WHEEL SYSTEMS

Going Beyond Security

MICHAŁ JARSKI

HE WAS NOT A
HACKER

SNOWDEN CASE

Snowden - former contractor who copied and leaked classified information from the National Security Agency (NSA)

1.7 million

documents had been copied revealing numerous global surveillance programs (1)

IMPORTANT:
Despite the fact that the USA spends over $52.6 billion every year on the US Intelligence Program, there has been a major access rights violation by a privileged user.

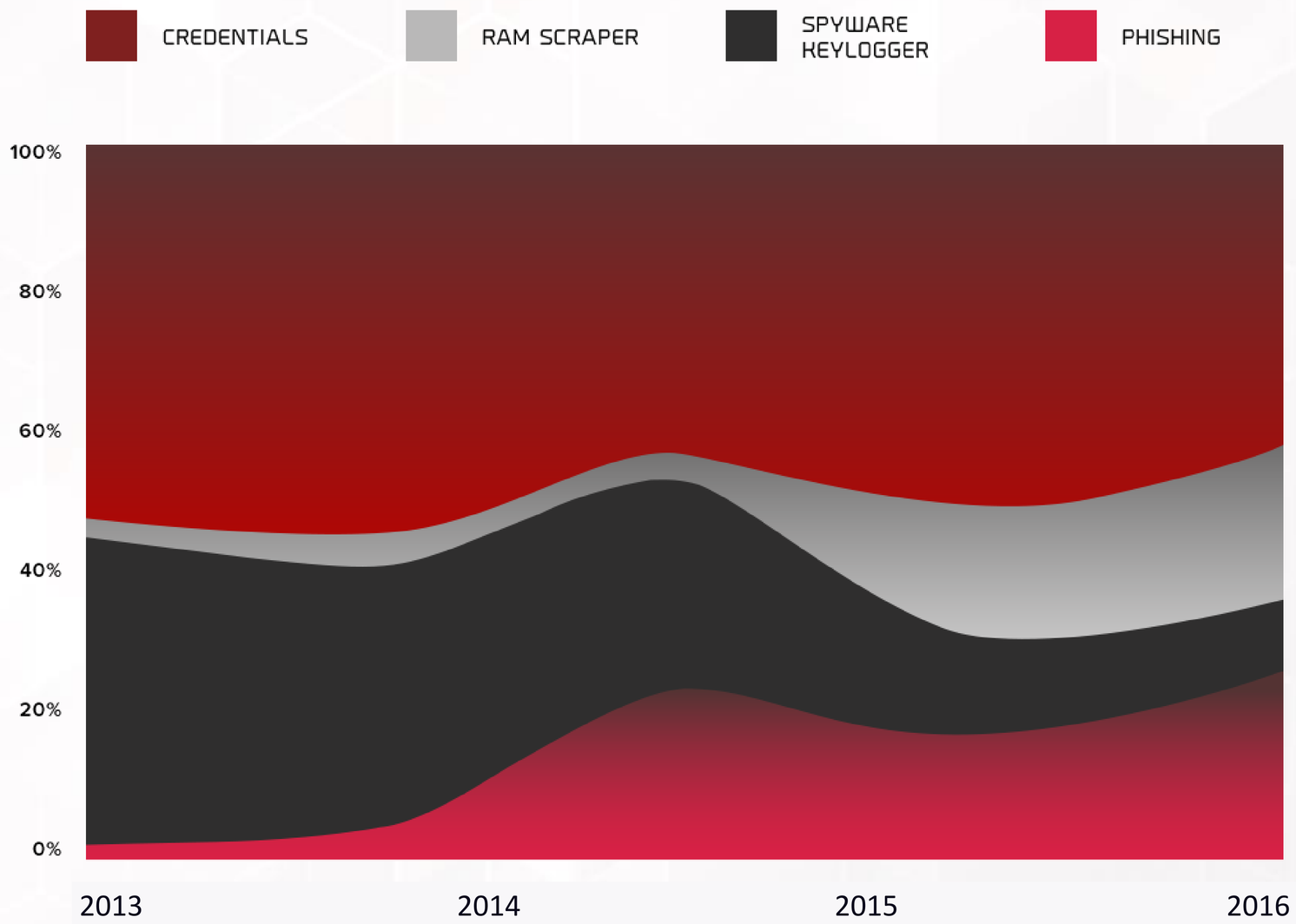
Source: (1) Bloomberg News. Retrieved February 1, 2014.

