SZKOŁA GŁÓWNA HANDLOWA W WARSZAWIE

BIG DATA FOR CYBERSECURITY

DOMENICO BILLÈ – PUBLIC SECURITY, DEFENSE AND CYBERSECURITY MANAGER CEE

Partner

SAS THE POWER TO KNOW.

Sponsor

BGK BANK GOSPODARSTWA KRAJOWEGO

Media Partners

COMPUTERWORLD Polska

Harvard Business Review POLSKA

ICAN INSTITUTE

ITWIZ TO CO ISTOTNE W IT

MANAGEMENT BUSINESS ASSOCIATION MBA MANAGER

The Third International Workshop • Advanced Analytics and Data Science

Europol: iOCTA (Internet Organised Crime Threat Assessment)

Emerging Threats:

- Hostile international Cybercrime, direct ransom requests, psychological blackmailing (Bitcoin)
- Malware keeps on being #1 threat
    - Lack of Best practices and security awareness extending vulnerabilities duration
    - More targets to be attacked in the Internet of Things (Smart Appliances, i-cars..)
- “Ceo Fraud”: asking employees for financial transactions on his behalf
- Major Cyber attacks in 2014 and 2015
    - Law Enforcement invovlment on large scale
    - Organized Cyber crime interested in data and Intellectual Property to sell on the darknet

Europol: iOCTA (Internet Organised Crime Threat Assessment)

2015 iOcta guidelines:

- International Law Enforcement cooperation
  - Focus on blocking Cybercrime communities
  - Onymous Operation
- More resoruces needed
- Cybercrime Awereness increase
- LEA activities to cooperate with Private Sector and Research Centres
- Focus on Artificial Intelligence and Blockchain Technology

Top 3 Cyber attacks in 2015

#3: US Government Office of Personnel Management

- 21.5M Federal Records data stolen
- Credits to China
- Twice victim of attack
- Information could be used for identity theft and cyber-espionage.

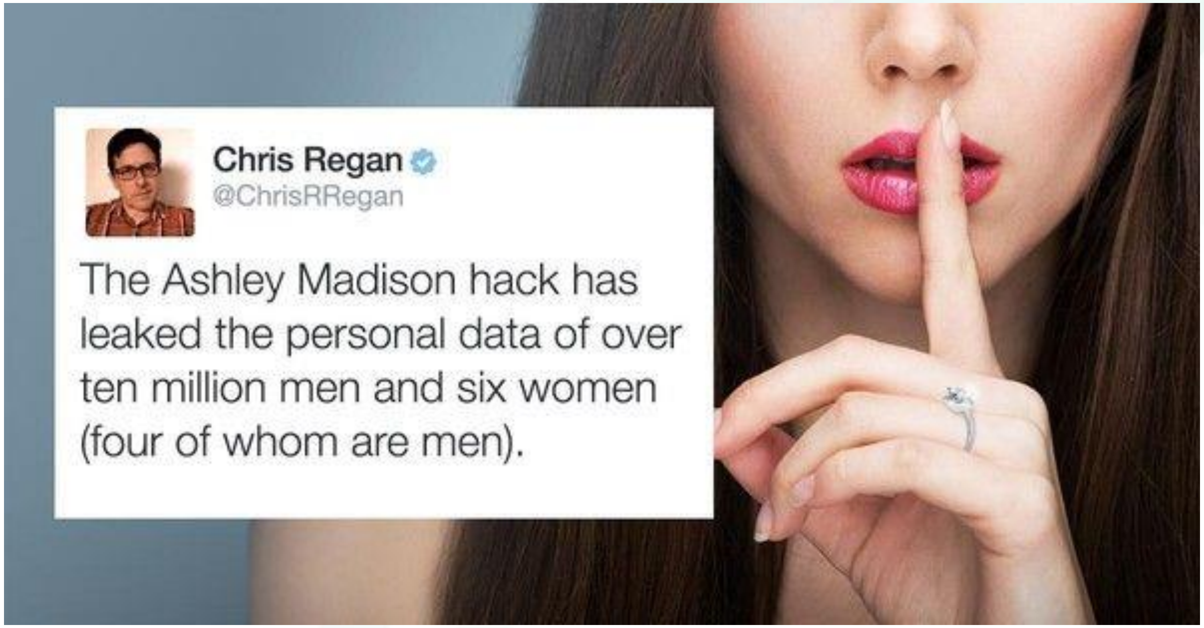
Top 3 Cyber attacks in 2015

~~#3: US Government Office of Personnel Management~~

#2: Ashley Madison "Life is short, have an affair.."

