Leveraging Behavior Analytics for Data Centric Audit & Protection (DCAP)

Brian Anderson - Principal Security Engineer, Strategic Accounts
March 2018
Behavior Analytics for DCAP

- Introduction
- State of data security
- *Gartner* Data Centric Audit & Protection (DCAP)
- Insider threats in Government
- Insider threat profiles
- Leveraging behavior analytics
- Q&A
Introduction

Brian Anderson

• Principal Security Engineer, Strategic Accounts
• 6 years at Imperva
• Email: ba@imperva.com
• Home: San Diego, California
Cybercrime Monetizes on DATA
More Data in More Places

Structured

Unstructured

Big Data

SaaS

- ORACLE
- SQL Server
- MongoDB
- cloudera
- hadoop
- cassandra
- Office 365

- NFS
- Windows Server
- Box
- Slack
- MailChimp
More Apps are Available

Web Apps
Customer portal
Mobile Apps
Web Services or APIs

More Data in More Places

Structured

Unstructured

Big Data

SaaS

© 2018 Imperva, Inc. All rights reserved.
More Apps are Available

Web Apps
Customer portal
Mobile Apps
Web Services or APIs

More Data in More Places

Structured

Unstructured

Big Data

SaaS

More People Can Access It

Knowledge Workers
Customers
Contractors
Privileged Users
More Apps are Available

Web Apps
Customer portal
Mobile Apps
Web Services or APIs

More Data in More Places

Structured

ORACLE

SQL Server

Big Data

NFS

Windows Server

mongoDB

cloudera

Hadoop

cassandra

Unstructured

SaaS

NFS

Windows Server

mongoDB

cloudera

Hadoop

cassandra

WikiLeaks

Office 365

More People Can Access It

Knowledge Workers

Customers

Contractors

Privileged Users

More Bad Actors

DARK WEB

confidential

© 2018 Imperva, Inc. All rights reserved.
CISOs Concerned that breaches go undetected\(^1\) 78%

Organizations Ignore security alerts and can’t keep up with the volume\(^2\) 54%

CISOs #1 concern in 2018\(^3\) “Lack of competent in-house staff” 70%

53% of companies estimate remediation costs of $100,000 and more, with 12% estimating a cost of more than $1 million.

---

1. The Global CISO Study, ServiceNow, July 2017
3. What CISOs Worry About in 2018, Ponemon Institute, January 2018
Profile
• Human Resources department for US Federal Government
• 2 million background checks per year for Secret & Top Secret clearance
• 18 million copies of Federal Security Clearance questionnaires
• Digital fingerprints of all US Federal Employees

Public Data Breach
• As reported in Wired Magazine and Reuters:
  • 2015 data breach of 4.2M personnel files and 5.6M digital fingerprints
  • 10 stolen administrator credentials used to gain access to databases
  • Earliest stolen credential was from a government contractor, who also had a data breach in 2014
  • Breach took over 1 year to detect
  • Anomalous behavior by allegedly authorized users
  • Determined and patient attacker was believed to be a nation-state
BREACHES ARE FOUND AT THE INTERSECTION OF USERS AND DATA
“Employees require access to information assets to perform their jobs, but malicious or ignorant abuse of authorized access is difficult to detect and high-risk.”

GARTNER, BEST PRACTICES FOR MANAGING ‘INSIDER’ SECURITY THREATS, ANDREW WALLS
6 October 2015
“DCAP is a category of products characterized by the ability to centrally manage data security policies and controls across unstructured, semistructured and structured repositories or silos.”

“The exponential growth in data generation and usage across multiple data silos is rendering current data security methods obsolete, requiring significant changes in both architecture and product approaches.”
Traditional security is not enough
Complicated by the move to the Cloud
Data Centric Audit & Protection (DCAP): 5 Data Categories

- **IaaS / PaaS**
  - Unsanctioned
  - Sanctioned
  - Google
  - Box
  - Amazon
  - Azure
  - Etc...

- **SaaS**
  - Unsanctioned
  - Sanctioned
  - Google Apps
  - Workday
  - Salesforce
  - Box
  - Office 365
  - ServiceNow
  - SAP Cloud
  - Etc...