WHO IS A PRIVILEGED USER

A privileged user can be a trusted internal employee, an external contractor, or an internally programmed service account. It can also be a malicious user with access to privileged accounts and resources.

A privileged user has access to company's most critical resources.

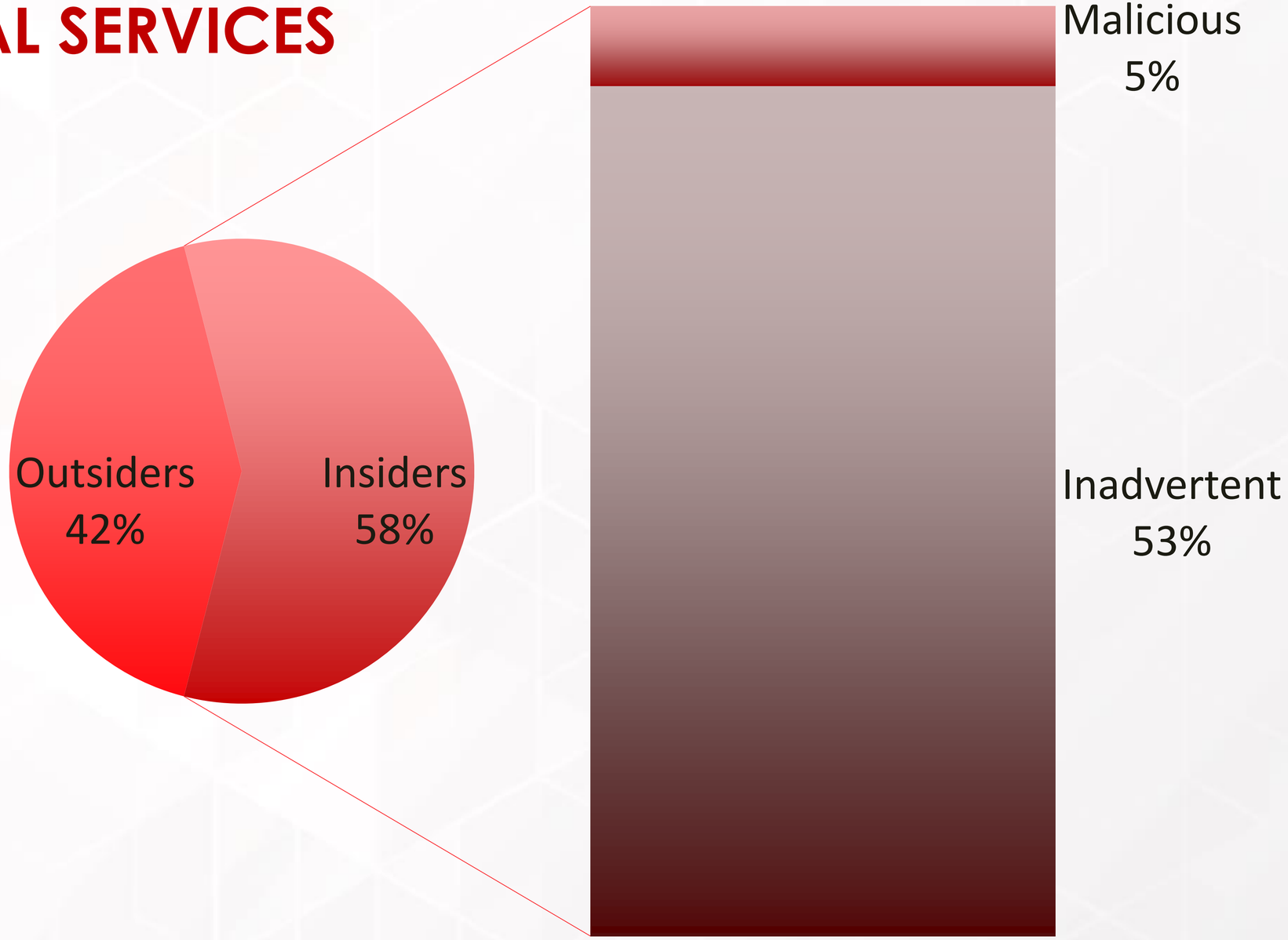
CREDENTIALS INCIDENTS - 40% OF ALL BREACHES



