Data Privacy and the Insider Threat

John Crossno
Compuware Corp

November 2018
Session FC

Abstract

- Data privacy and the insider threat are closely connected. So closely that it’s difficult to talk about one without addressing the other, and it’s difficult to effectively address them separately from an overall security perspective.
- This session will discuss the two in that light, and the importance of not trying to address the security aspects of data privacy, without also bringing the protections offered by securing against the insider threat into the discussion.

The Problem

Growing Cybersecurity Risks

- Breaches are increasing:
  - 5% increase between 2014 and 2015
  - 2016: 4B records stolen; >2x 2014 + 2015 combined[1]
  - 2017: 6.7% increase
- Takes too long to find breaches:
  - Global average time to detection = 146 days[2] (469 days for EMEA)

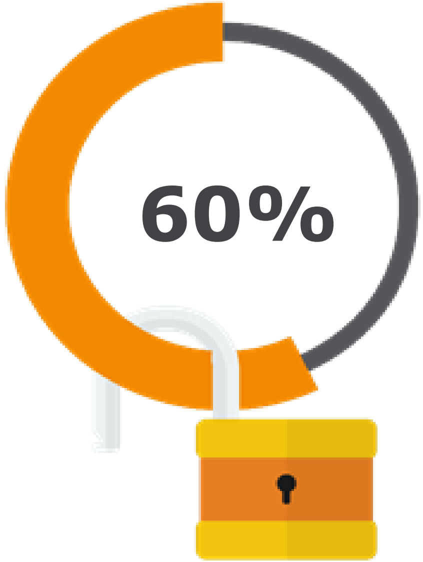
Increasing Compliance Mandates

- Risk non-compliance with regulations (e.g. GDPR) and industry mandates
  - Mechanisms to control, monitor and report access
  - Automated detection of breaches
  - Notifying those affected if breach occurs

[1] IBM X-Force® Research: 2016 & 2017 Data Breach Review

[2] FireEye Releases First Mandiant M-Trends EMEA Report

Cybersecurity Cost



of attacks are by **insiders**[1]

Average cost of breach is **$3.86M** per case[2]

Mega Breaches

$40M to $350M

Where 1M to 50M records are lost

1/3 of this cost: lost business

When uncovered by **active detection** (ex: monitoring), median loss and duration were **lower**[3]

[1] IBM X-Force® Research: 2017 Cyber Security Intelligence Index

[2] 2018 Cost of a Data Breach Study by Ponemon

[3] Association of Certified Fraud Examiners, 2016 Report on Occupational Fraud and Abuse

Additional Statistics

- 88 percent of end users say their job requires them to access and use proprietary information - *Varonis 2016 Study of US & European Organizations*
  - 62 percent say they have access to company data they probably shouldn't see
- 75% of incidents go unreported – *Carnegie Mellon US Cert*
- $500,000 is the cost that 75% of companies estimate to remediate an insider breach – *2016 Insider Threat Spotlight report*
- 2/3 of insider incidents are due to employee negligence – *2016 Ponemon Institute Survey*
- 56% of employees believe it's OK to take information with them when they leave a job – *Symantec*
- Trade Secrets Global Annual Impact Loss > $2.2T – *PwC 2016 Survey*
- 91% of hacking attacks begin with a phishing email - *Wired Magazine*

The Problem

- Most sensitive data and business-critical systems sit on mainframe
- Mainframe is **inherently highly secure and the most securable platform, but …**

