Insiders:
The Threat is Already Within

Shiri Margel & Itsik Mantin

June 2016

IMPERVA®

About us

- Shiri Margel
- Data Security Research Team Leader
- M. Sc. in Applied Math and Computer Science from the Weizmann Institute

- Itsik Mantin
- Director of Security Research
- M. Sc. in Applied Math and Computer Science from the Weizmann Institute

IMPERVA®

Agenda

- Introduction
- Behavioral Analysis
- Deception
- Summary

IMPERVA®


People are the
WEAK LINK

Compromised

Careless

Malicious

The Nature of Insider Breach

- Acquire small amount of sensitive information over a long period of time
- Noticed after damaging events
- Almost impossible to prevent

Early Detection

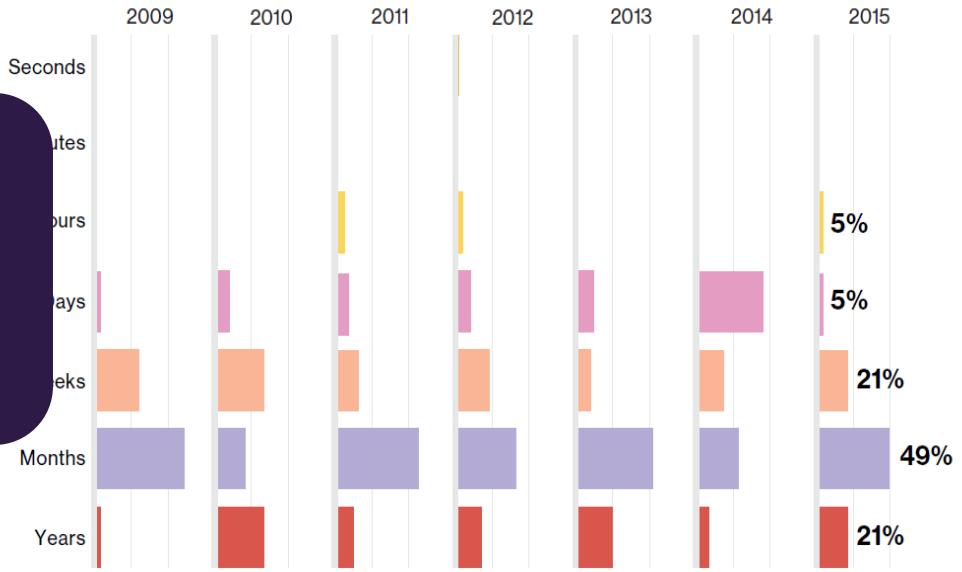


Figure 30.

Discovery timeline within Insider and Privilege Misuse over time, (n=358)