Source: Verizon Data Breach Investigation Report

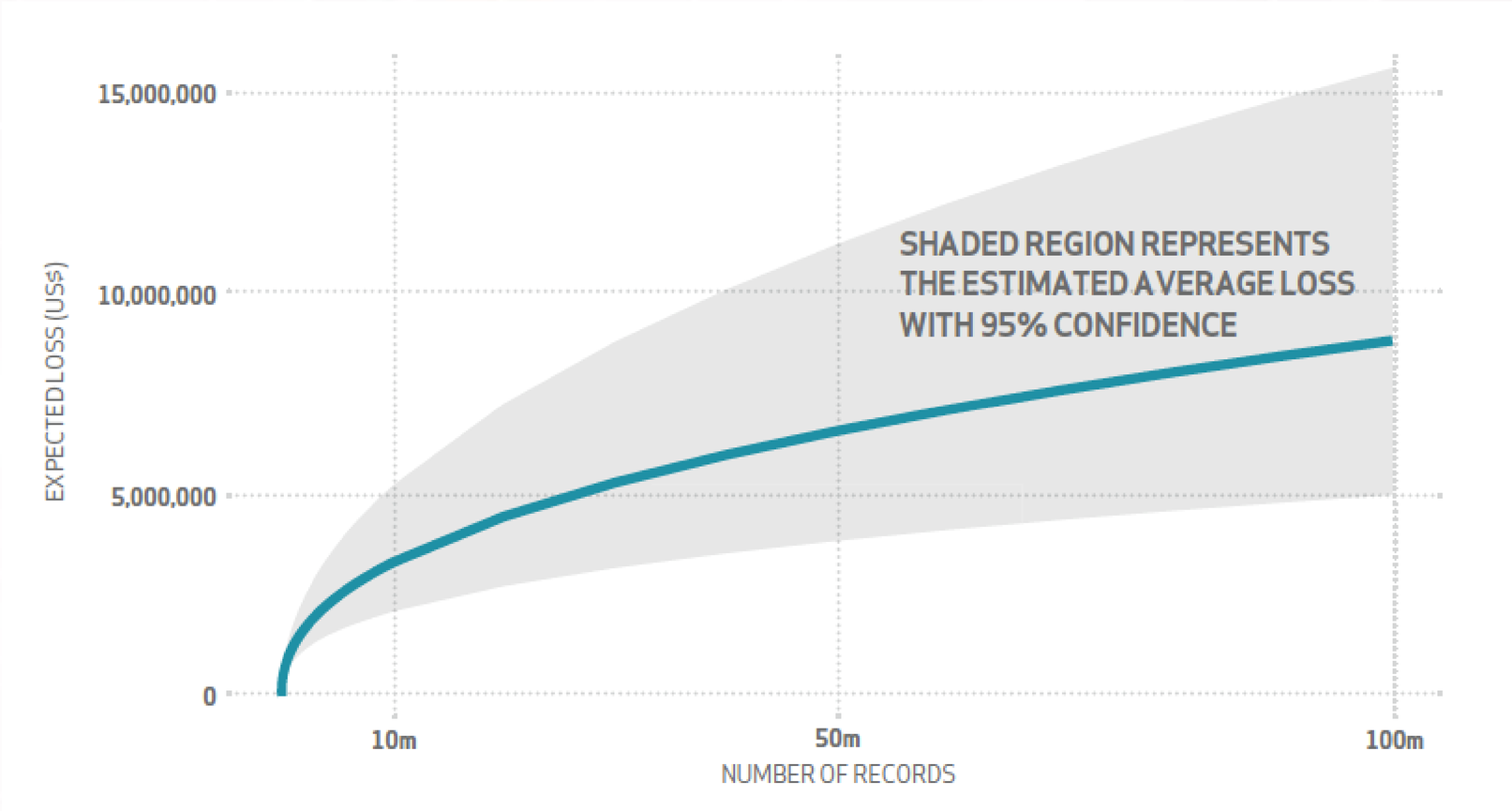
WHEEL SYSTEMS

SOURCE OF DATA BREACHES IN FINANCIAL SERVICES



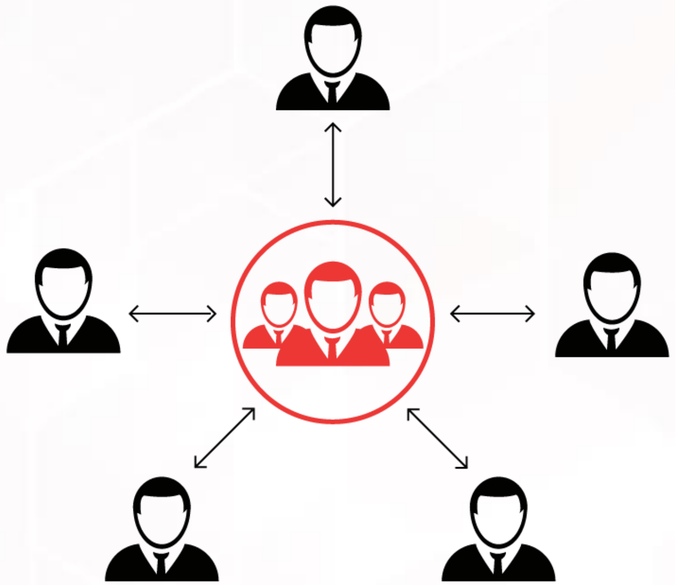
source: IBM X-Force 2017

The forecast average loss for a breach of 1,000 records is between $52,000 and $87,000 with 95% confidence. Compare that to a breach affecting 10 million records where the average loss is forecasted to be between $2.1 million and $5.2 million (note that these are average losses, not single-event losses).



Source: Verizon “2016 Data Breach Investigation report”

THREATS OF
PRIVILEGED SESSIONS



- ACTIVITIES AGAINST SERVICING CONTRACT
- UNAUTHORIZED ACCESS TO COMPANY DATA
- **THEFT OF DOCUMENTS, PATENTS, CONFIDENTIAL INFORMATION, FINANCIAL FRAUDS**
- DELETING OR MODIFYING ESSENTIAL INFORMATION
- **UNAUTHORIZED ACTIONS** (DELETING FILES, SETTING UP BACKDOORS, INFECTION, CONFIGURATION CHANGES)
- SUPPRESSING EVIDENCES OF A CRIME
- INCORRECT EXECUTION OF OFFICIAL ORDERS
- LACK OF COMPETENCIES
- RESPONSIBILITY ISSUES

WHEEL SYSTEMS

COMMON ADMINISTRATIVE PROBLEMS

- No centralized Privileged Access Management
- Lack of proper administrator account control
- Lack of session management
- Password sharing
- Lack of password rotation and password policies

COMPLIANCE

- PCI DSS v3.2 (since April 2017) – MFA for all CDE
- NIS Directive (2016-2018)
- GDPR Directive (2016-2018)
- ISO 27000

