

# **SECURITATEA IN SISTEMELE IT**

---

## **INTRODUCTION TO INFORMATION SECURITY**

Sl.dr.ing Tudor Mihai BLAGA  
[tudor.blaga@com.utcluj.ro](mailto:tudor.blaga@com.utcluj.ro)



- Orar
- Prezenta curs – “strongly recommended”
- Prezenta laborator 80/20%
- Adrese email – grup email
- Nota = miniproiect + examen (grila)
- Sustinere miniproiect - data

- The Team
  - Why Information Security?
  - What is Information Security?
  - Course Topics
  - InfoSec Resources
- 

# AGENDA

- **Vasile Dorca** (Betfair)
  - **Mihai Andreescu** (Betfair)
  - **Aurelian Caliman** (Betfair)
  - **Gabriel Lazar** (UTCN)
  - **Cristian Serban** (Betfair) & **Lucian Suta** (Defline Security)
  - **Adrian Chioreanu** (Betfair)
  - **Dan Lutas** (BitDefender)
  - **Tudor Blaga** (UTCN/Betfair)
- 

# THE TEAM



## Vasile Dorca

Head of Country Management, Information Security & Governance at Betfair

Romania | Computer Software

Current      Betfair

Previous     Nokia Romania, Securitas Security Services USA, Inc., Folda Security Group

Education    Universitatea Tehnică din Cluj-Napoca

As Country Manager in Information Security and Governance, I work for a team called Information & Technology Risk Management who define and implement the framework behind the identification and management of information security and technology risks across Betfair. We provide advice and guidance on risk assessment and mitigation as well as risk management training. We are spread across Australia, Portugal, Romania, the UK and the USA..

We are a part of Information Security and Governance who take care of all aspects of security right across our business. That means risk management, setting and putting in place policies and standards, seeing to it that we meet all the latest security legislation and standards, plus managing security incidents and investigations.

Betfair is one of the world's largest international online sports betting providers and pioneered the first successful Betting Exchange in 2000. The Betting Exchange, where customers come together in order to bet at odds sought by themselves or offered by other customers, has eliminated the need for a traditional bookmaker. Driven by world-leading technology the company now processes over five million transactions a day from its three million registered customers around the world. In addition to sports betting, Betfair offers a portfolio of innovative products including casino, exchange games, arcade and poker.

## Dan Lutas

Senior Research Lead at Bitdefender  
Romania | Information Technology and Services

Current      Bitdefender  
Previous     BitDefender, Net Brinel  
Education    Universitatea Tehnică din Cluj-Napoca

### Information Security Manager

Bitdefender

June 2013 – Present (1 year 5 months) | Bitdefender Cluj Napoca

B

### Senior Research Lead

Bitdefender

July 2012 – Present (2 years 4 months)

B

### Proactivity And Kernel Research Software Development Lead

BitDefender

March 2009 – July 2012 (3 years 5 months)

B

### Proactivity And Kernel Research Software Developer

BitDefender

July 2007 – February 2009 (1 year 8 months)

Developing kernel-mode drivers for the Active Virus Control technology

B

### Virus Researcher

BitDefender

May 2005 – June 2007 (2 years 2 months)

A virus analyst disassembles and analyzes new viruses in order to understand the way they function and spread.

B

Specialties: Windows Drivers Development (FS Minifilters, WDM, KMDF Device Drivers)  
Crash dump analysis / Windows Kernel Debugging  
x86 Architecture, Hardware Assisted Virtualization (both VMX and SVM)

InfoSec : Holding CISSP (til September 2014), CEHv7 Certifications, CISA (til April 2015), OSCP



# Mihai Andreeescu

SecOps Manager

Romania | Information Technology and Services

Current N/A

Previous EY, Dell SecureWorks, Dell

Education Universitatea Constantin Brancoveanu

Follow

## SecOps Manager

N/A

August 2016 – Present (3 months)



## Cybersecurity Manager

EY

October 2015 – August 2016 (11 months)



## Sr. Information Security Consultant

EY

January 2015 – October 2015 (10 months)



## Security Systems Sr. Analyst

Dell SecureWorks

May 2014 – December 2014 (8 months)



## System Administrator Analyst

Dell

December 2012 – May 2014 (1 year 6 months)

## Splunk Certified Architect

Splunk

## System & Network Administrator

Self-employed

2009 – November 2012 (3 years)



## FireEye Junior Systems Engineer

FireEye, Inc.

## System Administrator

Class IT Outsourcing

May 2008 – October 2009 (1 year 6 months) | Bucharest, Romania

## SourceFire Certified Security Engineer (SFCSE)

Sourcefire



## QualysGuard Vulnerability Management Certified Specialist

Qualys



## ITIL V3 Foundation

EXIN



**A** **Information Security Risk Manager**

Info Betfair

Ror June 2015 – Present (1 year 5 months)



Prev

**LIMS Implementation Specialist**

Edu BGASoft Inc

2014 – 2015 (1 year)

**COO**

HyperTalk



August 2012 – February 2014 (1 year 7 months) | Cluj County, Romania



HyperTalk – Bringing partners together. HyperTalk Systems offers professional video communications services through its novel web platform that supports web meetings, webinars and online training sessions.