Verizon DBIR 2016

IMPERVA®

Our Research

- Behavioral Analysis
- Deception

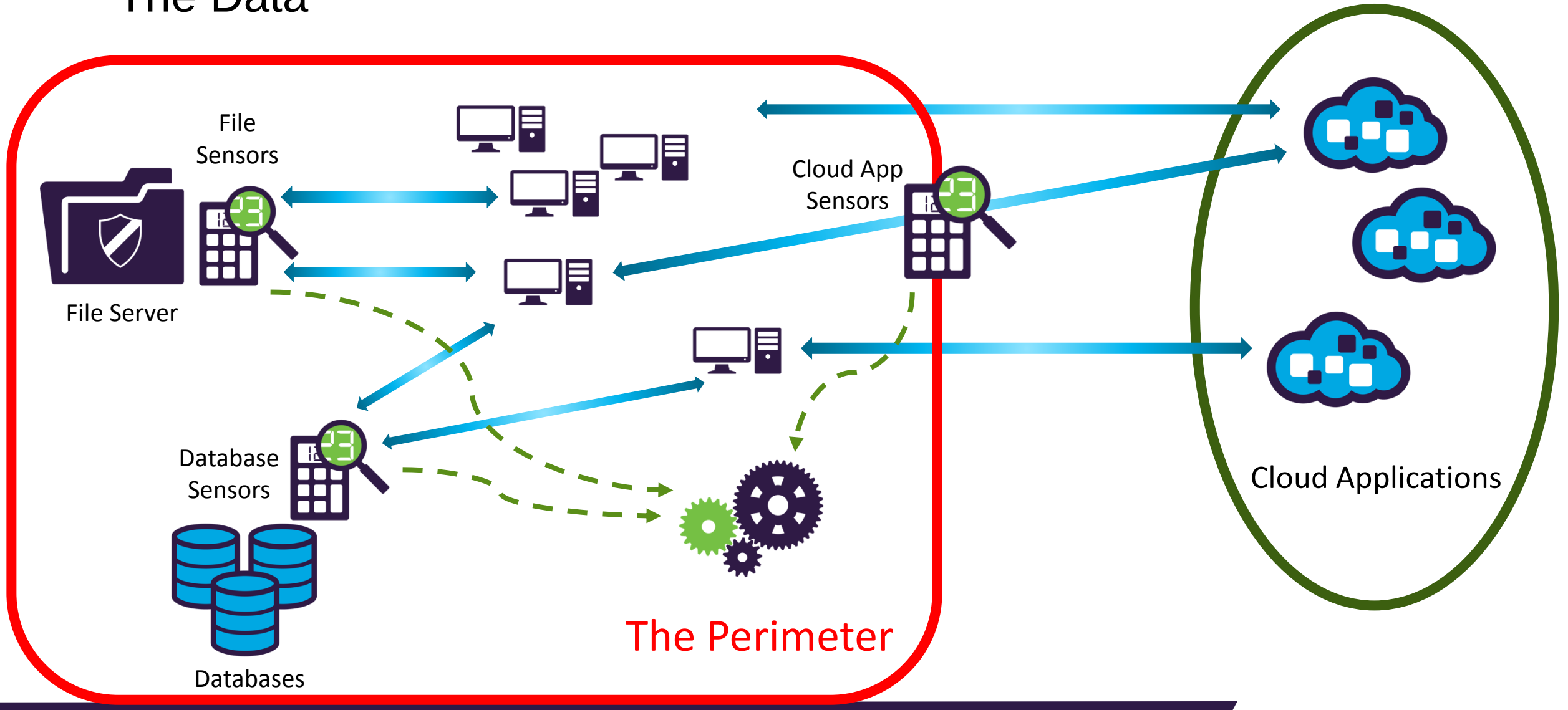
IMPERVA®

Our Research

- Behavioral Analysis
- Deception

IMPERVA®

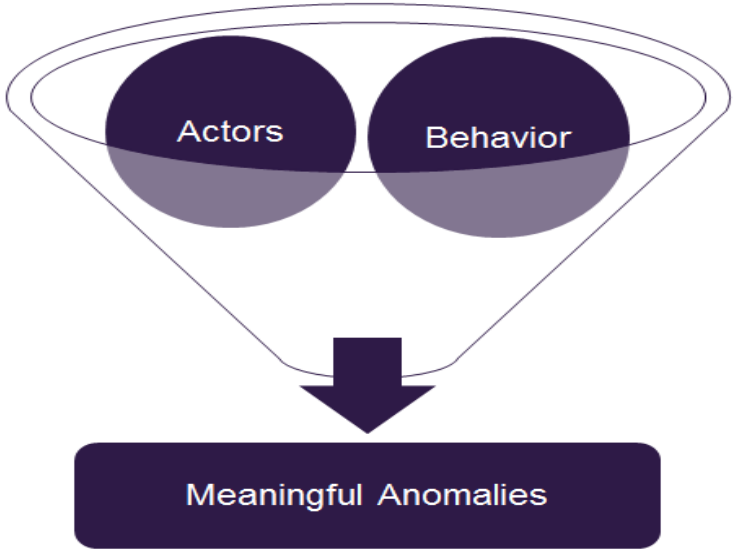
The Data



IMPERVA®

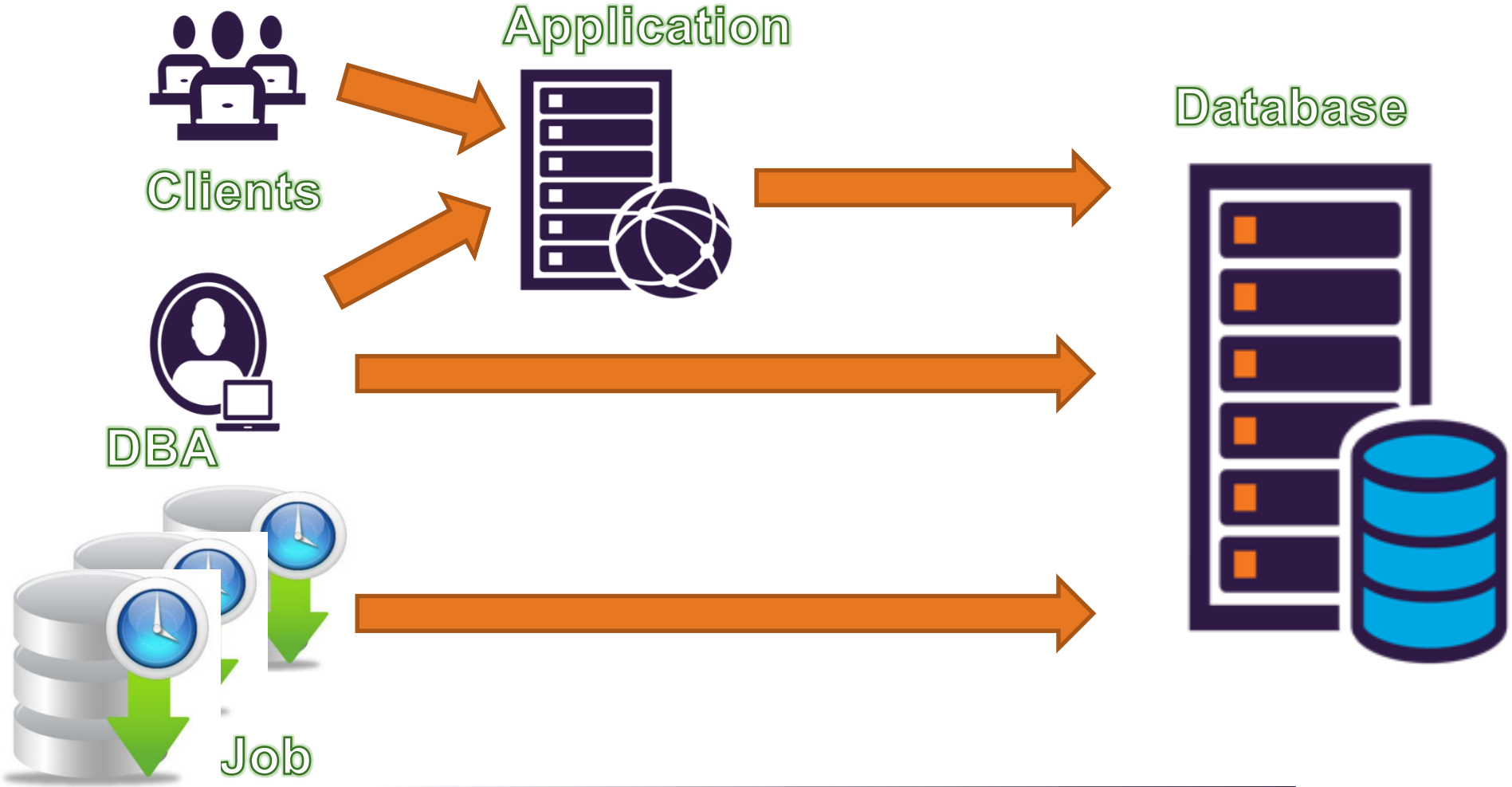
Our Research – Behavioral Analysis

- Collect live production data from several customers of Imperva
- Full database and file server audit trail - SecureSphere audit logs
- Machine learning algorithms identify “Actors” and “Good Behavior” in order to identify “Meaningful Anomalies”



IMPERVA®

Actors



IMPERVA®

Good Behavior

IMPERVA®

Behavioral Analysis Findings

- Malicious Insider
- Negligent Insider
- Compromised Insider

IMPERVA®

Behavioral Analysis Findings

- Malicious Insider
  - Hoarding IP before leaving the company
  - A DBA accessed financial information
- Negligent Insider
- Compromised Insider

IMPERVA®

Malicious Insider: Behavioral Analysis finds the IP Hoarder

- A Technical Writing employee copied > 100,000 files
- Employee was authorized to access data
- Operation took 3 weeks
- Each copy contained a few thousand files
- Some copies - in the middle of the night and/or on the weekend

IMPERVA®

Malicious Insider: Behavioral Analysis finds the IP Hoarder

- The employee / department never copied this amount of files
- The employee never worked on weekends / middle of the night