- 10GB of personal data stolen
- 20GB of Company data stolen
- The Impact Team threatening to release real names and associated data

Top 3 Cyber attacks in 2015



Chris Regan
@ChrisRRegan

The Ashley Madison hack has leaked the personal data of over ten million men and six women (four of whom are men).

Top 3 Cyber attacks in 2015

~~#3: US Government Office of Personnel Management~~

~~#2: Ashley Madison “Life is short, have an affair..”~~

#1: The Hacking Team

- Unidentified Hackers!!
- 400GB of sensitive data exposed
- Company confidential data + Source code released…

Big Data For Cybersecurity

No. 1 – Keeping up with the arms race.

Big Data For Cybersecurity

No. 2 - Massive amounts of data

Big Data For Cybersecurity

No. 3 – Making sense of what's happening, fast

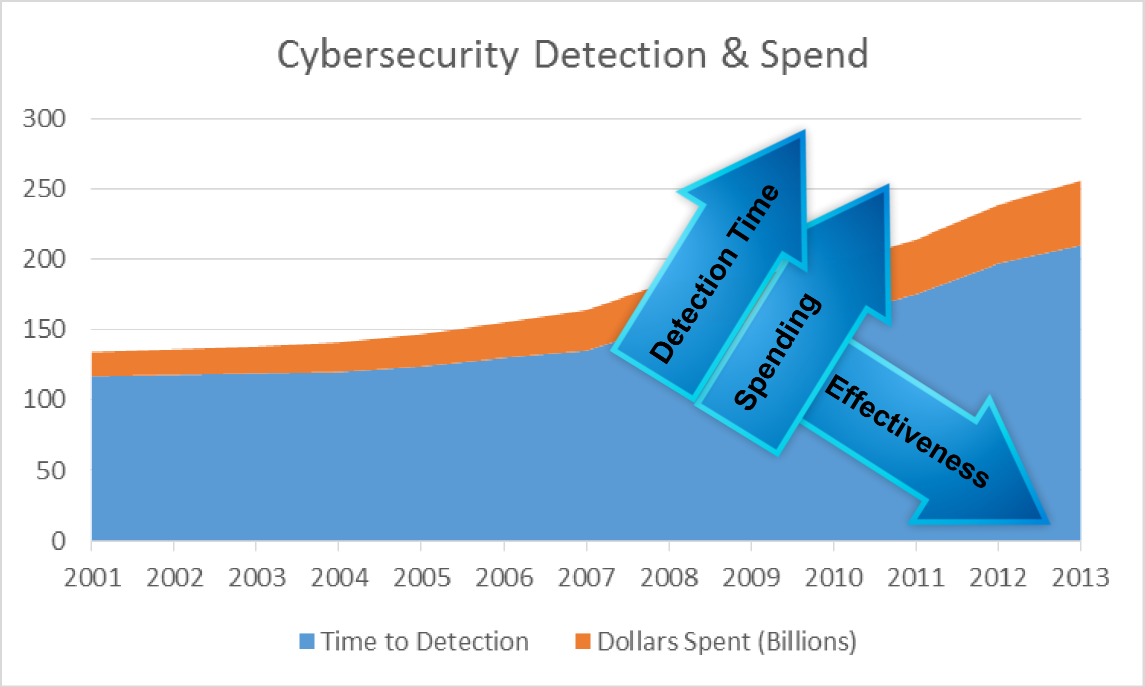
Big Data For Cybersecurity

No. 4 – Too many alerts

Big Data For Cybersecurity

No. 5 - Emerging threats

Effectiveness declines as spend increases



37% of victims discover breach internally

63% of victims were notified by an external entity

- 2% by a customer
- 4% by a business partner
- 15% by an outsourced service provider
- 42% by law enforcement

Mandiant 2013 Threat Report

The SAS Cyber Position

Why is SAS approaching this space now?

“64 percent of organizations attacked took more than 90 days to detect an intrusion**”**

- 2013 TRUSTWAVE GLOBAL SECURITY REPORT

“Average time for detection being 220 days - 35 days longer than in 2012”

- 2014 TRUSTWAVE GLOBAL SECURITY REPORT

Time to Detection increasing while global Cybersecurity spending increasing 10% annually

