, Design Engineer has sent sensitive Information outside the organization.

SureView 6.5 – DTAA demo Protected file attached to Email Example
3:38

Cleared for international release – 2010-052

Enterprise Monitoring Function and Flow

SureView™ Proactive Information Protection



“Eating our own dog food”

If you expect customers to buy your products, you should also be willing to use them

--Paul Maritz, Microsoft

- = When a company uses the products that it makes.
- Demonstrates confidence in its own products
- Popularized (per Wikipedia) in 1988, Microsoft manager Paul Maritz Paul Maritz sent an email titled "Eating our own Dog food” challenging another manager to make greater use of the company’s product
- The idea behind "eating your own dog food" is that if you expect customers to buy your products, you should also be willing to use them
- By God, we were going to do the same

Here's What We Did …

Raytheon
Oakley Systems

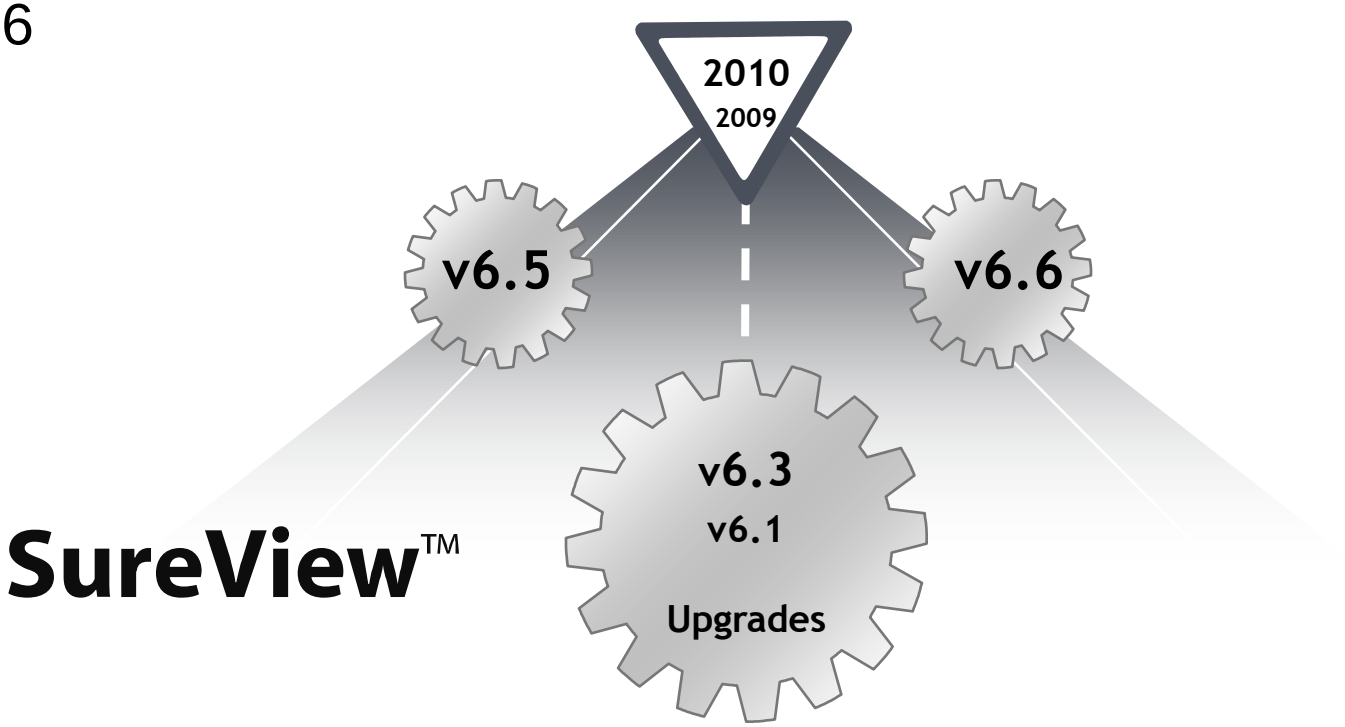
Diverse Customer Base

SureView™
V6 Solutions

- Timeline Overview:
  - This talk is about my experience with SureView
  - SureView is made by Raytheon Oakley Systems
  - Raytheon acquired Oakley in October 2007
  - Beta tested on Corporate IT users in 2008
  - Enterprise deployment in 2009/2010
  - Development based on feedback in 2010
  - Early adopter Version Upgrade in Q3 2010
  - Planned Enterprise Version Upgrade in Q1 2011