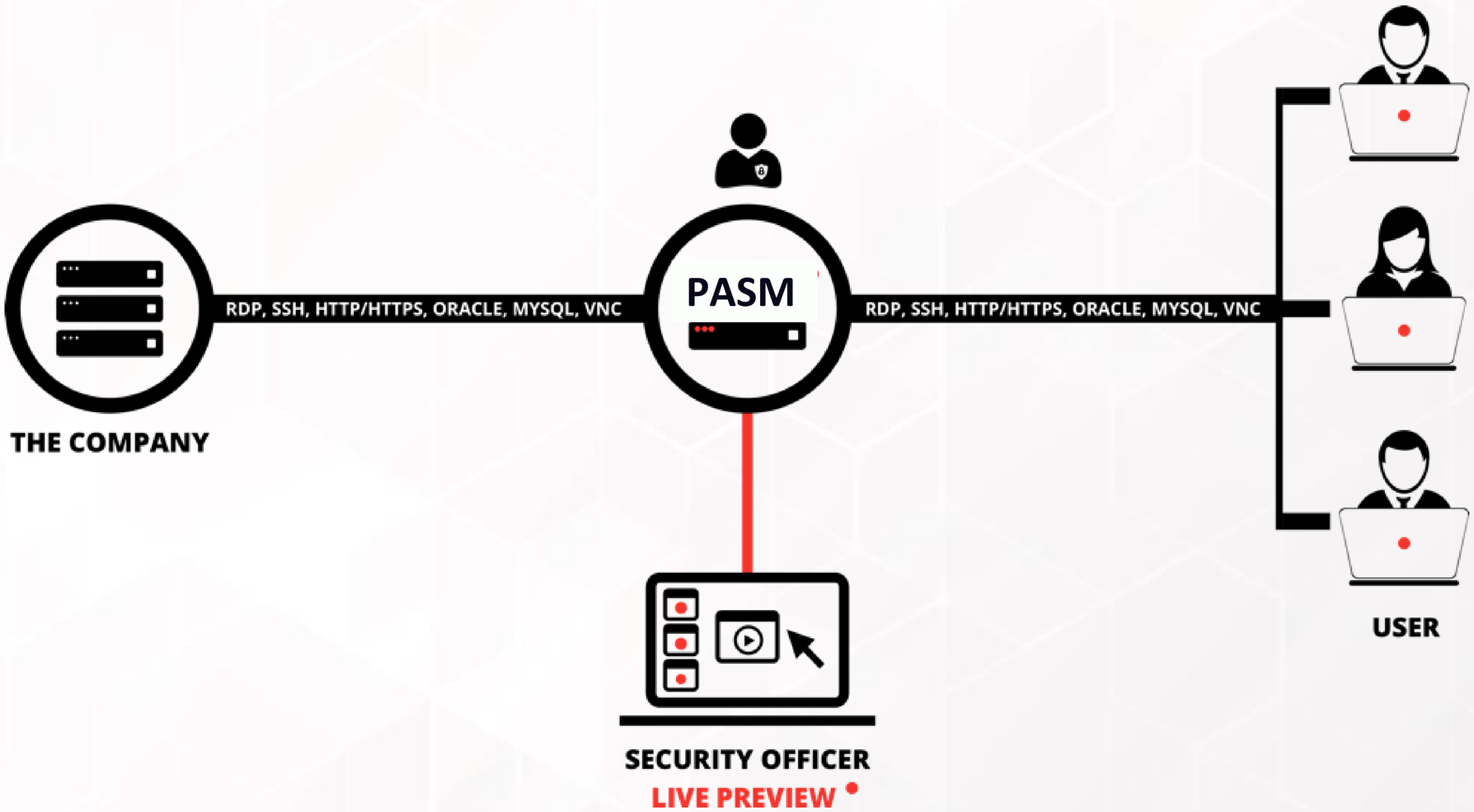
WHEEL SYSTEMS

WHAT TO DO?

- ENABLE MONITORING, RECORDING AND AUDITING OF REMOTE ACCESS SESSION AS IF YOU WERE LOOKING OVER A REMOTE USER'S SHOULDER

WHEEL SYSTEMS

HOW PASM WORKS



WHEEL SYSTEMS

USE CASE 01

INTENTIONAL WRONGDOING OF REMOTE CONSULTANTS

PROBLEM:

- **LACK OF STRONG EVIDENCE OF A QUESTIONABLE WORK.**
- **FIREWALL LOGS ONLY ALLOW PROVIDING PROOF THAT GIVEN RESOURCES HAD BEEN ACCESSED BUT WITHOUT PINPOINTING THE EXACT USER.**

SOLUTION:

- **PASM RECORDS ALL USER ACTIONS** (EXECUTED COMMANDS, TRANSFERRED FILES, ETC.)