KEEP
CALM
&
FOLLOW
THE RULES

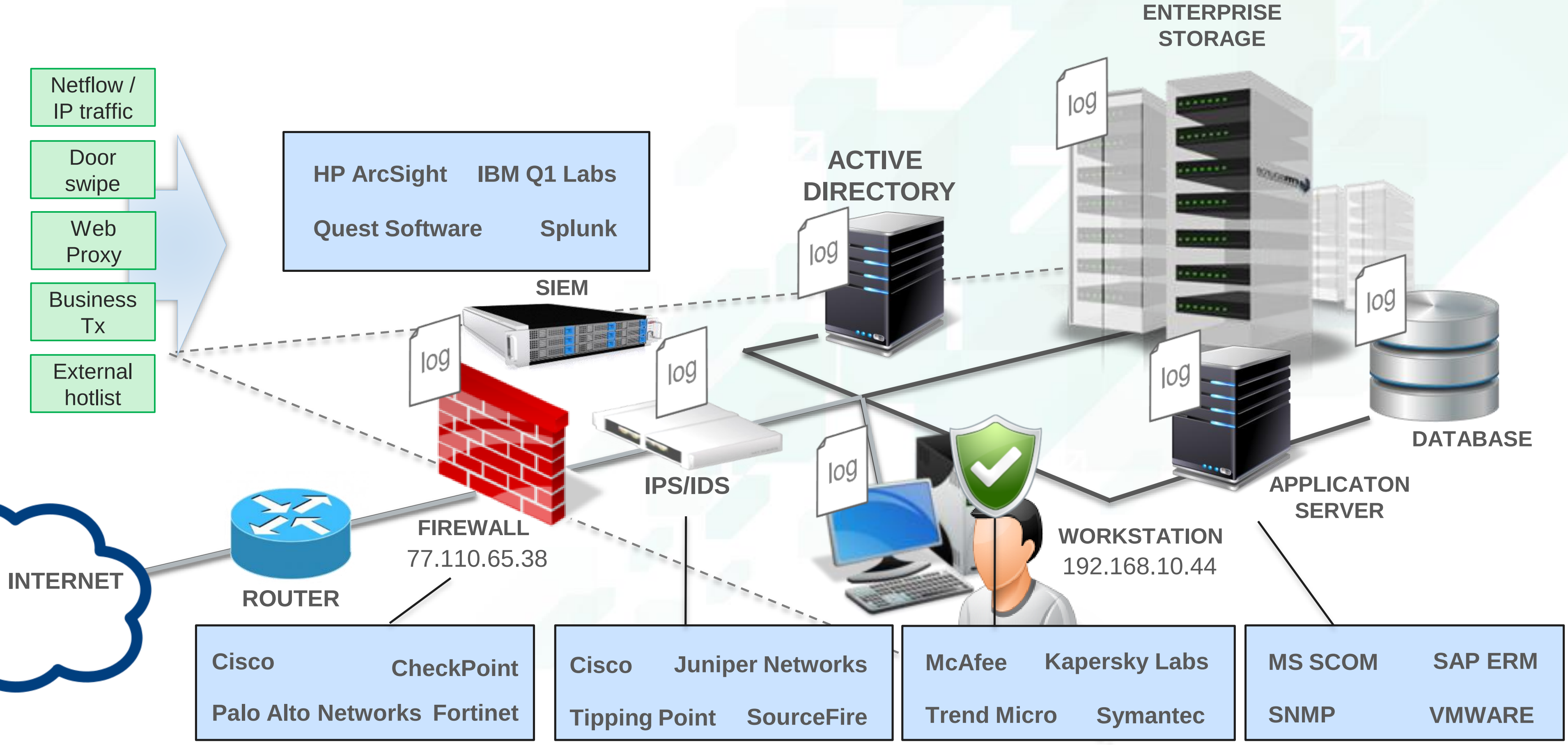
Current detection methodologies

- Intrusion Detection Systems: primarily signature based
- Intrusion Prevention Systems: primarily signature based
- Data Loss Prevention: signature and behavior based
- Anti malware solutions: signature based / easily circumvented
- Cloud Based Detection: signature based / providence questions

Output of all these systems working in concert is **significant amount of alerting and false positives** with time of detection hovering around 220 days

```
01:00:5E:00:00:01|0|'dod
internet
multicast:00:00:01'|14129568
70|1412957170|0|0|0|12|0|0|
0|0|0|0|0|0|0|0|0|0|720|0|0|0.0
0|0.00|0.00|0.00|0.00|0.00|0.
00|0.00|0.00|0.00|0.00|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|'01:00:5E:00:00:0
1'|
01:00:5E:00:00:0D|0|'dod
internet
multicast:00:00:0d'|14129552
55|1412957173|0|0|0|132|0|0
|0|0|0|0|0|0|0|0|0|0|9504|0|0|0
.00|0.00|0.00|0.00|0.00|0.00|
0.00|0.00|0.00|0.00|0.00|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|'01:00:5E:00:00:
0D'|
01:80:C2:00:00:0E|0|'reserve
d (ieee 802.1d '|
193.111.2.7|0|'193.111.2.7'|'n
s2.vdonsk.ru'|1412957133|14
12957134|49|49|2|2|370|190|
0|0|0|0|0|0|0|370|370|0|190|1
90|0|3.00|0.00|0.10|3.00|6.00
|0.00|0.19|6.00|9.00|0.00|9.0
0|0|0|0|0|370|190|0|0|0|370|0|
0|0|190|0|0|0|0|0|0|0|0|0|0|0|
192.168.0.100|0|'192.168.0.1
00'|'192.168.0.100'|
```