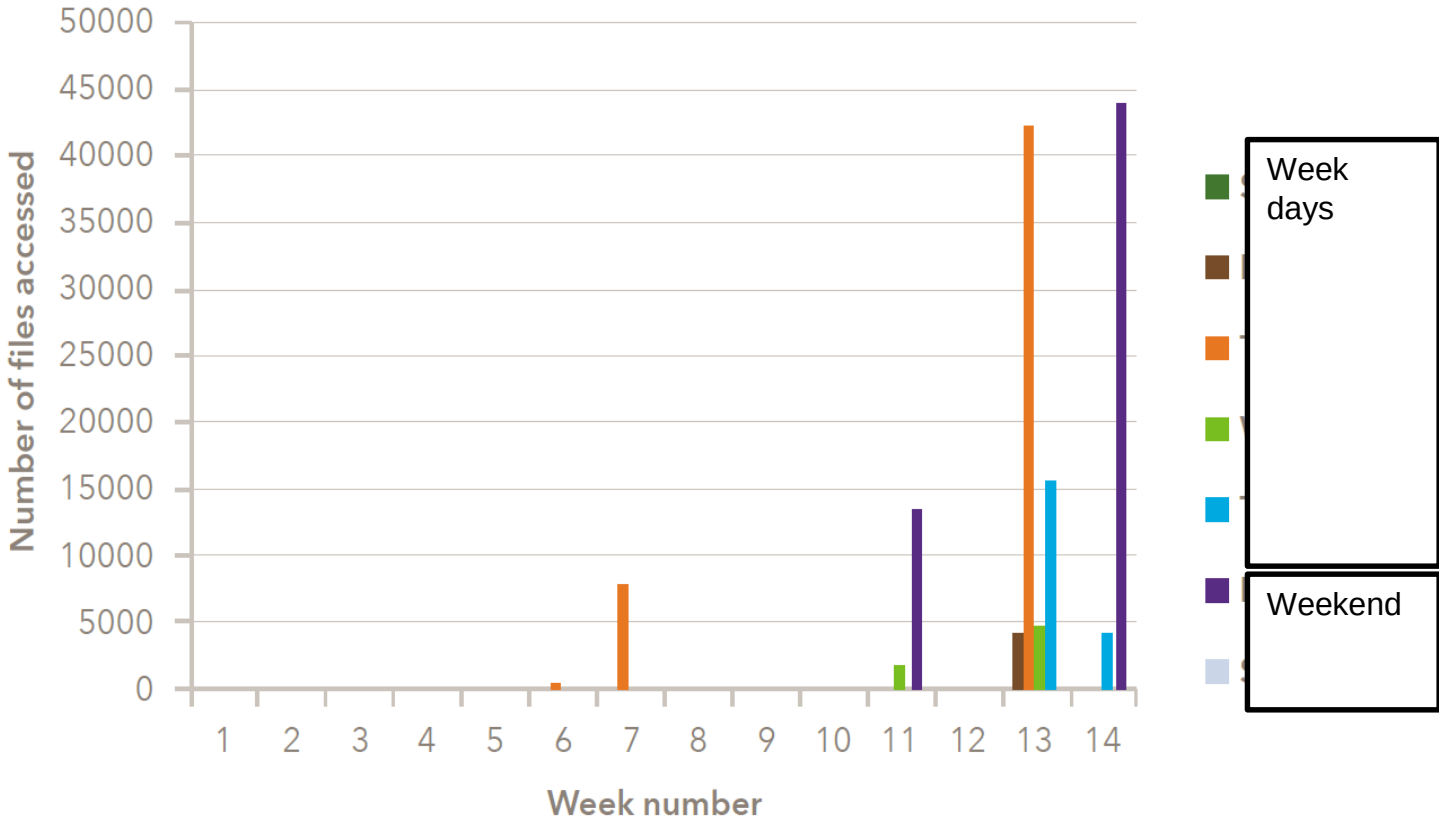


Figure 1: Number of files accessed by user in a week

IMPERVA®

Malicious Insider: Behavioral Analysis finds the IP Hoarder

- The employee / department never copied this amount of files
- The employee never worked on weekends / middle of the night