WHEEL SYSTEMS

USE CASE 02

UNINTENTIONAL WRONGDOING OF REMOTE CONSULTANTS

PROBLEM:

- **NO ACCOUNTABILITY FOR THE QUESTIONABLE WORK.**
- **ABILITY TO COVER UP THE MISTAKES.**
- **DELAY IN DETECTING MISTAKES OF REMOTE ADMINISTRATORS.**

SOLUTION:

- **PASM RECORDS ALL USER ACTIONS** (EXECUTED COMMANDS, TRANSFERRED FILES, ETC.)
- **PASM ACTIVELY MONITORS USER'S ACTIONS, CAN TERMINATE CONNECTION AUTOMATICALLY AND CAN DISABLE USER ACCOUNT UPON DETECTING ANY UNAUTHORIZED ACTIVITY**
- **PASM ENABLES VIEWING LIVE SESSIONS IN A WEB BROWSER**

WHEEL SYSTEMS

USE CASE 03

SHARING ACCOUNT WITH ADMINISTRATIVE PRIVILEGES

PROBLEM:

- **AN INABILITY TO DIFFERENTIATE AND UNEQUIVOCALLY IDENTIFY USERS WHO ACCESS THE SYSTEM.**
- **COMPLICATED MANAGEMENT OF ACCESS TO REMOTE RESOURCES.**
- **ABILITY TO INTENTIONALLY OR UNINTENTIONALLY BLOCK ACCESS FOR ALL THE ADMINISTRATORS SHARING A GIVEN ACCOUNT.**

SOLUTION:

- **EACH USER IS AUTHENTICATED BY PASM USING AN INDIVIDUAL LOGIN AND PASSWORD OR AAA SERVER**
- **UPON ESTABLISHING A CONNECTION PASM CAN SUBSTITUTE LOGIN CREDENTIALS**
- **PASM ENABLES GENERATING A DETAILED CONNECTION REPORT**

WHEEL SYSTEMS

USE CASE 04

DISTRIBUTED USER'S AUTHENTICATION CREDENTIALS

(DIFFERENT LOGIN INFORMATION ON EACH SERVER, DIVERSIFIED PASSWORD UPDATE POLICIES, ETC.)

PROBLEM:

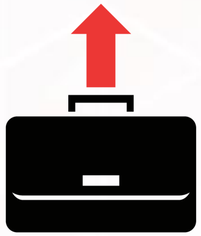
- **DIFFICULTIES IN MANAGING REMOTE USER ACCESS DUE TO LACK OF CENTRALIZED PROCESS.**
- **VARIETY OF USER AUTHENTICATION DATA TO DIFFERENT SYSTEMS.**

SOLUTION:

- **PASM ENABLES ACCESS TO A NUMBER OF DIFFERENT RESOURCES** (UNIX, WINDOWS, DATABASES, WEB SITES, ETC.) **USING SINGLE LOGIN/PASSWORD COMBINATION**
- **SINGLE SIGN-ON**

WHEEL SYSTEMS

USE CASE 05



INFORMATION LEAK

PROBLEM:

- **ADMINISTRATORS CAN DOWNLOAD FILES AND EASILY COVER THEIR TRACKS.**

SOLUTION:

- **PASM RECORDS ALL UESR ACTIONS**
- **PASM SUPPORTS TRUSTED TIME STAMPING ALLOWING TO PRECISELY IDENTIFY WHOM AND FROM WHAT LOCATION THE UNIDENTIFIED USER ACCESSED A GIVEN FILE**

WHEEL SYSTEMS

USE CASE 06

WEAK EVIDENCE IN COURT

PROBLEM:

- NO ACCOUNTABILITY OF REMOTE ADMINISTRATORS' WORK.
- INSUFFICIENT INFORMATION INCLUDED IN SYSTEMS LOGS TO SERVE AS CONCRETE EVIDENCE.
- NO GUARANTEE OF THE DATA INTEGRITY GATHERED BY SIEM.