– **Security teams lack visibility into application user behavior**

- Users with access
- Users with unauthorized access

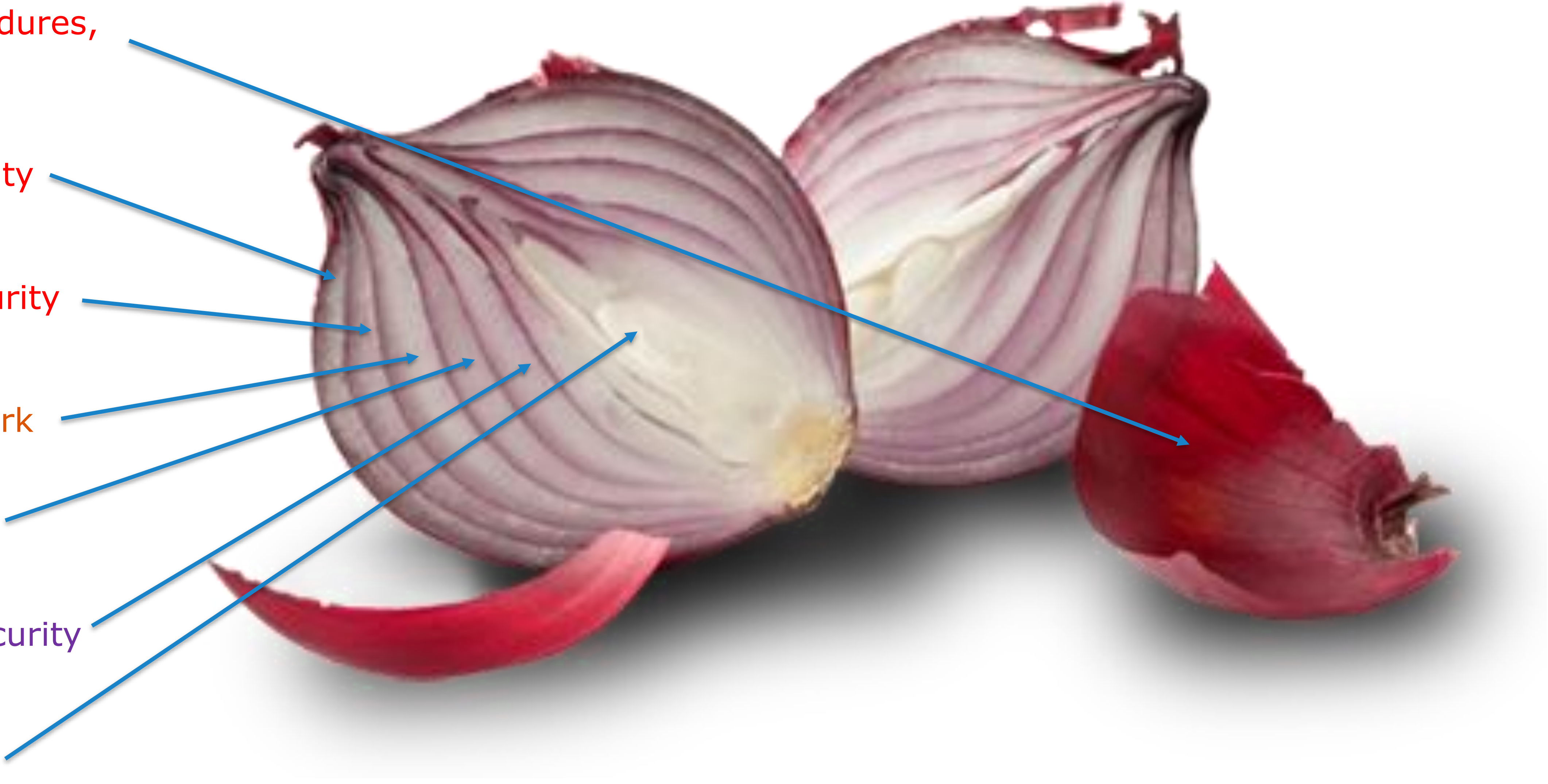
– **Security teams are reliant on insiders or outsourcers that may be ones committing crime**

Note: All systems have this problem!

Current Practices

- SMF data
- Scans of disparate logs
- SIEM tools
- RACF, CA ACF2, CA Top Secret

Peeling Back The Layers Of Security



Policies, procedures, awareness

Physical Security

Perimeter Security

Internal Network

Host Security

Application Security

Data Security

Insider Threat

Insider

Any individual who has valid credentials to access internal resources

Insider Threat

Individual who uses authorized access to negatively impact system integrity or confidentiality of intellectual property or data

Who may pose insider threat?