Existing Landscape



Netflow / IP traffic

Door swipe

Web Proxy

Business Tx

External hotlist

HP ArcSight IBM Q1 Labs

Quest Software Splunk

SIEM

ACTIVE DIRECTORY

ENTERPRISE STORAGE

DATABASE

APPLICATON SERVER

WORKSTATION
192.168.10.44

IPS/IDS

FIREWALL
77.110.65.38

ROUTER

INTERNET

Cisco CheckPoint

Palo Alto Networks Fortinet

Cisco Juniper Networks

Tipping Point SourceFire

McAfee Kapersky Labs

Trend Micro Symantec

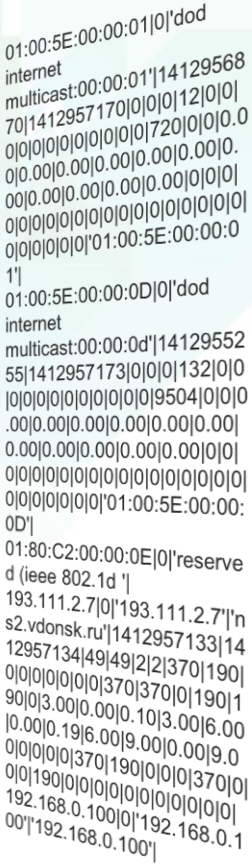
MS SCOM SAP ERM

SNMP VMWARE

Sas Detection Methodologies

- Behavior based detection algorithms
- Large scale ingest of good and bad traffic
- Enrichment: utilizes data already created in your environment
- Reduce false positives / highlight investigations of priority

This is not detective work, you don’t need to know what questions to ask before investigating. SAS provides a voice to the data

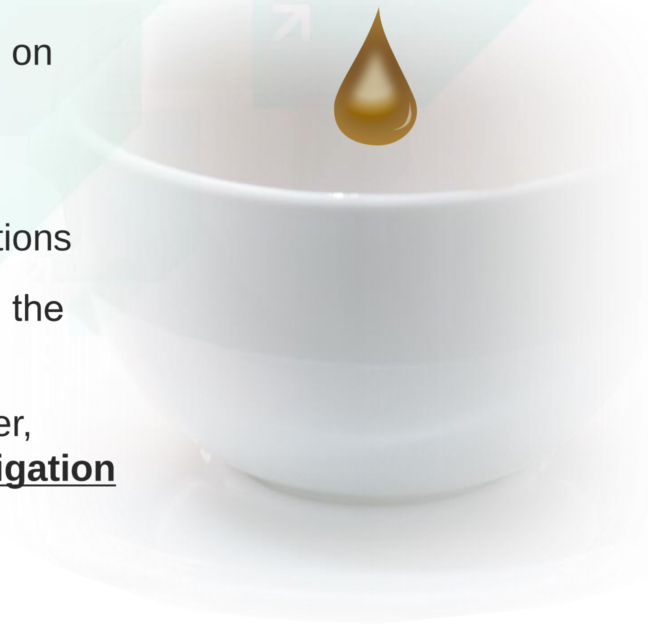


```
01:00:5E:00:00:01|0|'dod
internet
multicast:00:00:01'|14129568
70|1412957170|0|0|0|12|0|0|
0|0|0|0|0|0|0|0|0|720|0|0|0.0
0|0.00|0.00|0.00|0.00|0.00|0.
00|0.00|0.00|0.00|0.00|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|'01:00:5E:00:00:0
1'|
01:00:5E:00:00:0D|0|'dod
internet
multicast:00:00:0d'|14129552
55|1412957173|0|0|0|132|0|0
|0|0|0|0|0|0|0|0|0|0|9504|0|0|0
.00|0.00|0.00|0.00|0.00|0.00|
0.00|0.00|0.00|0.00|0.00|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|'01:00:5E:00:00:
0D'|
01:80:C2:00:00:0E|0|'reserve
d (ieee 802.1d '|
193.111.2.7|0|'193.111.2.7'|'n
s2.vdonsk.ru'|1412957133|14
12957134|49|49|2|2|370|190|
0|0|0|0|0|0|0|370|370|0|190|1
90|0|3.00|0.00|0.10|3.00|6.00
|0.00|0.19|6.00|9.00|0.00|9.0
0|0|0|0|0|370|190|0|0|0|370|0|
0|0|190|0|0|0|0|0|0|0|0|0|0|0|
192.168.0.100|0|'192.168.0.1
00'|'192.168.0.100'|
```