My mission at Hypertalk Systems includes: Supervision & prioritization of short and long term operations, Risk management, Planning & benchmarking, Manage resources, Identifying, assessing & prioritizing business opportunities.

**Assoc Lecturer (MSc Programmes) Project Management**

Technical University of Cluj-Napoca

2011 – January 2014 (3 years) | Cluj County, Romania

eStart MSc Programmes - Project Management classes

**Researcher, PhD**

RESIN part of UTCN

September 2009 – June 2013 (3 years 10 months)

**Post PhD**

UTCN

2010 – 2013 (3 years)



## Aurelian Caliman

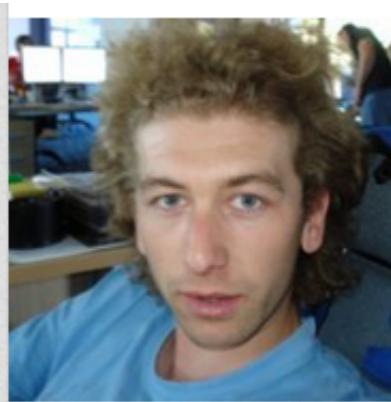
1st

Senior System Engineer - Windows Server Platform,  
Information Technology at Betfair Romania  
Cluj County, Romania | Information Technology and Services

Current      Betfair  
Previous     Betfair, Jolidon Import Export  
Education    Universitatea Tehnică din Cluj-Napoca

[Send a message](#)500+  
connections

- Microsoft® Certified Solutions Associate (MCSA) - Windows Server® 2008
- ITIL Foundation Examination Version 3
- Certified ScrumMaster by the Scrum Alliance, Inc.
- Certified Kepner-Tregoe Resolve Workshop
- Kepner-Tregoe (<http://www.kepner-tregoe.com/>), License 798041
- Microsoft® Certified IT Professional Enterprise Administrator (MCITP) - Windows Server® 2008
- Microsoft® Certified IT Professional Server Administrator (MCITP) - Windows Server® 2008
- Microsoft® Certified Technology Specialist (MCTS) - Windows Server® 2008 R2, Server Virtualization
- Microsoft® Certified Technology Specialist (MCTS) - Windows Server® 2008 R2, Desktop Virtualization
- Microsoft® Certified System Administrator: Messaging (MCSA) - Microsoft Windows Server® 2003
- Microsoft® Certified Technology Specialist (MCTS) - Windows Server® 2008 Active Directory, Configuration
- Microsoft® Certified Technology Specialist (MCTS) - Windows Server® 2008 Network Infrastructure, Configuration
- Microsoft® Certified Technology Specialist (MCTS) - Windows Server® 2008 Applications Infrastructure, Configuration
- Microsoft® Certified Technology Specialist (MCTS) - Windows® 7, Configuration
- Microsoft® Certified Professional (MCP) - MCP 2.0 - Certified Professional



## Cristian Serban

Application Security at Betfair

Romania | Gambling & Casinos

1st

Previous William Hill, Betfair, Sente Software  
Education Universitate Tehnică din Cluj-Napoca

Send a message



266

connections



### Application Security

Betfair

August 2014 – Present (3 months)



### Application Security Specialist

William Hill

January 2013 – July 2014 (1 year 7 months) | Gibraltar

Responsible for software security developed in 3 development offices.

Coordinate security testing of wide range of products, mobile, web internal and externally developed.

Implement SDLC in Agile projects by training Security Champions in each dev team and include automated security testing in continuous delivery environment.



### Senior Application Security Analyst

Betfair

June 2007 – January 2013 (5 years 8 months) | Cluj-Napoca

- Betfair is a bluechip world leading online betting exchange and gaming company, performing over 6.5 mil transactions/day, >4 mil customers
- Application Security Analyst member of the global Information Security team, responsible for protecting customers money and company reputation
- Responsible for secure software development of ~100 developers in Romania office, embedded in agile scrum teams
- Worked on security assessments, SDLC, fraud detection, incident response, penetration testing, code reviews, design reviews, delivering trainings to developers.
- Also involved in PCI Certification, ISO 27001, third party assessments

## Lucian Suta

Development Security Advisor

Cluj County, Romania | Computer Software

Current Betfair

Previous Betfair, Latitudini International, Qualcomm, Inc.

Education University of California, San Diego

### Development Security Advisor

Betfair

August 2014 – Present (3 months) | Cluj-Napoca, Romania



### Application Security Analyst

Betfair

July 2011 – August 2014 (3 years 2 months) | Cluj-Napoca, Romania



### Cofounder

Latitudini International

October 2008 – June 2011 (2 years 9 months)

Designing and implementing an end-to-end software solution for the hospitality and service industries.