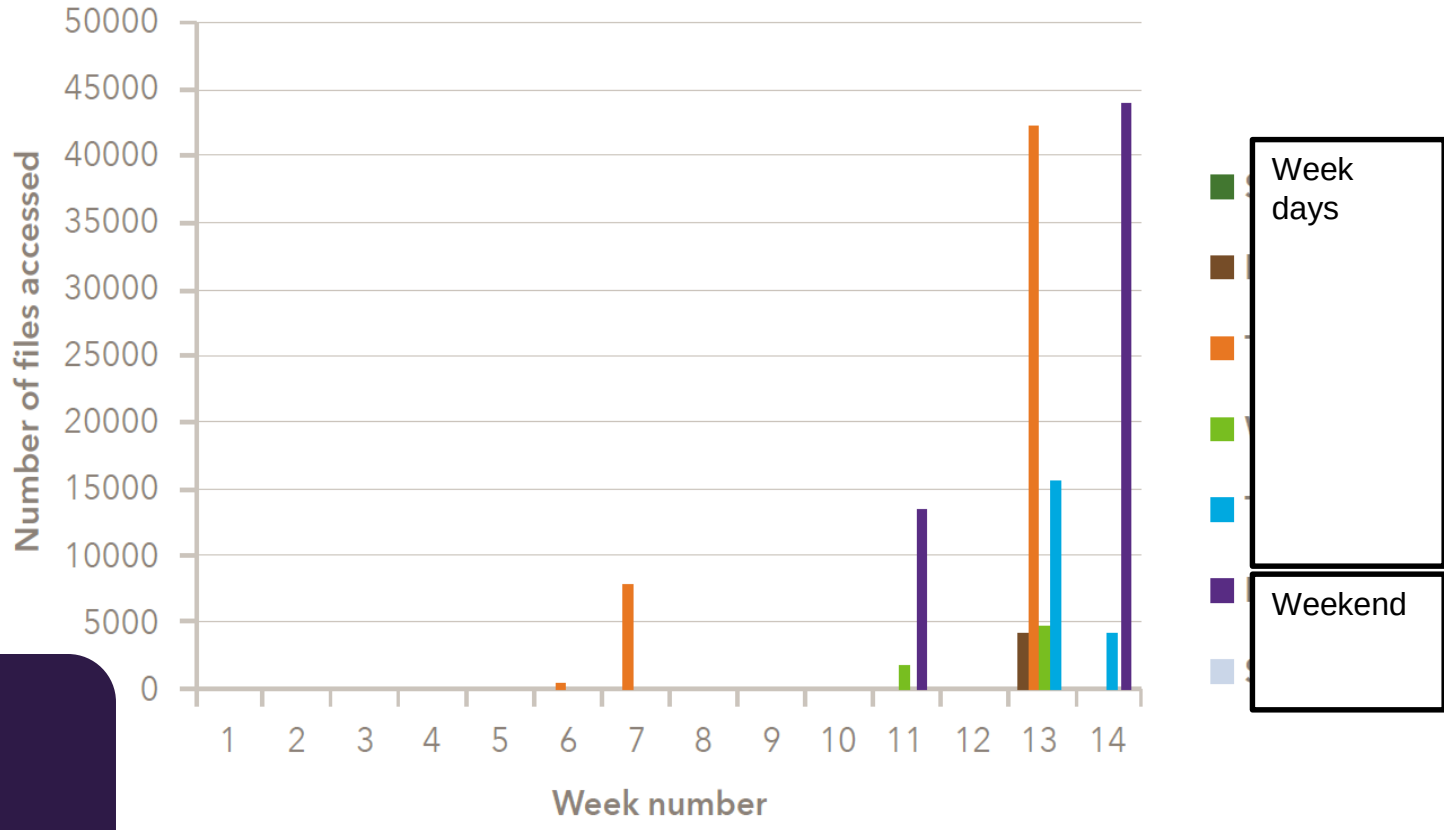


Figure 1: Number of files accessed by user in a week

Employee was authorized to access data

IMPERVA®

Malicious Insider: Behavioral Analysis finds the IP Hoarder

Organization Feedback:

- The employee was planning to leave the organization shortly after the incident took place

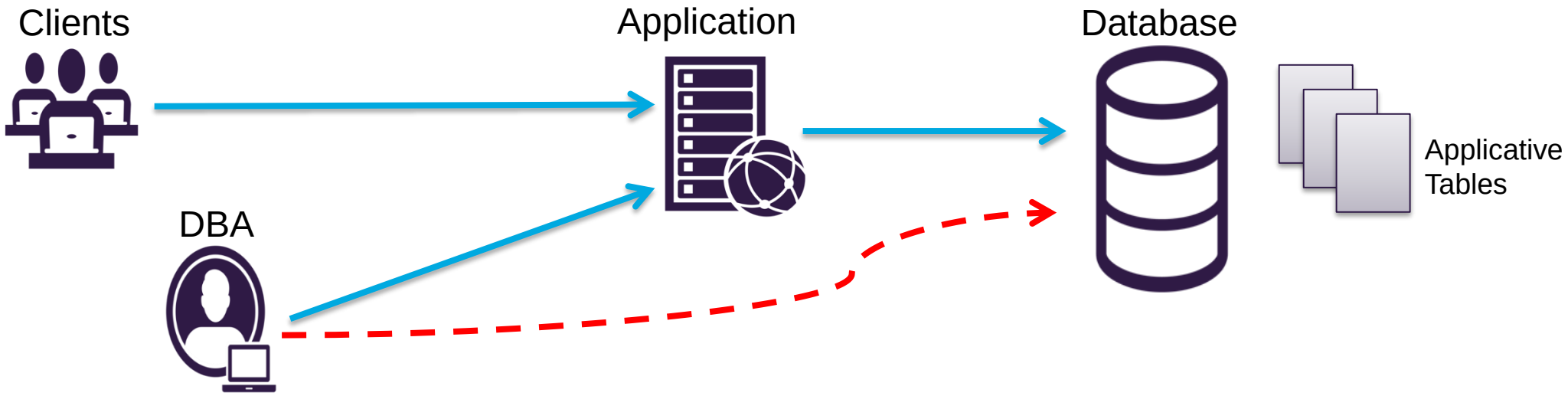
IMPERVA®

Behavioral Analysis Findings

- Malicious Insider
  - Hoarding IP before leaving the company
  - A DBA accessed financial information
- Negligent Insider
- Compromised Insider

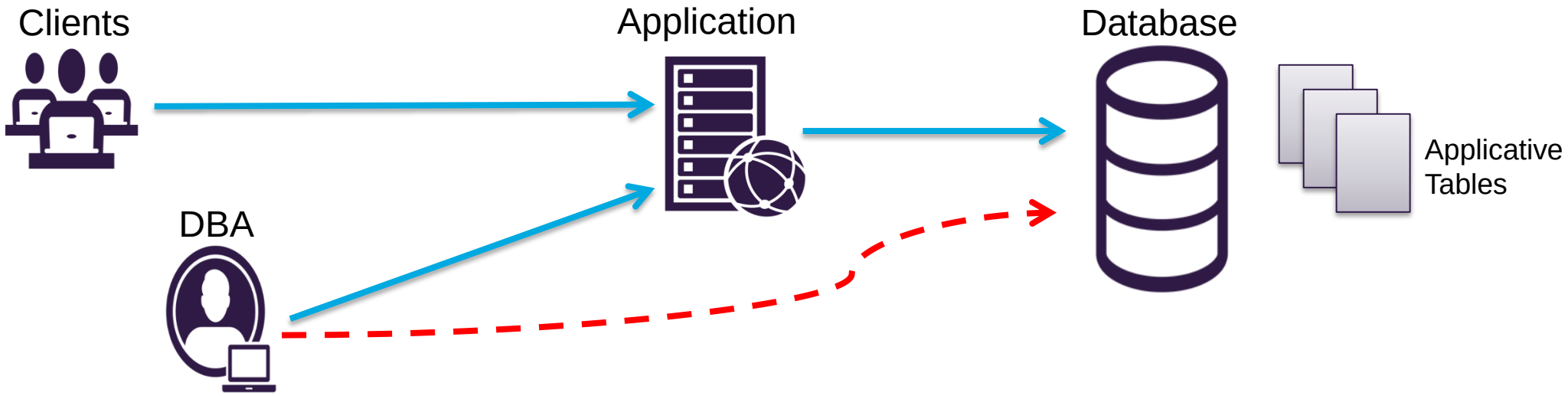
IMPERVA®

Malicious Insider: Behavioral Analysis flags DBA abusing privileges



IMPERVA®

Malicious Insider: Behavioral Analysis flags DBA abusing privileges



- A DBA from IT retrieved and modified multiple records from PeopleSoft application tables on a specific day
- Didn’t access these tables through the PeopleSoft interface