Types of Insider Threat Actors

Malicious

Negligent

Inadvertent

Characteristics of Potential “At Risk” Insider

Malicious or Negligent

- Self-entitlement
- Debilitating introversion
- Intolerant of criticism
- Lack of empathy
- Passive aggressive
- Ethical flexibility
- Greed or financial distress
- Susceptibility to blackmail
- Extreme compulsiveness

Characteristics of Potential “At Risk” Insider

Inadvertent

- Unwitting
- Careless
- Unawareness
- Inattention
- Needs training

Examples of “Insider” Breaches

U.K. Bank

Privileged user accesses bank app to transfer funds into dummy accounts also set up through standard banking apps

European Credit Card Processor

Contracted SysProg accesses apps to monitor and report/sell geography info for particular credit card usage

U.S. Healthcare Provider

Stolen credentials used to breach mainframe sensitive data

U.S. Government Agency

Hackers steal credentials later used to access mainframe data

Equifax

Last but not least

And on and on …

What Do Companies Stand to Lose?

- Forfeiture of revenue
- Remediation expenditures
- Diminished market share
- Business disruption
- Collateral security risks
- Compromised intellectual property
- Legal and Regulatory repercussions
  (GDPR, HIPAA, NDB, PCI DSS, California, NY, Corp Policies, etc.)
- Degraded brand reputation
  - "It takes 20 years to build a reputation, and five minutes to ruin it."
    – Warren Buffet

Be Offensive!

"The best defense is a good offense." — Vince Lombardi

- Today's threats are ever evolving, But one constant is the human element as a primary threat vector.
- Get ahead of a potential incident by identifying human threat indicators
- Can't just monitor network/database activity and block when something doesn't look right.
- Don't ignore analysis – Connect the dots – User behavior analytics

Data must be analyzed, or why bother collecting it?

How Does This Relate to Data Privacy?

Data Privacy and Compliance

The “Insider Threat” is after the Sensitive Data!

- Data has to be secured and protected
- $$ Money is the primary driver

Compliance

- GDPR/NDB
- HIPAA
- Corporate policies
- Others

Top 5 Information Security Pain Points

1. User behavior – 29%
2. Compliance-related costs/requirements – 21%
3. Staffing information security – 20%
4. Cloud security – 19%
5. Lack of budget – 18%

Top 5 Information Security Projects, 12 months

1. Regulatory Compliance – 35%
2. Security awareness initiatives – 19%
3. Cloud infrastructure security – 18%
4. SIEM/Security analytics – 17%
5. Vulnerability assessment – 16%

451 Research, Information Security, Workloads and Key Projects 2018

How Security Helps with Compliance

Mechanisms to control and monitor access

- Control = access authorizations
- Monitor = Knowing who accesses what
  - Level of granularity plays a critical role

Automated detection of breaches

- What is a “Breach”?

Data for notifying those affected if breach occurs

- What was seen?
- When was it seen?
- How often was it seen?
- What was done with it?

Employee Privacy and Monitoring

- The downside of monitoring users

- How do employees feel about being monitored?
  - Is “Big Brother” really watching?

- The value of monitoring users
  - Improved breach detection
  - User Behavior Analytics
  - Prevention of “negligent” behavior
  - Protection of sensitive data
  - **Protection for the employee**
- **Education is needed!**

The Importance of Test Data Privacy

Is production data the best for dev/test/QA?

- Does it provide for better testing?
- How do you protect it?
- How do you know when it’s been “breached”?
- How do you comply with regulatory mandates?
- How does it complicate matters?

What changes if production data is privatized?

- No need for the same protection as production
- Are concerns about it being breached the same?
- Are regulatory mandates still in play?
- Limited exposure!