### Staff Engineer

Qualcomm, Inc.

October 2004 – June 2007 (2 years 9 months)

### Senior Engineer

Incisix, Inc.

March 2004 – October 2004 (8 months)



### Senior Engineer

Enosys Software, Inc.

April 2000 – March 2003 (3 years)

### Engineering Intern

Qualcomm, Inc.

June 1998 – April 2000 (1 year 11 months)



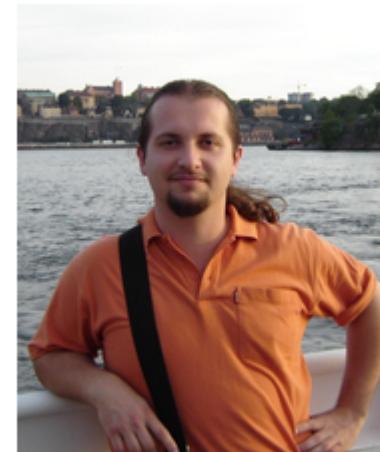
### Gabriel Lazar

Network Administrator at Technical University of Cluj-Napoca  
Romania | Telecommunications

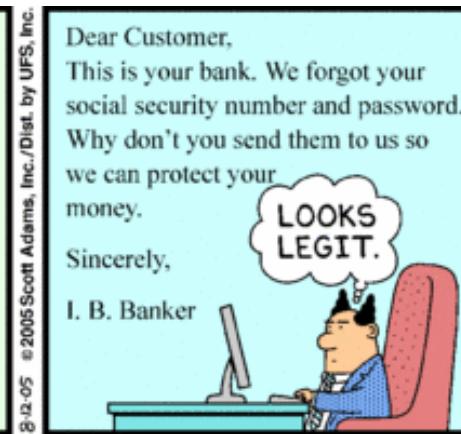
### Tudor Mihai Blaga

Security Analyst at Betfair & Assistant Professor at  
TUCN  
Cluj County, Romania | Education Management

Current      [Betfair, UTCN](#)  
Previous    [Betfair, UTCN](#)  
Education    [SANS London Summer 2014](#)



# WHY INFORMATION SECURITY?



# Why Information Security?

- ▶ Every **1min** a host accesses a malicious website
- ▶ Every **9mins** a High Risk application is being used
- ▶ Every **27mins** unknown malware is downloaded
- ▶ Every **49mins** sensitive data is sent outside the organization
- ▶ Every **24h** a host is infected with a bot

<http://www.checkpoint.com/campaigns/securitycheckup/index.html>

**AN AVERAGE DAY  
IN AN ENTERPRISE  
ORGANIZATION**

Every **1 min** a host  
accesses a malicious website

Every **3 mins** a bot is  
communicating with its  
command and control center

Every **9 mins** a High Risk  
application is being used

Every **10 mins**  
a known malware is  
being downloaded

Every **27 mins**  
an unknown malware is  
being downloaded

Every **49 mins**  
sensitive data is sent  
outside the organization

Every **24h** a host is  
infected with a bot



<http://www.checkpoint.com/campaigns/securitycheckup/index.html>

BREACH LEVEL INDEX CALCULATE YOUR RISK SCORE 

Home Breach Database Risk Assessment Learn More Contact Us Report a Breach

RECORDS LOST: SINCE 2013

2,286,460,586

RECENT DATA BREACHES

OCTOBER 2: JPMorgan Chase 1,000,000 Records	OCTOBER 1: Pima City School District 500 records	OCTOBER 1: Hong Kong Citizens Unknown Records	SEPTEMBER 30: Lincoln Prairie Elementary School Unknown Records
---	--	---	--

<http://www.breachlevelindex.com>

Home

Breach Database

Risk Assessment

Learn More

Contact Us

Report a Breach

RECORDS LOST: SINCE 2013

3,338,874,326

RECENT DATA BREACHES

**SEPTEMBER 5:**

*Bank of America in Goffstown  
Unknown Records*

**SEPTEMBER 4:**

*Human Rights Commission 1 Records*

**SEPTEMBER 3:**

*HMRC  
500 Records*

**SEPTEMBER 3:**

*Aurora ATM  
Unknown Records*



## TOTAL RECORDS LOST BY MONTH IN

2014

AUG: 1,229,178,182

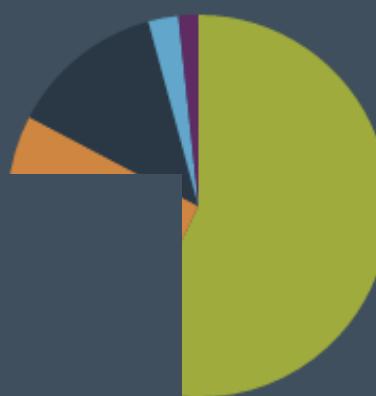


## TOP DATA BREACH INCIDENTS BY SOURCE

Calculate by date range, hover over pie chart to display totals.