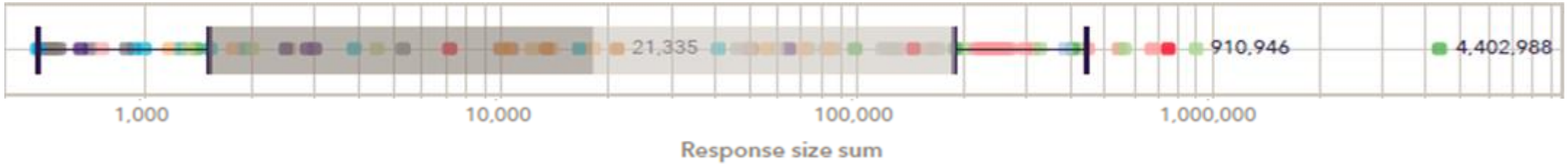
→ bypassed PeopleSoft logging and retrieval limitations

IMPERVA®

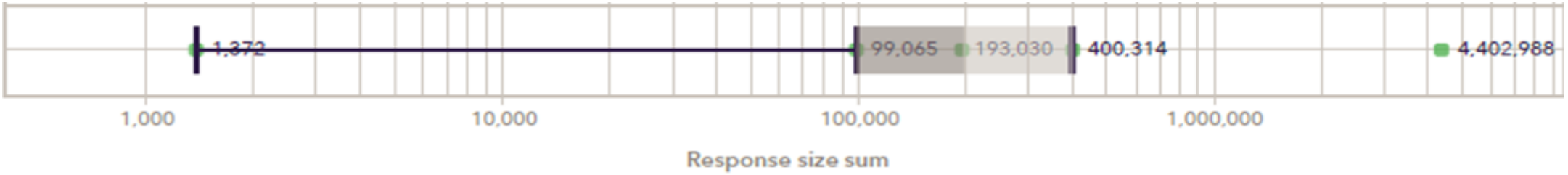
Malicious Insider: Behavioral Analysis flags DBA abusing privileges

- Retrieved many records

Compared to other users -



Compared to himself -



IMPERVA®

Malicious Insider: Behavioral Analysis flags DBA abusing privileges

- Modified several thousands of records in one table
- The tables contained sensitive financial information

IMPERVA®

Malicious Insider: Behavioral Analysis flags DBA abusing privileges

- Modified several thousands of records in one table
- The tables contained sensitive financial information

Should a DBA access financial information ???

IMPERVA®

Malicious Insider: Behavioral Analysis flags DBA abusing privileges

Organization Feedback:

- A DBA from IT should never be exposed to financial information
- Certainly not modify this information outside of application processes

IMPERVA®

Behavioral Analysis Findings

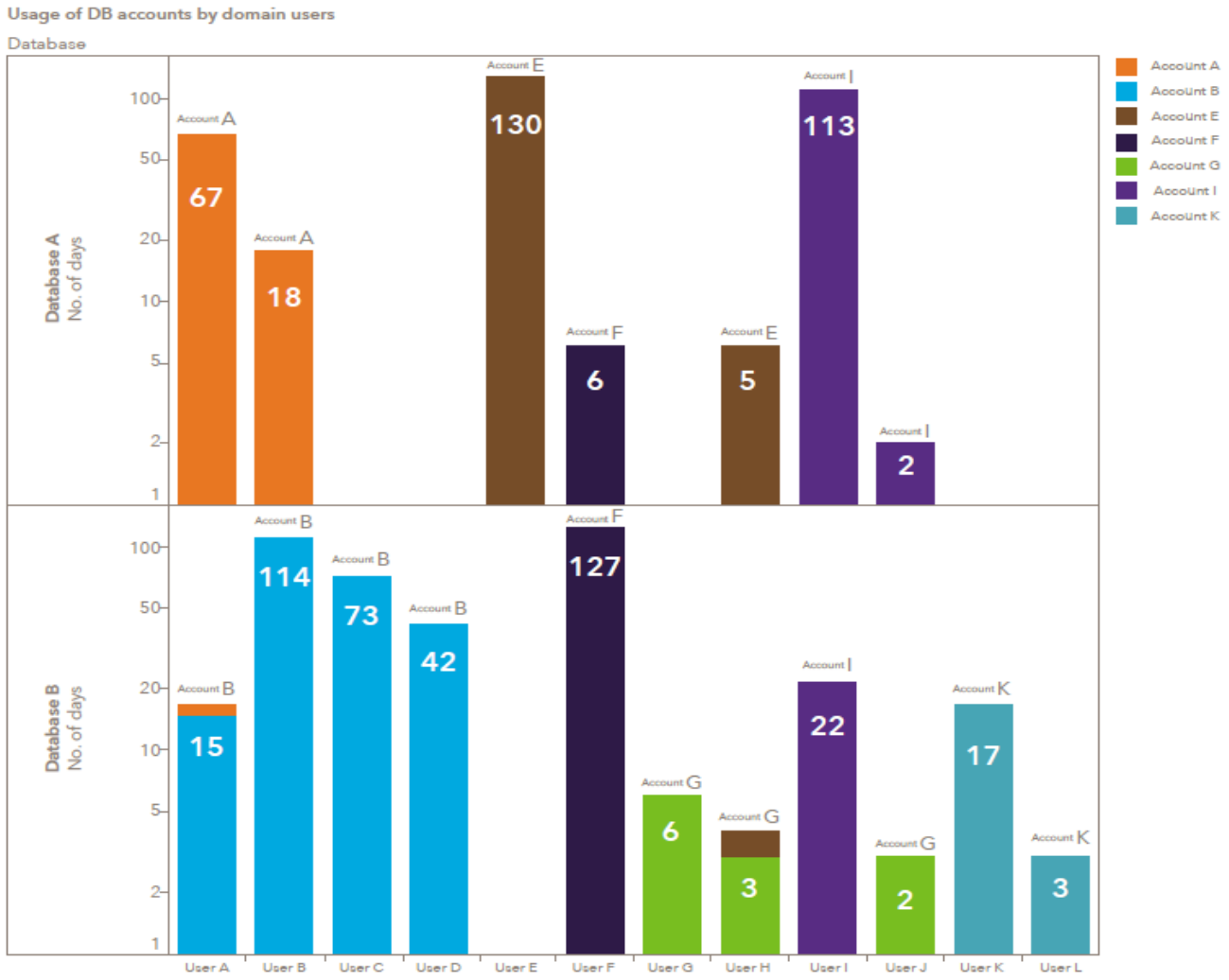
- Malicious Insider
- Negligent Insider
  - Account Sharing
- Compromised Insider