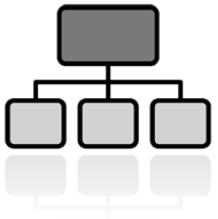
Deployment Timeline Details

- Late 2008 : Early adopters from Corporate IT, version 6.1
- 2009: First full scale deployment of version 6.3 to all US based unclassified network machines
- 2010 (ongoing) : first full scale upgrade of version 6.3 to 6.5 or 6.6



Scale of the task

- User monitoring applications are intrusive, by definition
- They are comparable to AntiVirus apps or Firewalls
- They may examine:
  - Every process
  - Every file opened or closed
  - Network sockets
  - Etc.
- What happens when your process spins off dozens of child processes (e.g., Compilers)?
- High file I/O in brief time? (I'm looking at you Pro/E)



Scale of the task: Applications

The Department of Defense and the IC trust Raytheon personnel their most sensitive information – we are making these same cleared, vetted resources, available to commercial enterprise customers – who better to handle your sensitive operational and security data

- We are an Engineering company: 40K of the employees are engineers (as of 2010)
- Yeah, Finance has wonky applications but *nothing* compares to Engineering
  - Thousands of standard applications
  - Thousands of not-so-standard applications
  - And I'm just talking about Windows based apps (as of 2010 …..) that will be analyzed by SureView

Scale of the Task: Encryption Infrastructure

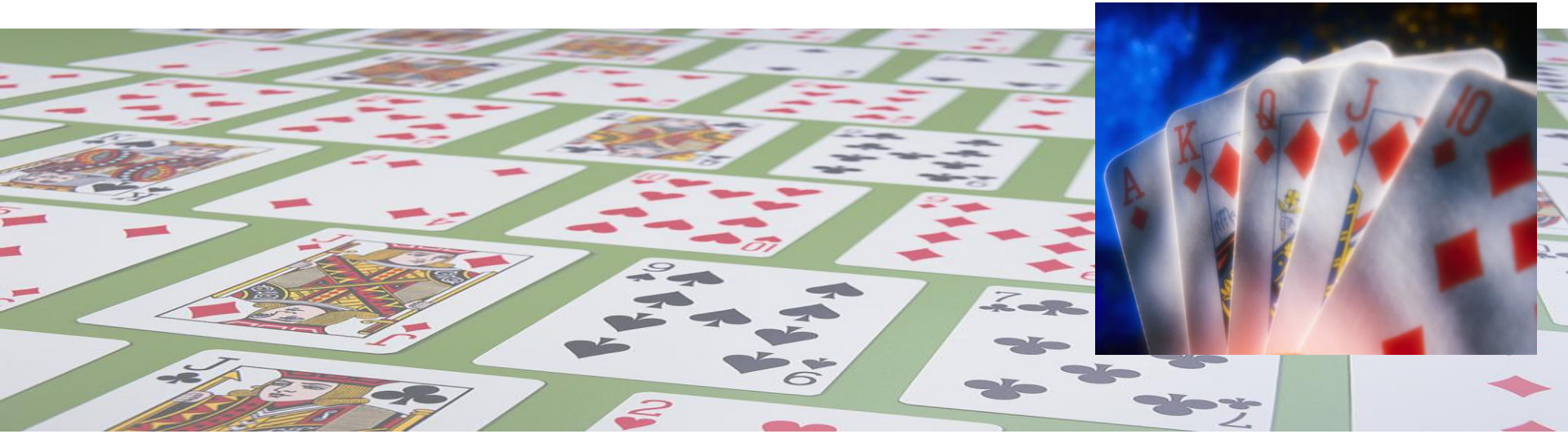
Raytheon

- We have an enterprise PGP encryption solution in place
- SureView has to detect when encryption is properly used
  - Hardware encrypted thumb drives
  - Generic thumb drives encrypted with our PGP is O.K.