MM/DD/YY ▾

MM/DD/YY ▾



## TOP DATA BREACH RECORDS BY INDUSTRY

Calculate by date range, hover over pie chart to display totals.

MM/DD/YY ▾ MM/DD/YY ▾



- 0,814,943 Records
- Retail ( 35.76% )
  - Technology ( 31.49% )
  - Financial ( 11.14% )
  - Government ( 9.25% )
  - Other ( 9.04% )
  - Healthcare ( 3.32% )

<http://www.breachlevelindex.com/>



I FIND YOUR LACK OF  
PASSWORD STRENGTH  
DISTURBING



# DOCTOR FUN

17 May 2006



"Yeah - we used to call them cell phones."

Copyright © 2006 David Farley, d-farley@ibiblio.org  
<http://ibiblio.org/Dave/drfun.html>

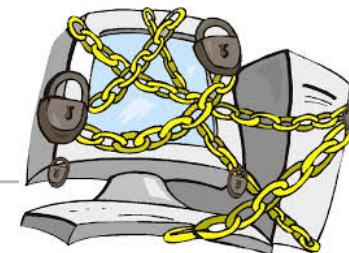
This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.

# WHAT IS INFORMATION SECURITY?



## Information security

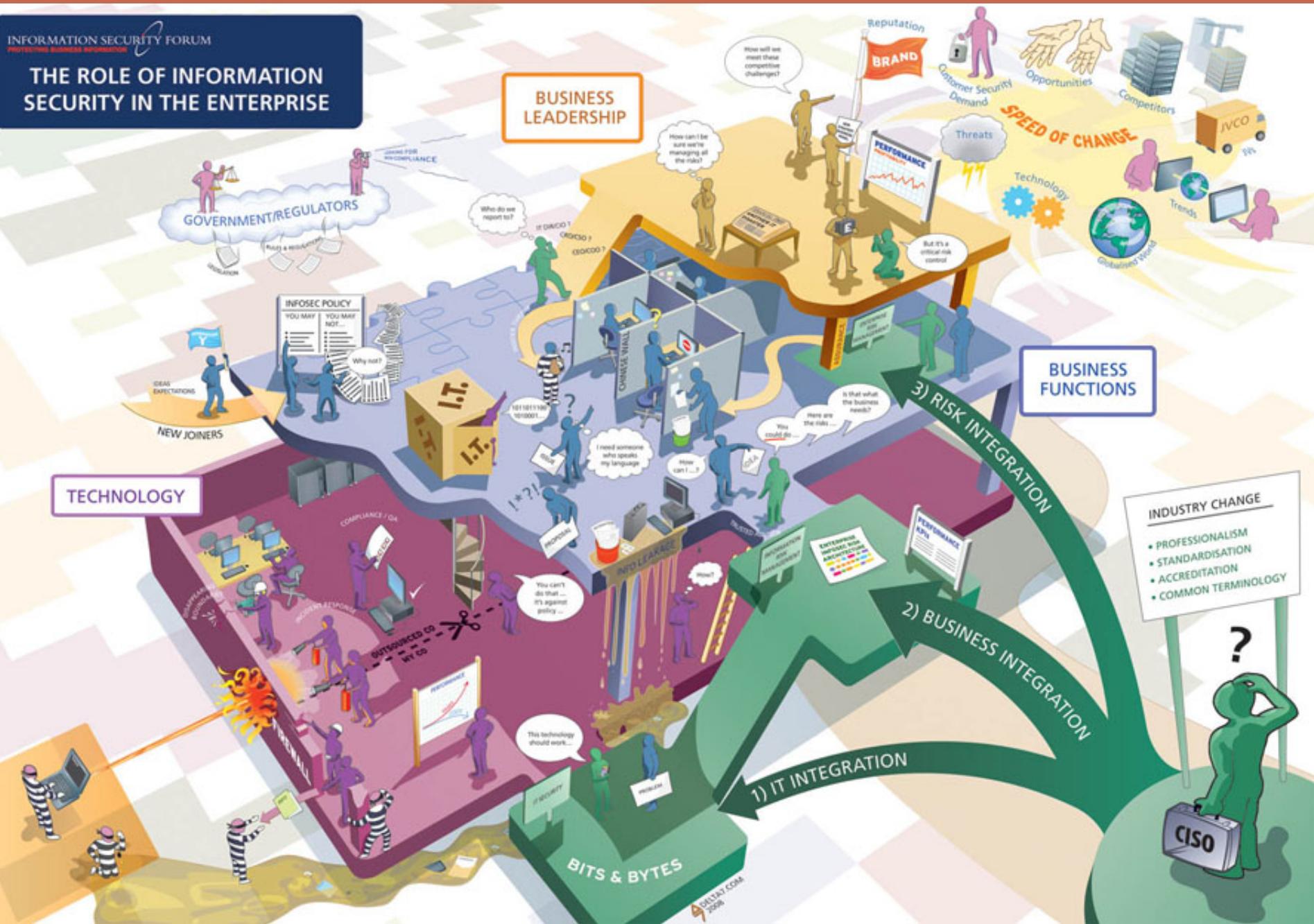
From Wikipedia, the free encyclopedia



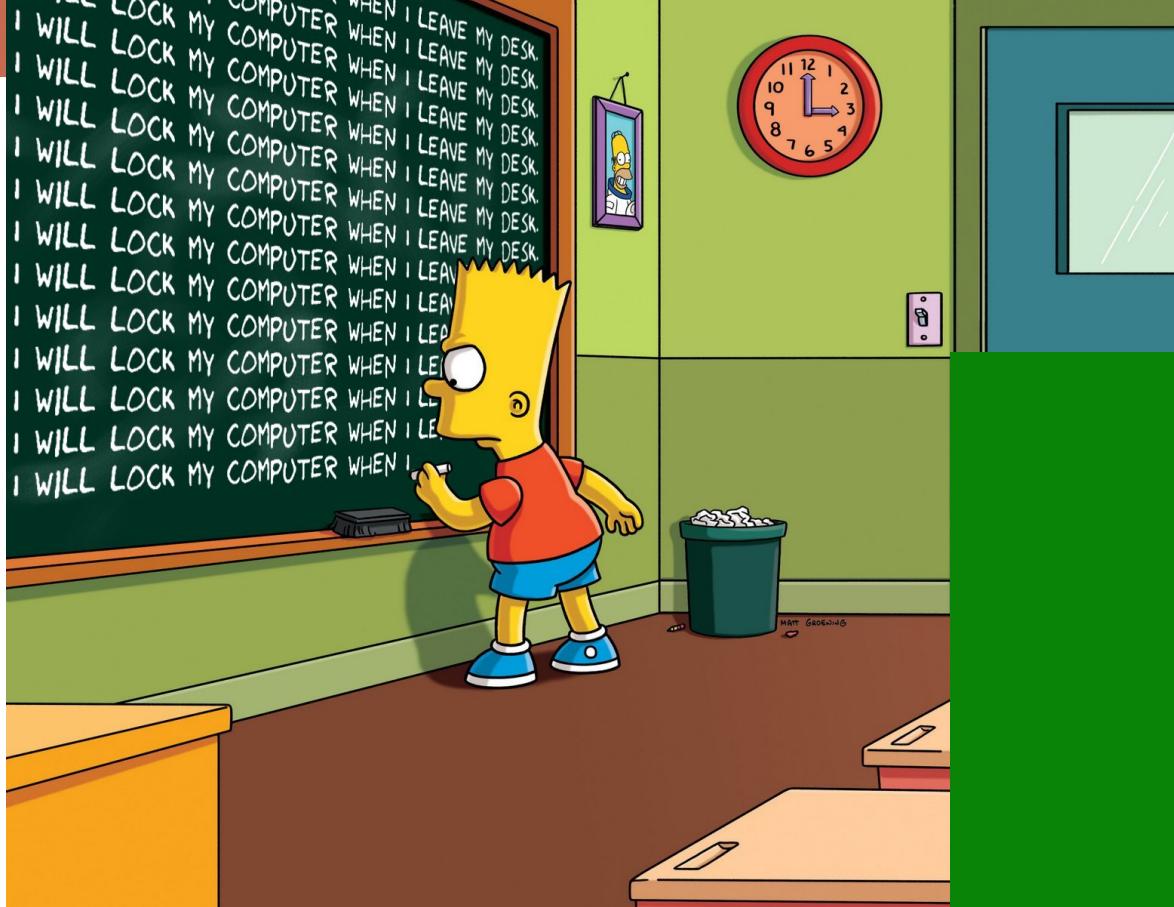
**Information security**, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.)



## THE ROLE OF INFORMATION SECURITY IN THE ENTERPRISE



- INDUSTRY CHANGE**
- PROFESSIONALISM
  - STANDARDISATION
  - ACCREDITATION
  - COMMON TERMINOLOGY



KEEP  
CALM  
AND  
LOCK YOUR  
COMPUTER

- Defense-in-Depth
  - Incident Handling
  - Network Security
  - Windows/Linux Security
  - Web App Security
  - Malware
  - Risk Management/ISO27001
  - Security Awareness
- 

# COURSE TOPICS

# INFOSEC RESOURCES

---

News, blogs, vendors, webinars, training ...

# The Register®

Data Centre Software Networks Security Business Hardware Science

**Sir Tim Berners-Lee defends decision not to bake security into www**

**IP Expo** 'The idea that privacy is dead is hopelessly sad'

John Leyden, 08 Oct 12:24

38

**Chatting to Al Qaeda? Try not to do that – Ex spy chief defends post-Snowden NSA**

Everyone spies but 'someone has to lead' – Keith Alexander

Darren Pauli, 08 Oct 12:02

32

**Credit card thieves setting up safe seller certifications**

**Breakpoint** Researchers hit Tor, find sophisticated self-regulating market

Darren Pauli, 08 Oct 05:32

**Adobe spies on reading habits over unencrypted web because your 'privacy is important'**

Is Adobe facing its Sony rootkit moment?