IMPERVA®

Negligent Users: Behavioral Analysis flags Account Sharing

- Bypass organization permissions and privileges
- Provide people with access that they are not entitled to
- Leave incorrect access trail to the data
- **Sharing is not caring!**

Negligent Users: Behavioral Analysis flags Account Sharing



- A and B share privileges
- C and D use B's account
- H uses the accounts of E, G
- J uses the accounts of G, I
- L uses the account of K

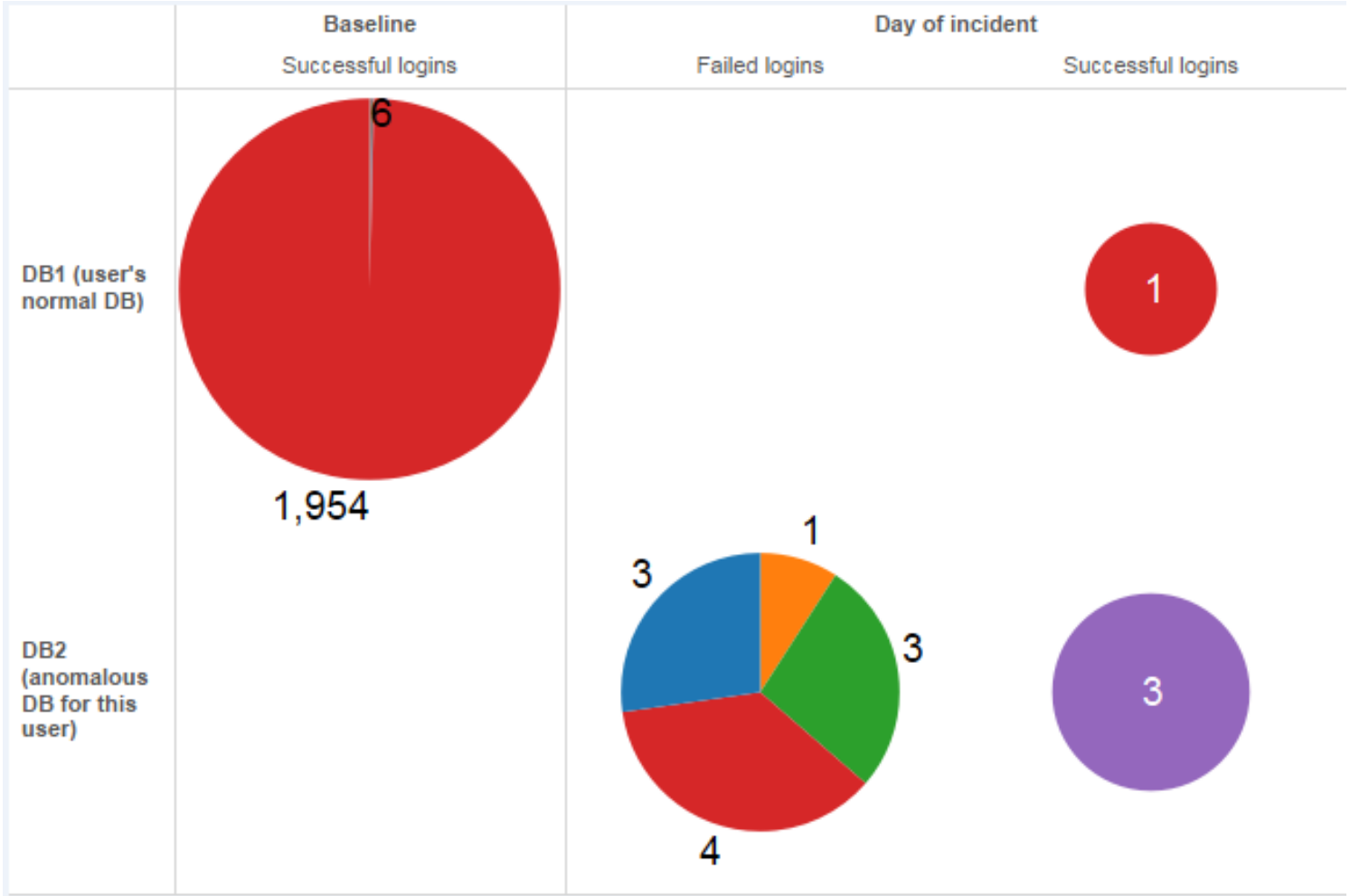
IMPERVA®

Behavioral Analysis Findings

- Malicious Insider
- Negligent Insider
- Compromised Insider
  - Multiple failed login attempts

IMPERVA®

Compromised Users : How failed logins are flagged as anomalous



- Baseline period
  - the user always successfully logs into DB1 using “red” account
  - never logs into DB2
- On the day of the incident
  - the user tried and failed to log into DB2 11 times using 4 different account
  - Succeeded using 5th account

IMPERVA®

Behavioral Analysis - Summary

IMPERVA®

Behavioral Analysis - Summary

- We found interesting incidents for all insiders options
- It was hard to find them without behavioral analysis methods
  - Used valid privileges
  - Chose “meaningful” anomalies
- Concentrated on the **actors** and on their access to the **data**