SOLUTION:

- PASM ENCRYPTS STORED DATA
- PASM ENSURES DATA INTEGRITY
- USERS' INDENTITY CAN BE VERIFIED BY USING AN EXTERNAL AUTHENTICATION SYSTEM
- PASM ENABLES TRUSTED TIME STAMPING, CERTIFYING THE AUTHENTICITY OF ALL RECORDED MATERIAL
- SESSION DATA RECORDED ON PASM IS CONCRETE EVIDENCE IN COURT

WHEEL SYSTEMS

USE CASE 07

INEFFICIENT HIRED CONSULTANTS

PROBLEM:

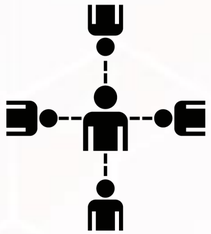
- **EXPENSIVE YET INEFFICIENT SERVICES OFFERED BY CONSULTING COMPANIES.**
- **LACK OF MEANS TO VERIFY THE TIME IT TOOK TO PROVIDE THE CONTRACTED SERVICE.**

SOLUTION:

- **PASM RECORDS USERS' ACTIONS ALLOWING TO REPLAY THE SESSION IN VIDEO STREAM**
- **PASM PROVIDES THE CONFIRMATION OF CONSULTANT'S ACTUAL WORKING TIME**

WHEEL SYSTEMS

USE CASE 08



SESSION SHARING

PROBLEM:

- **LACK OF COMPETENCIES TO PERFORM A GIVEN TASK.**
- **INABILITY TO PERFORM ACTIONS WHICH REQUIRE ADDITIONAL AUTHENTICATION, WITHOUT GIVING OUT THE ACTUAL AUTHENTICATION INFORMATION.**

SOLUTION:

- **PASM ENABLES SIMULTANEOUS WORK OF THE SYSTEM ADMINISTRATOR AND REMOTE USER IN THE SAME SESSION**
- **DURING THE SESSION, A PASM ADMINISTRATOR CAN INPUT A PASSWORD TO ACCESS CERTAIN RESOURCES, WITHOUT GIVING IT OUT TO THE REMOTE USER BY SIMPLY USING A WEB BROWSER**

WHEEL SYSTEMS

USE CASE 09

POST-MORTEM / FORENSIC ANALYSIS

PROBLEM:

- HIGH COST OF ANALYSIS AFTER THE BREAK-IN DUE TO THE NEED TO HIRE HIGH-PRICED INVESTIGATION ENGINEER.
- LACK OF CLEAR EVIDENCE.

SOLUTION:

- PASM RECORDS AND STORES ALL RDP, SSH, HTTP/HTTPS, VNC, ORACLE, MYSQL AND TELNET CONNECTIONS
- PASM ENABLES FINDING DESIRED ACCESS SESSIONS AND REVIEWING CONTENTS AS VIDEO STREAM
- PASM ENABLES SEARCHING FOR OCCURRENCES OF DESIRED PHRASES IN SESSIONS

WHEEL SYSTEMS

USE CASE 10

DOCUMENTING WORK AND PREPARING TRAINING MATERIALS

PROBLEM:

- **ABSORBING AND TIME CONSUMING DOCUMENTING OF COMPLETED TASKS.**
- **ADVANTAGE OF VIDEO MATERIALS OVER WRITTEN DOCUMENTATION.**

SOLUTION:

- **RECORDED SESSIONS CAN BE TRANSFORMED INTO DOCUMENTATION OF COMPLETED WORK IN A VIDEO FORMAT**
- **RECORDED SESSIONS CAN BE USED AS TRAINING MATERIALS**

WHEEL SYSTEMS

USE CASE

SUMMARY

- KEEP YOUR FINGER ON THE PULSE – **PROACTIVELY MONITOR REMOTE ACCESS SESSIONS**
- **MINIMIZE COSTS** OF POST-MORTEM ANALYSIS
- USE RECORDED MATERIAL IN THE COURT
- **INCREASE EXTERNAL CONSULTANTS' PRODUCTIVITY**
- **WORK ALONG HIRED** CONSULTANTS
- **CENTRALLY MANAGE** ACCESS TO YOUR RESOURCES
- **DOCUMENT AND UTILISE COMPLETED TASKS FOR TRAINING PURPOSES**

WHEEL SYSTEMS

HE WAS NOT A
HACKER

THANK YOU

Al. Jerozolimskie 178,
02-486 Warsaw, Poland

31 N 2nd Street 370,
San Jose, CA 95113

sales@wheelsystems.com
info@wheelsystems.com

Phone: +48 22 10 06 700
Fax: +48 22 10 06 7001

Phone: +1 (408) 320 0980

www.wheelsystems.com

WHEEL SYSTEMS | GOING BEYOND SECURITY