- **Big Data**
  - MongoDB
  - IBM
  - Hortonworks
  - Cloudera
  - Cassandra

- **Databases**
  - Oracle
  - IBM
  - Mainframe
  - DB2
  - Microsoft SQL Server
  - Progress
  - Teradata
  - Netezza
  - DB2
  - Sybase IQ
  - SAP IQ
  - HANA
  - PostgreSQL
  - MySQL

- **Files Shares**
  - SharePoint
  - Network File Sharing

Confidential
DCAP: Protect data where it ‘lives’

External Threats

IaaS / PaaS
- Unsanctioned
  - Google
  - Box
  - Etc...
- Sanctioned
  - Google Apps
  - Workday
  - Salesforce
  - Etc...

Big Data
- MongoDB
- IBM
- Hortonworks
- Cloudera
- Cassandra

Databases
- Oracle
- IBM DB2
- Microsoft SQL Server
- Progress
- Teradata
- Netezza
- SAP HANA
- MySQL
- PostgreSQL

Files Shares
- SharePoint

Internal Threats

SaaS
- Unsanctioned
- Sanctioned

IaaS / PaaS
- Unsanctioned
- Sanctioned

Big Data
- MongoDB
- IBM
- Hortonworks
- Cloudera
- Cassandra

Databases
- Oracle
- IBM DB2
- Microsoft SQL Server
- Progress
- Teradata
- Netezza
- SAP HANA
- MySQL
- PostgreSQL

Files Shares
- SharePoint
Cloud and Hybrid

ON-PREMISE  HYBRID  CLOUD
People are the WEAK LINK
“You can’t patch people...”
Imperva’s internal security “Phishme” training campaign…

On Aug 16, 2016, at 8:27 PM, Drew Schuil <drew@imperva.com> wrote:

Should I click on links that say “deepseaphishing.com” on them, supervisor?

My old boss, Chief Technology Officer…
…security engineer…14 yrs at Imperva

Dude. This is so nailed me. I was in a massive hurry to get flights changed from tomorrow putting kids to bed and rearranging kid coverage due to my schedule change then I see this message that my email won’t work if I don’t do it. 🙄!
59% of exiting employees admit to stealing data.¹

Source 1 - Ponemon Institute Survey
A More Likely Threat

• Every organization has their own… “Dave”
Challenges detecting Insider threats…
Insider and Privilege Misuse

Key Finding:
“When the threat actor is already inside your defenses, they can be quite a challenge to detect - and most of the incidents are still taking months and years to discover.”

Figure 45: Breach discovery timeline within Insider and Privilege Misuse (n=77)

2017 Verizon Data Breach Investigations Report
3 Insider Threat User Profiles

Compromised

Careless

Malicious
Challenges: Why Detection is so Difficult?

Users have legitimate data access

Near impossible to distinguish good access from bad access

Security teams overloaded with alerts
Factoring in the Unknown

Who is connecting to the database?

How do they connect to the database?

What data are they accessing?

Do their peers access data in the same way?

How much data do they query?

When do they usually work?
The query is each of several DBs:

Standard SQL: CREATE TABLE t2 ( LIKE t1 )

PostgreSQL: CREATE TABLE copytable AS SELECT * FROM viewname WHERE false

DB2: CREATE TABLE t2 LIKE t1 INCLUDING DEFAULTS

MySQL: SELECT * INTO t2 FROM t1 WHERE 1<>1

Oracle: CREATE TABLE t2 AS SELECT * FROM t1 WHERE 1<>1

Who is connecting to the database?

What data are they accessing?

How much data do they query?
# Use Cases

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Service Account Abuse</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Suspicious Application Data Abuse</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Machine Takeover</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Excessive Database or File Access</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Suspicious Dynamic SQL Activity</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Data Access Outside of Working Hours</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Excessive Failed Logins by User</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Excessive Failed Logins from App Server</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Suspicious File Access by User</td>
</tr>
</tbody>
</table>
Gartner Mandate:

“Organizations that have not developed data security governance to apply consistent policies and security controls across data silos need to act”

Our Recommendations:

– Build security and compliance into cloud migration
– Invest in post compromise attack detection
– Leverage behavioral analysis
SELECT * FROM QUESTIONS;