Our Research

- Behavioral Analysis
- Deception

IMPERVA®

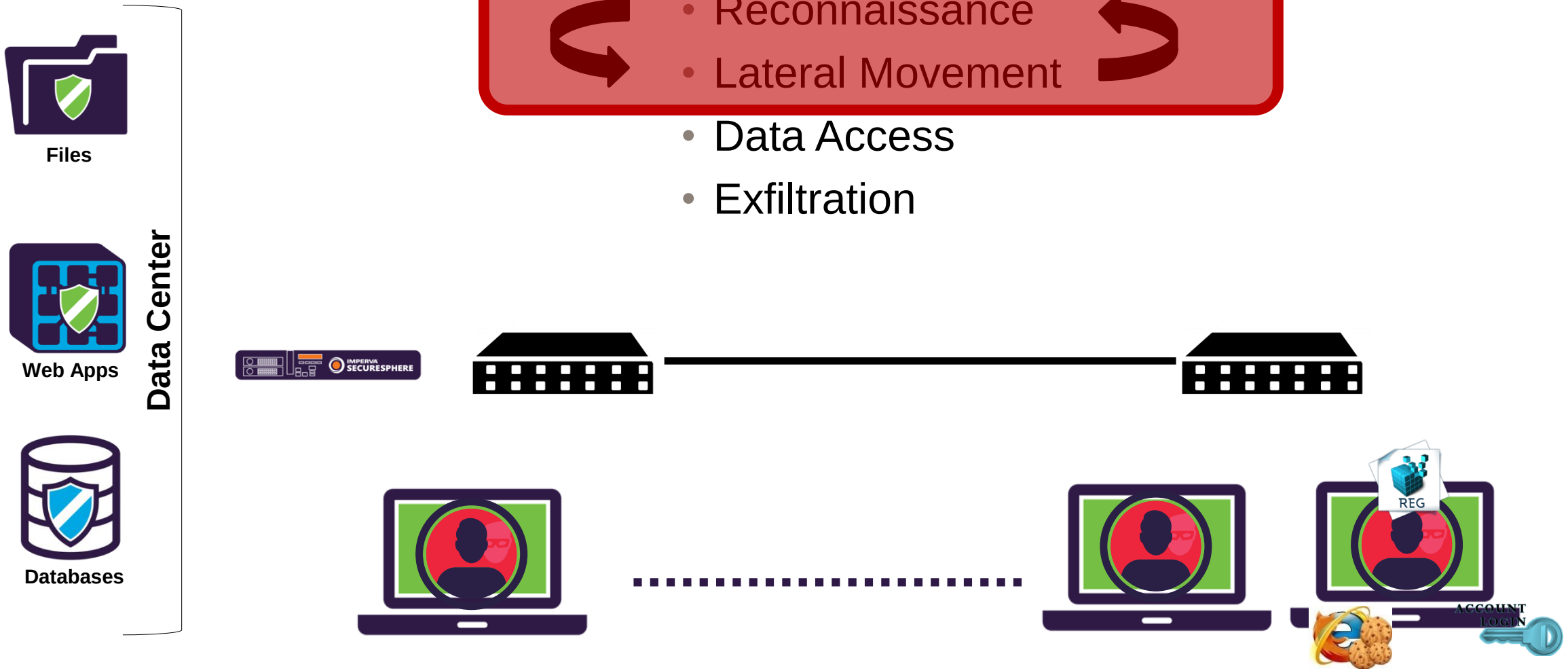
Deception Why?

- Because **Compromise is Inevitable**
  - No Perimeter: BYOD, Cloud Apps, VPN
  - Legitimate apps (TeamViewer, DropBox)
  - Zero Days
  - Social Engineering
- Find **Data Breach** within **Compromises**
  - Compromises happen all the time… **few** of them may turn into a breach!
  - Response team have to prioritize
  - **100 alerts << 1 alert**
- **Detect** a breach **ASAP**
  - Reconnaissance & Lateral Movement

IMPERVA®

Attack Cycle

- Compromise
- Reconnaissance
- Lateral Movement
- Data Access
- Exfiltration



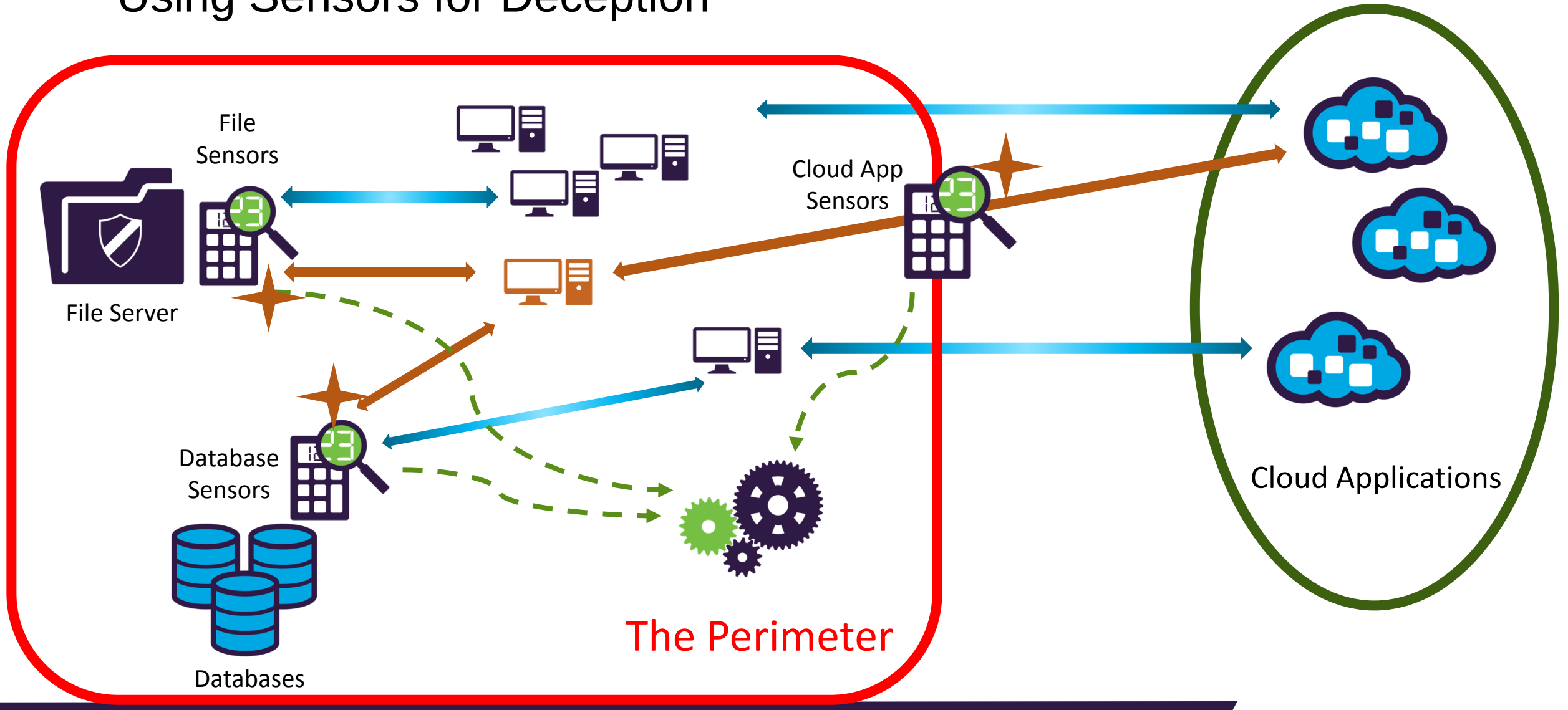
IMPERVA®

Deception Tokens

- **Point** the attacker towards a **Trap**
  - Web, File, DB Server (etc)
  - Local / Domain Account
  - Passwords, Cookies, Authentication Tokens
- Trap Server is **Real**
  - Not a Honeypot
- **Detection** = Harvest + Use token
  - Deliberate attempt at the data center / gain more privileges