Raytheon

Cards We Were Dealt:

- Get some early adopters in non-IT areas, but don't tell them what we were doing (blind testing)
- Draw up a schedule for full deployment before the early adopter tests were concluded
- Pressure to adhere to schedule
- No separate funding for labor for the non-IT people



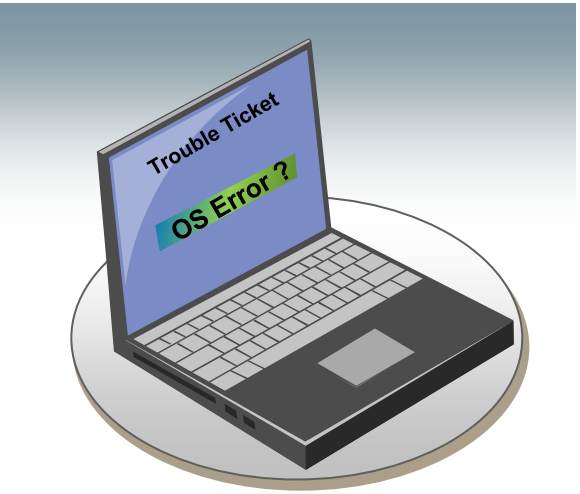
Early lessons learned

- "Get some early adopters in non-IT areas, but don't tell them what we are doing (blind testing)": Personal Opinion - this was the worst mistake we made.
  - Engineers are smart people. They quickly located the new "DLP.exe" process on the their machine.

  - Story break: my buddy Brian …
  - Word spread quickly.
  - Uninstall, whitelist, reinstall …

- Good news is that SureView can be set to run "quieter" than nearly any other process running at the endpoint

Dealing with problem applications



Many users assume monitoring software causes performance issues…

…claim performance hits even when its not actually installed

- Log problems (visible to all project support folks)
  - We kept an issues database (eRoom) so that others could see first appearance of the problem, progress, correlations, etc.
- Confirm SureView was actually installed
  - Many cases of users blaming SureView for performance hits when it was not actually installed
- Usual approach was to whitelist the app, then do deeper debug
- Some problems were *really* obscure
  - A lockup only occurred when Vista users enabled Aero theme

Dealing with Problem Applications

- A-B-A test used religiously:
  - A: Observe and confirm the problem **state**
  - **B: Disable SureView**
    - **Observe and confirm the problem state disappears**
  - **A: Re-enable SureView**
    - **Observe and confirm the problem state returns**
  - If all three observations existed, we declared it a SureView problem
- Some problems could be dealt with by simply changing desktop agent's tunable parameters
- Some problems could only be mitigated via whitelist

Reports

- Initial state: reporting was manual labor intensive
- Linux to the rescue. We were able to automate parsing of Excel derived analysis results, to produce formal emails.
- Decision: do you send to the employee with the violation, their manager, or both
  - Concrete not set on this decision, in our case
- Situational Awareness report example::
  - “DLP reported xxx new alerts in SureView resulting in yyy confirmed policy violations. These events were logged, filed, and reported to ……”

Enterprise Scale Employee Monitoring

Final thoughts

Lessons learned: The Bad

- Hiding the original deployment was **extremely** counterproductive. **Don't hide it**.
  - Caused wild goose chases when applications suddenly developed intermittent failures
  - Angered early adopter engineers once news of the deployment was disclosed
- At one point, our ability to uninstall was removed due to perceived misuse of uninstall capability
  - Not being able to uninstall deters current/future testers
  - Volunteers really want assurance that you can do something about a problem "Right Freakin' Now™"
  - Compromise was struck by reducing number of people who received uninstall capability

Lessons Learned: The Good

- Performance throttling put into the version 6.5 desktop agent **dramatically** reduced performance issues
  - In considering any monitoring solution on the market, you should ask if the agent has any built in self-limiting triggers to prevent resource exhaustion and promote future optimization (Hmm, could apply to A/V too …)
- A-B-A testing was a solid methodology, easily understood, perceived as fair
- Stop/Start/Uninstall executables were password protected and expired after a while
  - Prevented misuse and avoiding an install
- Automated reporting processes were important
  - Underestimated the need; they really reduced manual processes

Is it Legal?

- You are virtually guaranteed to get this question
- Important: your peers and your boss (and their boss) are unqualified to answer it
- If you have any doubts, consult legal staff
- It took me 3 months to get an answer from legal:
  - "case law in this area of the law is very sparse"
  - "I am comfortable that the planned use of Sureview (as well as keystroke logging) are currently legal" in relevant jurisdictions
- The answer above works for me but is not transferrable. Only you can get a valid answer for your jurisdiction

Enterprise Scale Employee Monitoring

Thanks

- Reviewers (Carolyn, Alan, Jeffrey @Oakley)
- Senior management consultations
- Formal Approvers (all 4)
- Da Boss, for sending me here
- Coworkers who helped deploy
- Engineers for their patience

Enterprise Scale Employee Monitoring

Questions?