Iain Thomson, 08 Oct 00:39

83

**Mandiant to probe gaps in rusty unpatchable utility systems**

Says attackers may only exploit ICS hooks during WAR

Darren Pauli, 08 Oct 05:02

**Revealed: Malware that forces weak ATMs to spit out 'ALL THE CASH'**

**Video** Banks, lock down your cash machines

John Leyden, 08 Oct 09:55

73

**What's happened since Beijing's hacker unit was exposed? Nothing**

Snowden gets PLA 61398 off the hook, but it's now hacking harder than ever

Darren Pauli, 08 Oct 01:02

11

**Adobe spies on readers: 'EVERY page you turn, EVERY book you own' leaked back to base**

**Updated** App sends data over the net unencrypted

Iain Thomson, 07 Oct 18:10

74

**Aussie builds contactless card cloner app, shops at Woolies with fake card**

Pro tip: public transport is a great place to scan for card credentials

Darren Pauli, 07 Oct 22:50

11

# Krebs on Security

In-depth security news and investigation

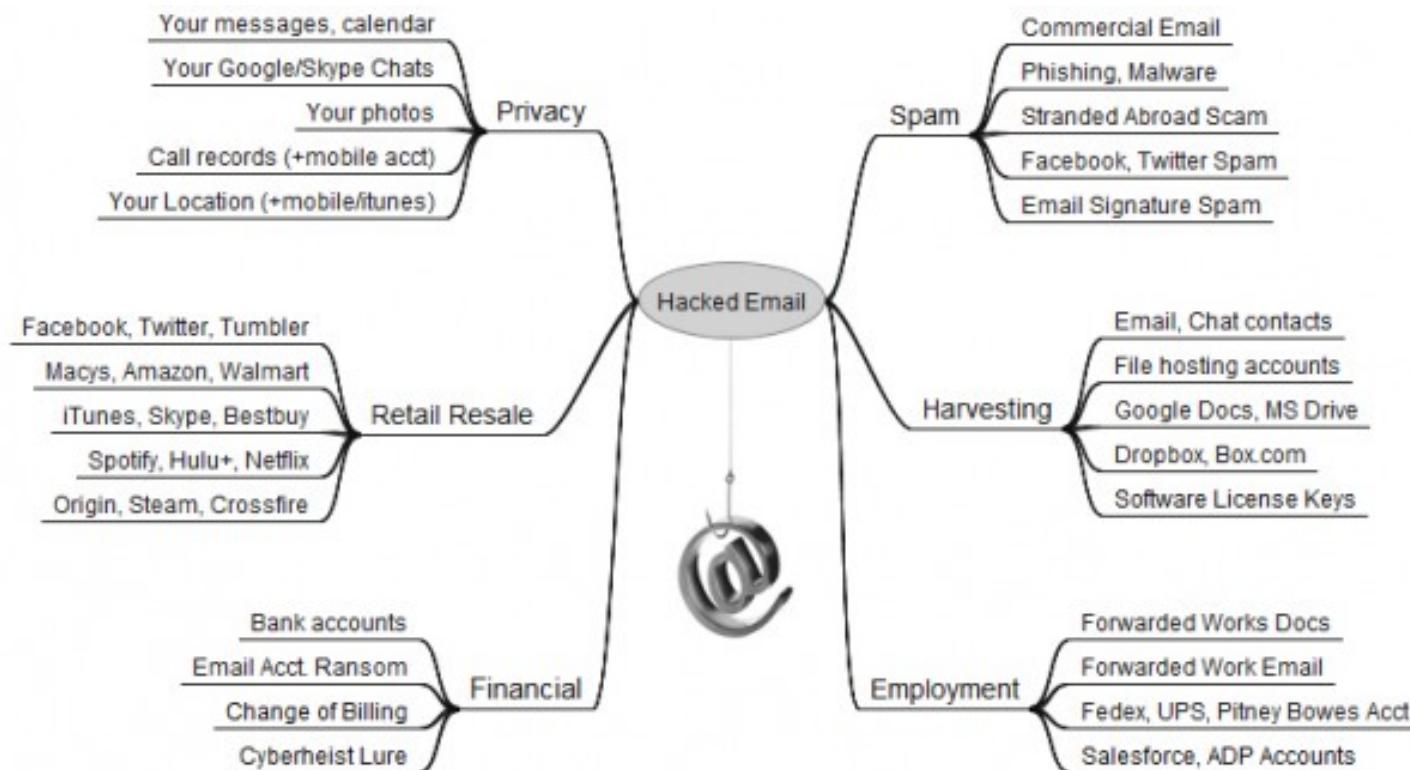


## 10 The Value of a Hacked Email Account

JUN 13



One of the most-viewed stories on this site is a [blog post+graphic](#) that I put together last year to illustrate the ways that bad guys can monetize hacked computers. But just as folks who don't bank online or sto someone would want to they have invested in th thieves.