Think about 6.5 billion daily events

Imagine a single cup of coffee … that cup contains about a million grains of sand

- Then imagine 6,500 coffee cups of sand in front of you … that approximates the 6.5 billion daily events that SAS ingested
- SAS took those 6,500 coffee cups of sand and sorted each grain based on whether each grain connected to another grain
- SAS then enriched the grains with other security data
- SAS then analyzed the pairs of grains with a multitude of other calculations
- SAS then eliminated 6,499 coffee cups … the single remaining cup had the equivalent of a single drop of coffee
- It is this drop of coffee that we are most interested in investigating further, resembling **the few dozen IP address SAS recommended for investigation**



Behavioural Modelling

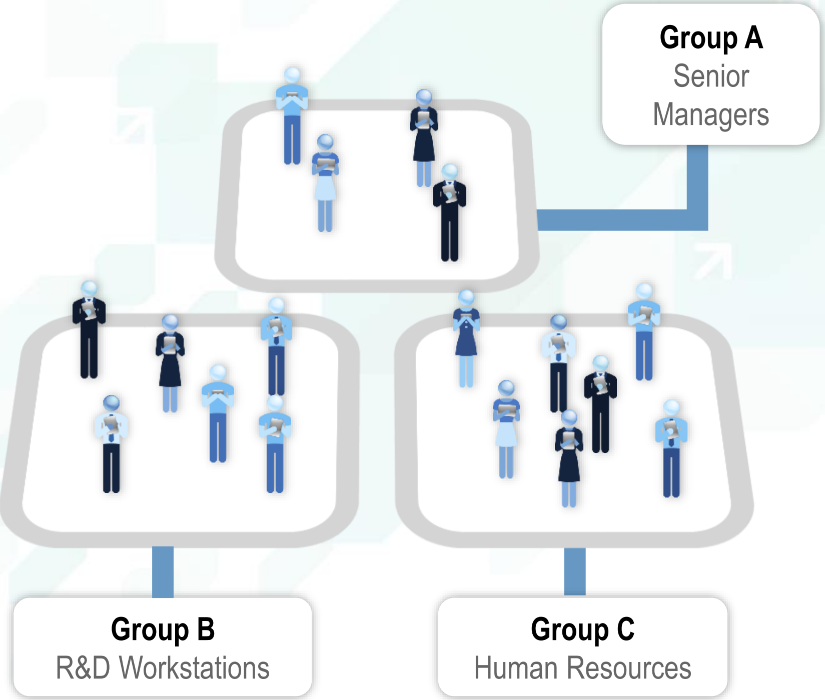
- ❑ What do people do and how do they react to different circumstances?
- ❑ What do people do normally?
- ❑ Are people doing what we want them to?