Limiting the Exposure to Sensitive Data

Growing Cybersecurity Risks

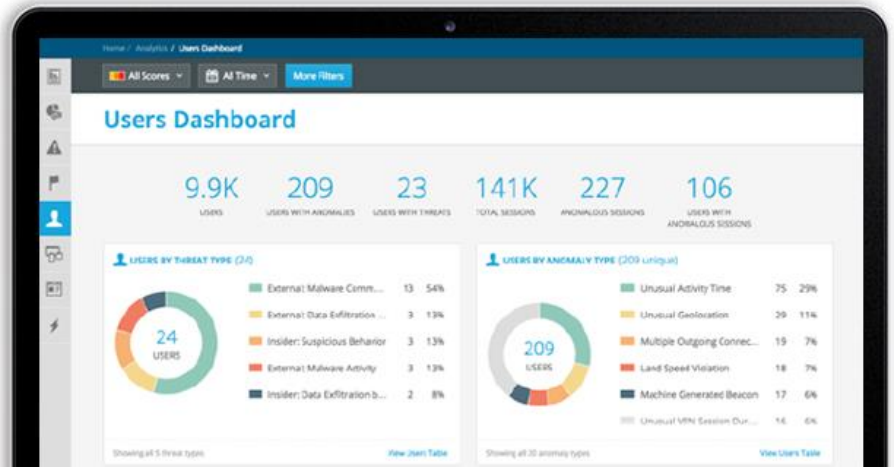
- Gain insight to address the increasing breaches, by insider threat actors
- Reduce the time it takes to detect breaches

Increasing Compliance Mandates

- Helps address the risks of non-compliance with regulations (e.g. GDPR) and industry mandates
  - Mechanisms to control, monitor and report access
  - Automated detection of breaches
  - Notifying those affected if breach occurs

“Never, never, never give up” – Winston Churchill

Focus On The Insider Threat



Home / Analytics / Users Dashboard

All Scores ⌄ | All Time ⌄ | More Filters

Users Dashboard

9.9K	209	23	141K	227	106
USERS	USERS WITH ANOMALIES	USERS WITH THREATS	TOTAL SESSIONS	ANOMALOUS SESSIONS	USERS WITH ANOMALOUS SESSIONS

USERS BY THREAT TYPE (24)

24 USERS

External: Malware Comm...	13	54%
External: Data Exfiltration ...	3	13%
Insider: Suspicious Behavior	3	13%
External: Malware Activity	3	13%
Insider: Data Exfiltration b...	2	8%

Showing all 5 threat types — View Users Table

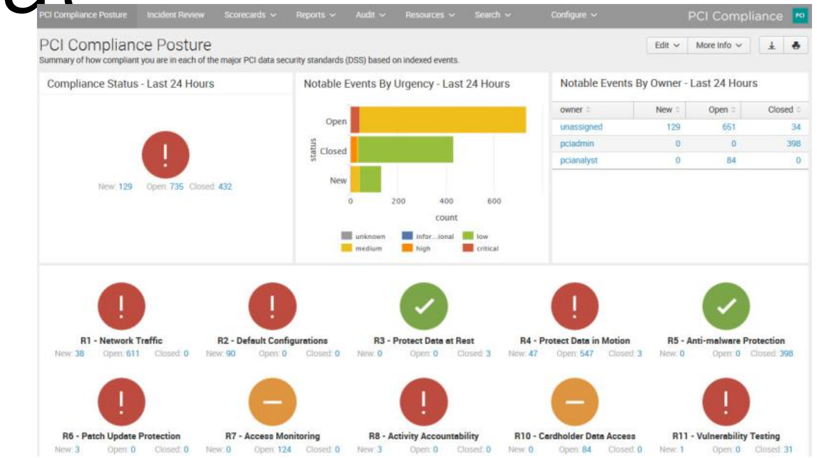
USERS BY ANOMALY TYPE (209 unique)

209 USERS

Unusual Activity Time	75	29%
Unusual Geolocation	29	11%
Multiple Outgoing Connec...	19	7%
Land Speed Violation	18	7%
Machine Generated Beacon	17	6%
Unusual VPN Session Dur...	16	6%

Showing all 30 anomaly types — View Users Table

Compliance



PCI Compliance Posture | Incident Review | Scorecards ⌄ | Reports ⌄ | Audit ⌄ | Resources ⌄ | Search ⌄ | Configure ⌄ | PCI Compliance

PCI Compliance Posture

Edit ⌄ | More Info ⌄

Summary of how compliant you are in each of the major PCI data security standards (DSS) based on indexed events.