# naked security

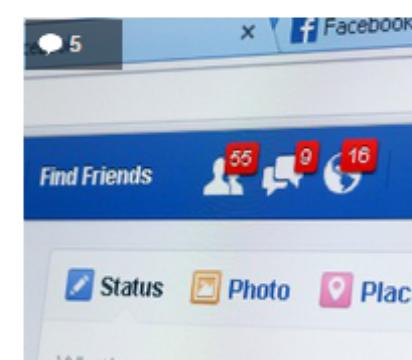
Award-winning news, opinion, advice and research from **SOPHOS**



malware mac facebook android vulnerability data loss privacy more... search articles



**SOPHOS**  
chetchat



Adobe will update e-reader to mop up clear-text data spillage

Twitter sues US federal agencies in attempt to remove the gag around surveillance

SSCC 168 - Amaze your friends by ruining all their USB drives! [PODCAST]

DEA agent steals woman's identity and photos to lure in suspects on Facebook

## Latest Articles

**Adobe will update e-reader to mop up clear-text data spillage**



Naked Security  
from Sophos

Like 251,135

# InfoSec Resources

- <http://www.theregister.co.uk/security/>
- <http://krebsonsecurity.com/>
- <http://nakedsecurity.sophos.com/>
- <https://isc.sans.edu/>
- <http://slashdot.org/stories/security>
- <http://arstechnica.com/security/>
- <http://www.darkreading.com/>
- <http://thehackernews.com/>

# InfoSec Resources

- <http://malware.dontneedcoffee.com/>
- <http://www.infosecurity-magazine.com/>
- <http://threatpost.com/>
- <http://www.h-online.com/security/>
- <http://www.us-cert.gov/>
- <http://blogs.mcafee.com/>
- <http://blog.trendmicro.com/>
- <http://www.f-secure.com/>
- <https://www.brighttalk.com/community/it-security>

# InfoSec Training/Certification

- <http://www.sans.org>
- <http://www.eccouncil.org>
- <http://www.offensive-security.com>



- <https://www.isc2.org/>



# Certified Information Systems Security Professional

<https://www.youtube.com/watch?v=whEWE6WC1Ew>

# FUN

- [https://www.youtube.com/watch?v=Fm6Qe\\_uUuk4](https://www.youtube.com/watch?v=Fm6Qe_uUuk4)

# **SECURITATEA IN SISTEMELE IT**

---

## **DEFENCE-IN-DEPTH**

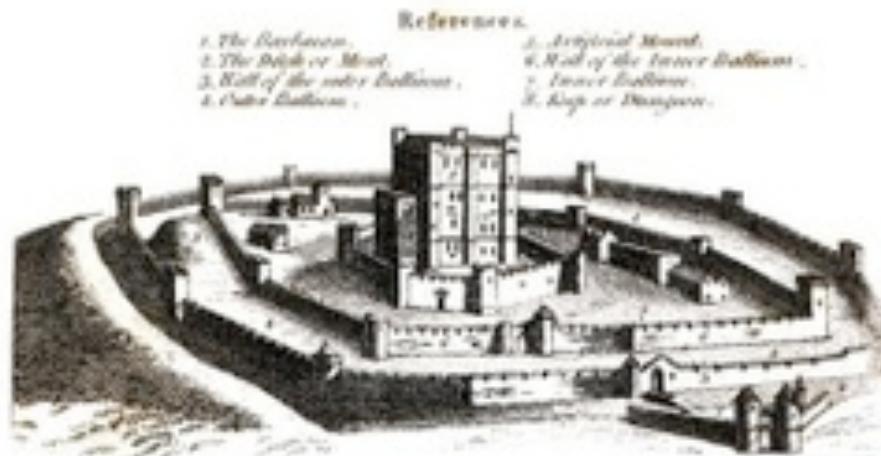
Sl.dr.ing Tudor Mihai BLAGA

- **What is Defence-in-Depth?**
  - **Risk = Threat x Vulnerability**
  - **DiD Approaches**
  - **Information Security Process**  
**(Prevention, Detection and Response)**
  - **SANS 20 Critical Controls**
- 