IMPERVA®

Using Sensors for Deception



IMPERVA®

Browser Passwords

- Where are autocomplete passwords saved?
- Are they safe?

Browser Passwords

Return to Index

IMPERVA®

MimiKatz

- Pulling plaintext passwords from Windows
- Relies on Wdigest interface through LSASS

- Wdigest: a DLL used to authenticate users against HTTP Digest authentication and Simple Authentication Security Layer (SASL) exchanges.

- (un)fortunately, these require the plain-text password

IMPERVA®

MimiKatz


```
mimikatz 2.0 alpha x64

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Sep 30 2013 23:42:09)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz
  '#####'                                     with  10 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 196180 (00000000:0002fe54)
Session           : Interactive from 1
User Name         : user
Domain            : VM-7x64-test
        msv :
         [00000003] Primary
         * Username : user
         * Domain   : VM-7x64-test
         * LM       : 00000000000000000000000000000000
         * NTLM     : 5058dcdf3965e4cff53994b1302e3174
        tspkg :
         * Username : user
         * Domain   : VM-7x64-test
         * Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
        wdigest :
         * Username : user
         * Domain   : VM-7x64-test
         * Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
        kerberos :
         * Username : user
         * Domain   : VM-7x64-test
         * Password : ImagineTryingToCrackSomeSuperLongP@$$w0rdLikeThis!!!
        ssp :
```


Return to Index

IMPERVA®

Compromised User Scenario

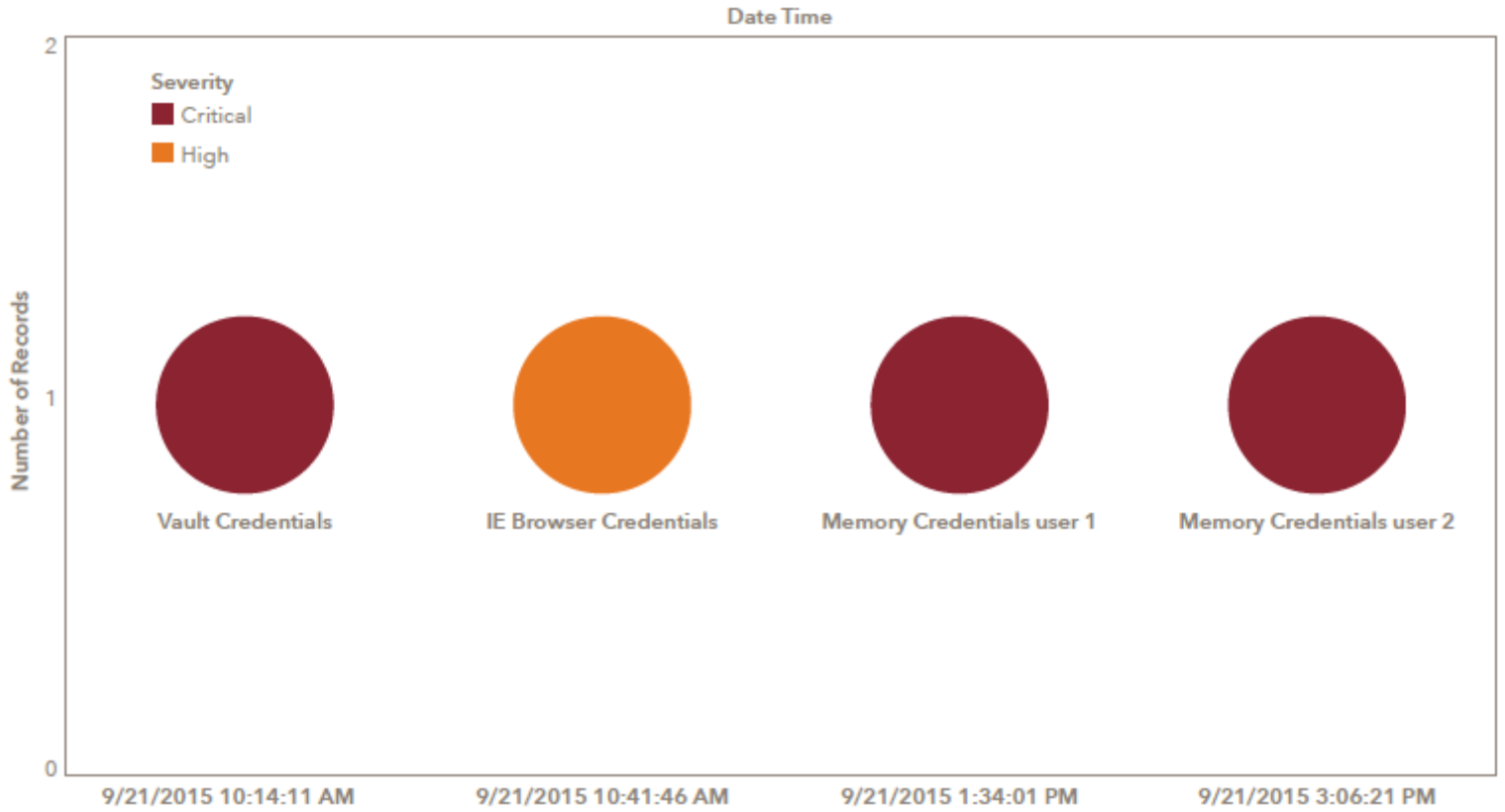


Figure 5: Example of credential dumps

- Trojan got through to the endpoint via phishing
- Planted credentials inside Windows Vault, Internet Explorer were used
- Determine the source and scope of the attack without tipping off the attacker

IMPERVA®

IMPERVA®