Compliance Status - Last 24 Hours

New: 129 Open: 735 Closed: 432

Notable Events By Urgency - Last 24 Hours

Notable Events By Owner - Last 24 Hours

owner	New	Open	Closed
unassigned	129	651	34
pciadmin	0	0	398
pcianalyst	0	84	0

R1 - Network Traffic — New: 38 Open: 611 Closed: 0

R2 - Default Configurations — New: 90 Open: 0 Closed: 0

R3 - Protect Data at Rest — New: 0 Open: 0 Closed: 3

R4 - Protect Data in Motion — New: 47 Open: 547 Closed: 3

R5 - Anti-malware Protection — New: 0 Open: 0 Closed: 398

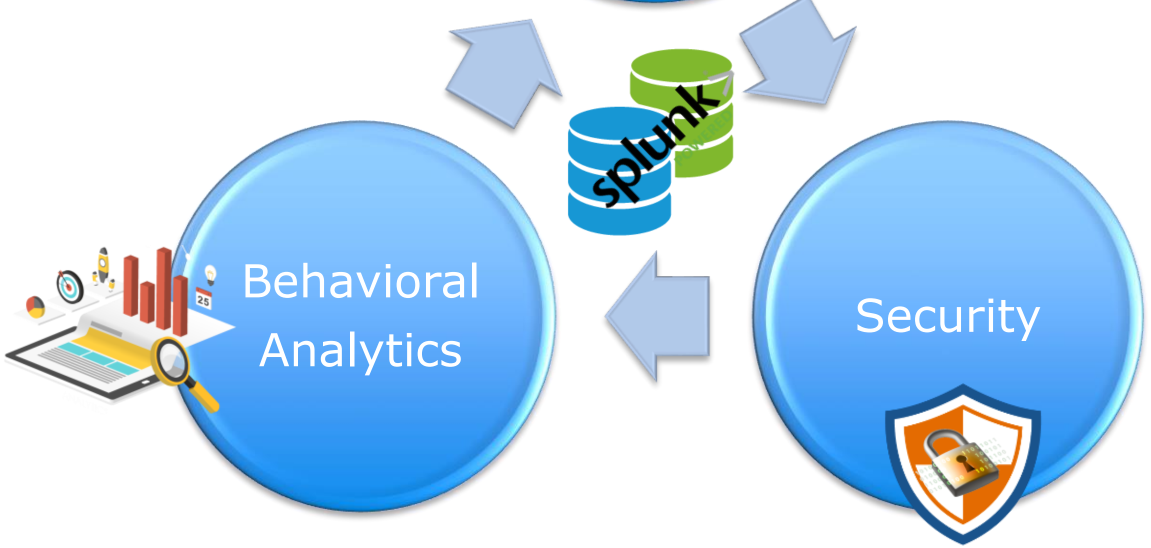
R6 - Patch Update Protection — New: 3 Open: 0 Closed: 0

R7 - Access Monitoring — New: 0 Open: 124 Closed: 0

R8 - Activity Accountability — New: 3 Open: 0 Closed: 0

R10 - Cardholder Data Access — New: 0 Open: 84 Closed: 0

R11 - Vulnerability Testing — New: 1 Open: 0 Closed: 31



Splunk App for Enterprise Security

Pre-built searches, alerts, reports, dashboards, incident workflow, and threat intelligence feeds

Dashboards & Reports

Incident Investigations and Management

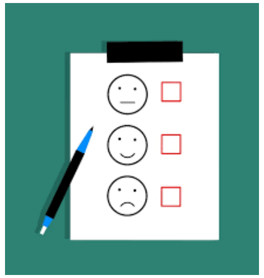
Statistical Outliers & Risk Scoring

Asset & Identity Aware

splunk>live!

We want your feedback!

- Please submit your feedback online at ….
  - ➢ http://conferences.gse.org.uk/2018/feedback/fc
- Paper feedback forms are also available from the Chair person
- This session is FC



THANK YOU!

Session FC

Johnathan Crossno
Principal Product Manager

+1 313 227 7775
john.crossno@compuware.com
linkedin.com/in/johncrossno
@john_crossno

One Campus Martius, Detroit, MI 48226, USA **www.compuware.com**

➢ http://conferences.gse.org.uk/2018/feedback/fc