Think about 6.5 billion daily events

PEER GROUP ANALYSIS

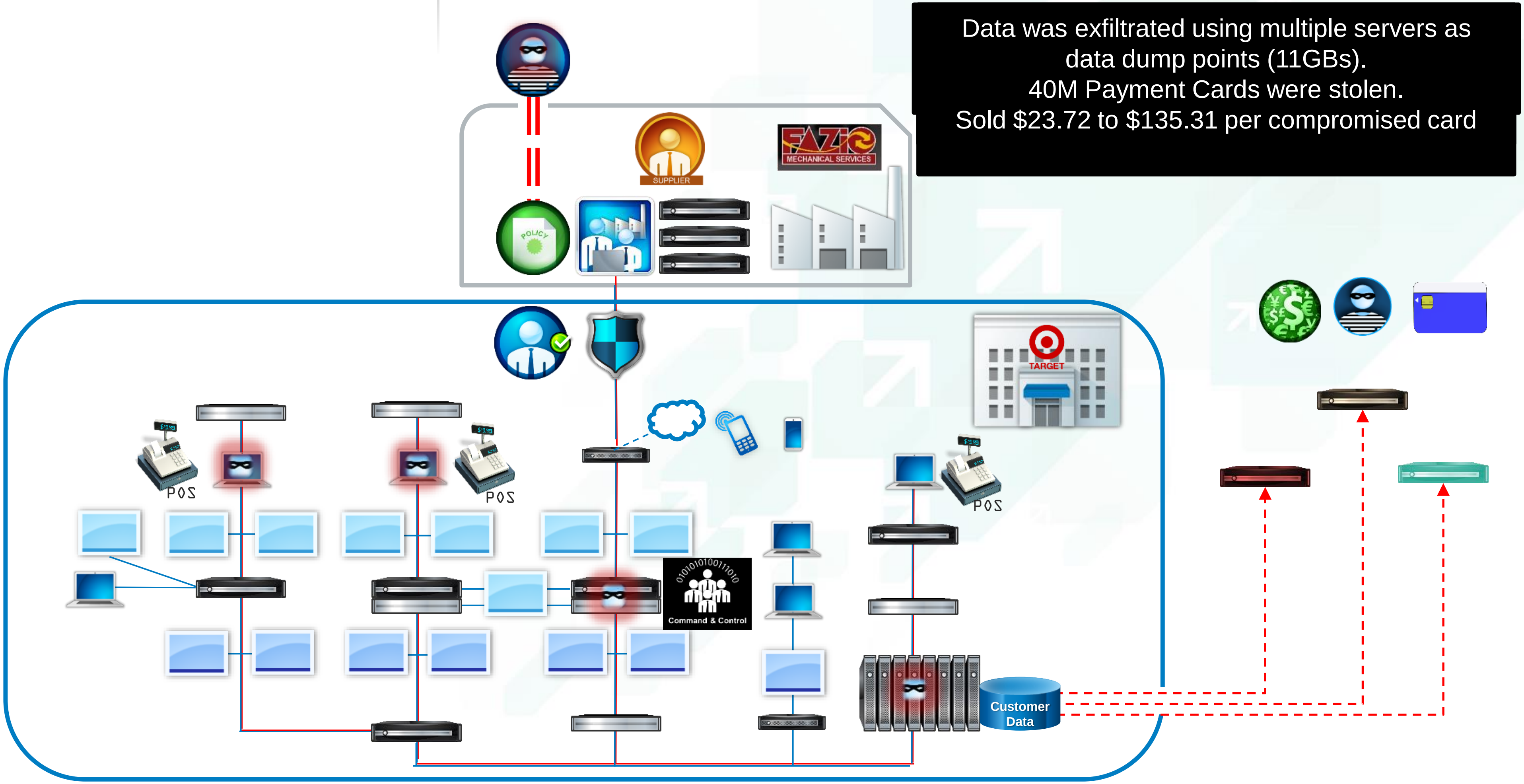
“Create groups that have similar characteristics.

A measure of how different each group is from the others.”

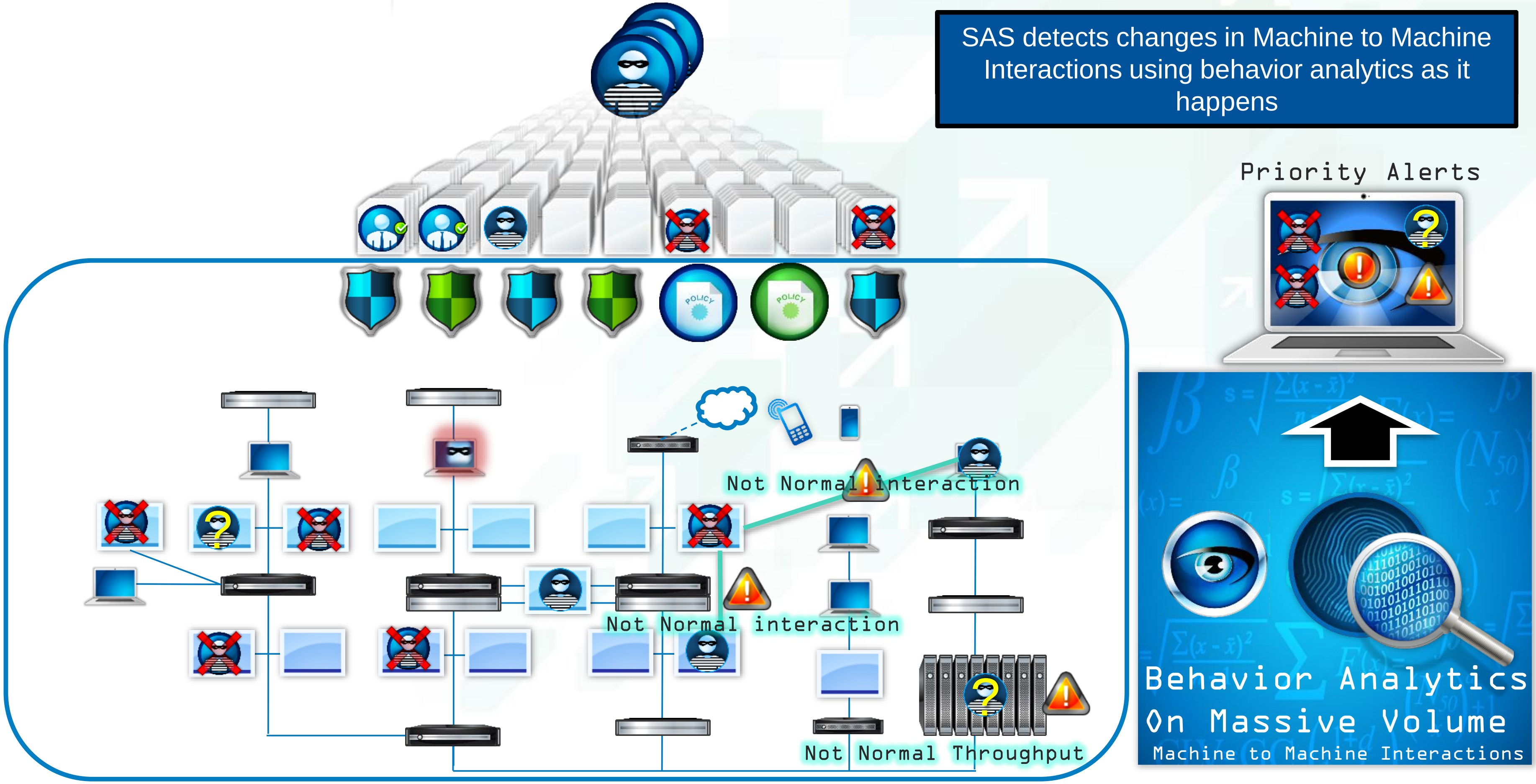


Anatomy of a sophisticated Cyber Attack

Data was exfiltrated using multiple servers as data dump points (11GBs).
40M Payment Cards were stolen.
Sold $23.72 to $135.31 per compromised card

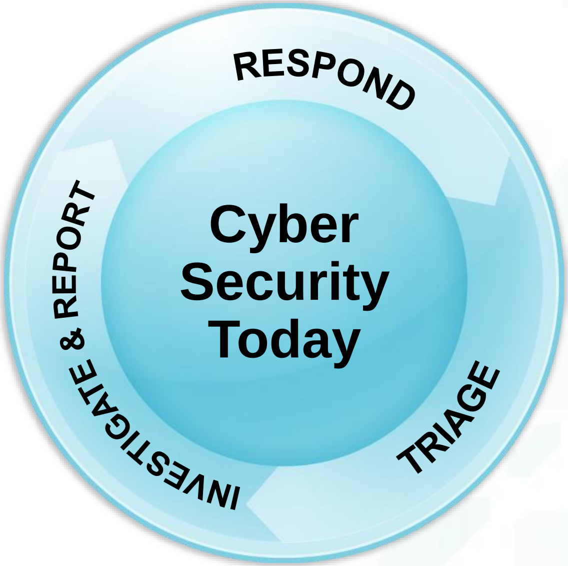


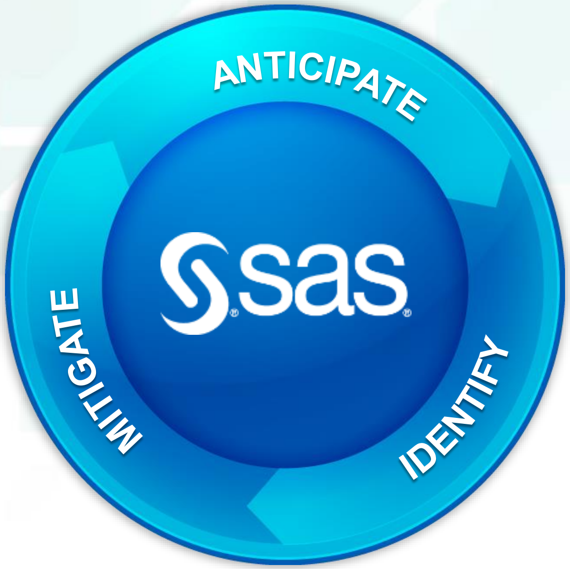
SAS behavioral Analytics Approach



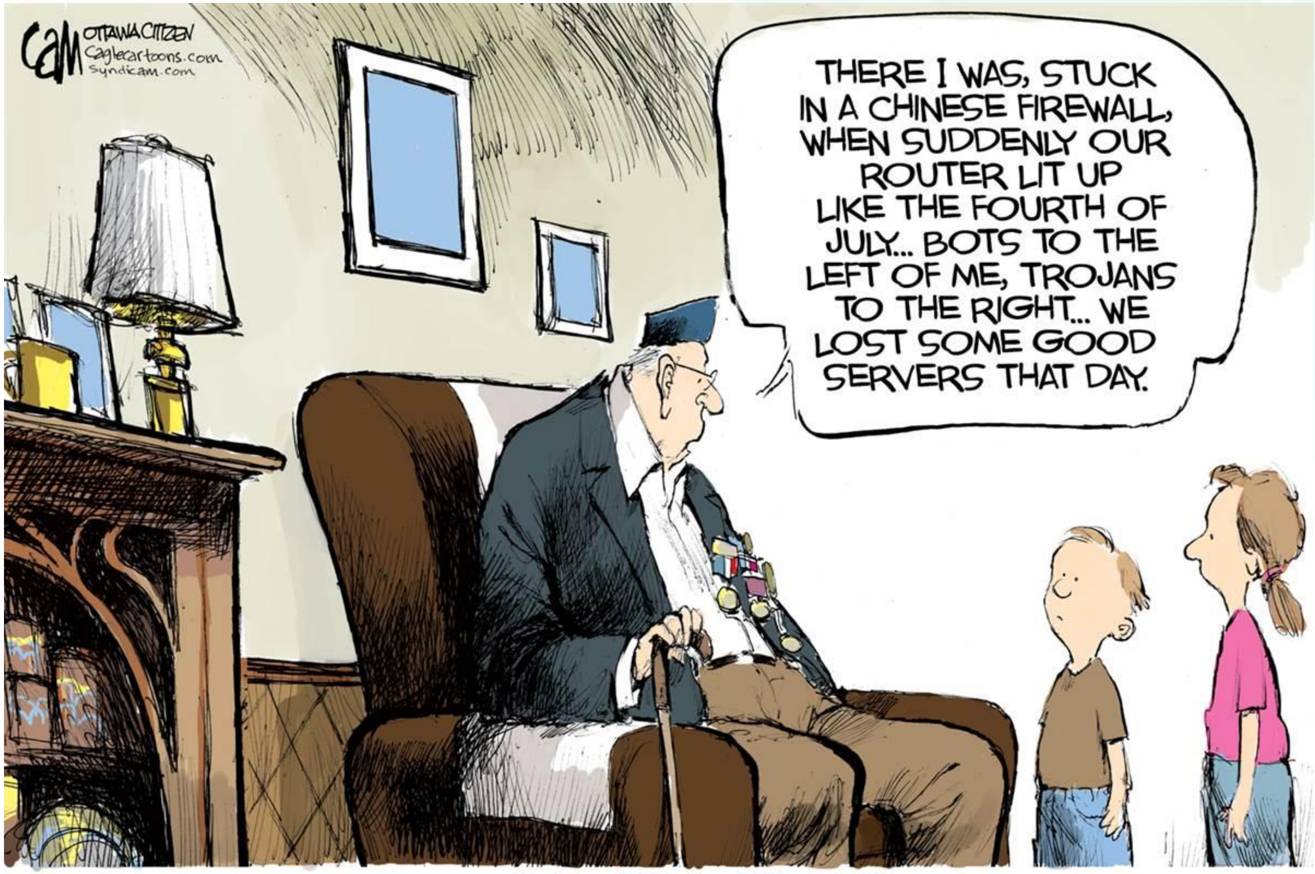
SAS detects changes in Machine to Machine Interactions using behavior analytics as it happens

Transitioning from reactive to proactive





Future War Stories...


CAM OTTAWA CITIZEN Caglecartoons.com syndicam.com
THERE I WAS, STUCK IN A CHINESE FIREWALL, WHEN SUDDENLY OUR ROUTER LIT UP LIKE THE FOURTH OF JULY... BOTS TO THE LEFT OF ME, TROJANS TO THE RIGHT... WE LOST SOME GOOD SERVERS THAT DAY.

FUTURE WAR STORIES

SZKOŁA GŁÓWNA HANDLOWA W WARSZAWIE

The Third International Workshop

Advanced Analytics and Data Science

Partner

SAS THE POWER TO KNOW.

Sponsor

BGK BANK GOSPODARSTWA KRAJOWEGO

Media Partners

COMPUTERWORLD Polska

Harvard Business Review POLSKA

ICAN INSTITUTE

ITWIZ TO CO ISTOTNE W IT

MANAGEMENT BUSINESS ASSOCIATION MANAGER