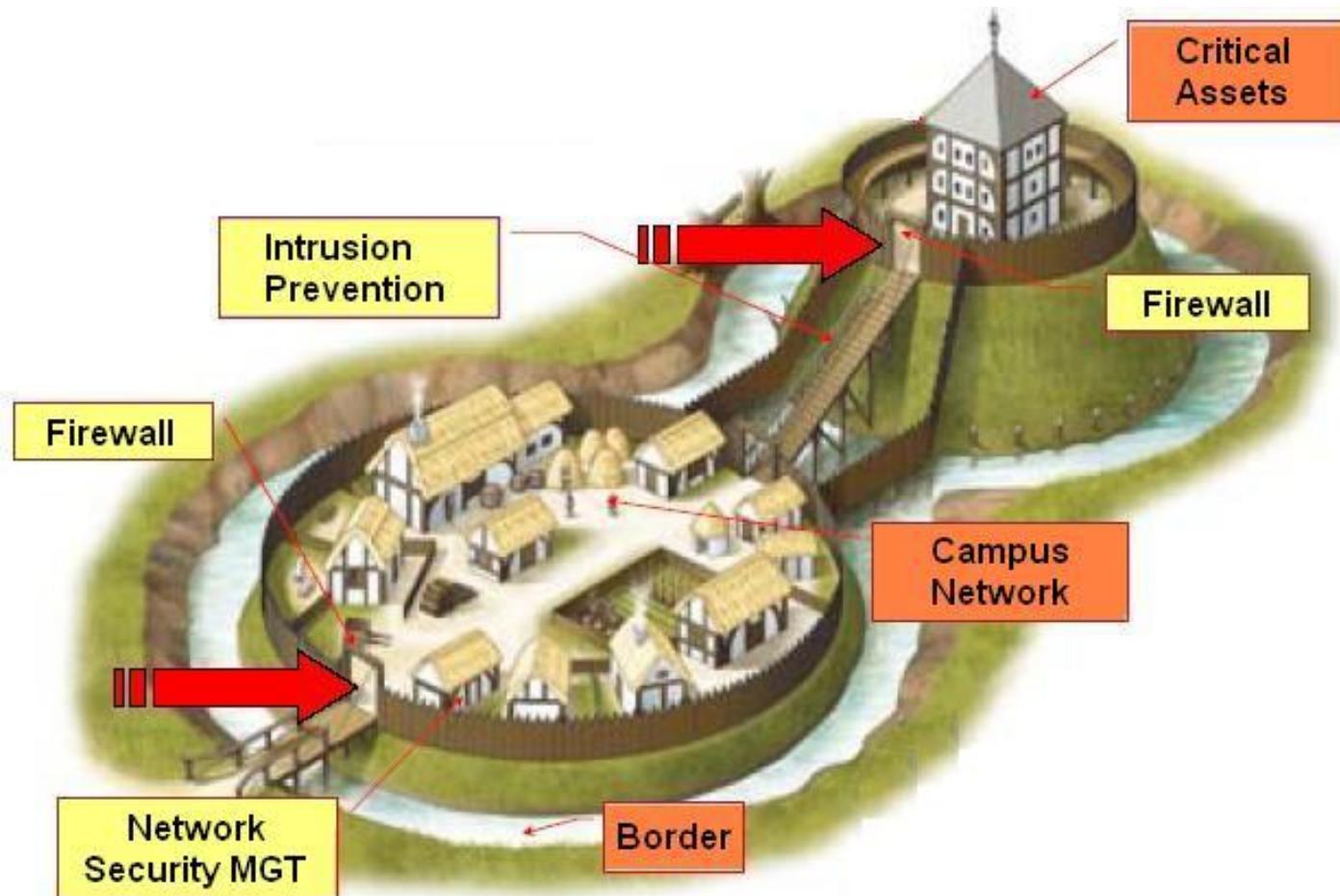
# AGENDA

# WHAT IS DEFENCE-IN-DEPTH?

---



# What is Defence-in-Depth? (1)



# What is DiD? (2)



# What is DiD? (3)



# What is DiD? (4)

- Security - no bullet proof solution, product, ...
- Any of the protection layers might fail
- **MULTIPLE LAYERS ARE NEEDED**

⇒ **Defence-in-Depth**

- Security measure = wide range of controls
  - Prevention
  - Detection
  - Response (Incident Handling)
- “Prevention is ideal but Detection is a must”

# What is DiD?

- **Defense in Depth** (also known as **Castle Approach**) is an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of *personnel, procedural, technical* and *physical* for the duration of the system's life cycle.

# RISK-THREAT-VULNERABILITY

---

Copyright 2006 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**"No fingerprints, no picture ID, no Social Security number.  
I'm afraid your baby presents a serious security risk."**

# Risk = key focus of Security

- Security = managing risk to your critical assets
- Security is basically an exercise in loss reduction
- Impossible to totally eliminate risk => residual risk
- Risk is the probability of a threat crossing or touching a vulnerability
- Risk is managed by utilizing defense-in-depth (DiD)
- Risk = threat x vulnerabilities

# RISK - CIA

- Confidentiality / Disclosure
- Integrity / Alteration
- Availability / Destruction



# CIA - Priorities

- While all three areas of CIA are important to an organization, there is always one area that is more critical than others
- Confidentiality
  - Health Care Organizations
  - Hospitals
- Integrity
  - Financial Institutions
  - Banks
- Availability
  - E-commerce based organizations
  - Online banking

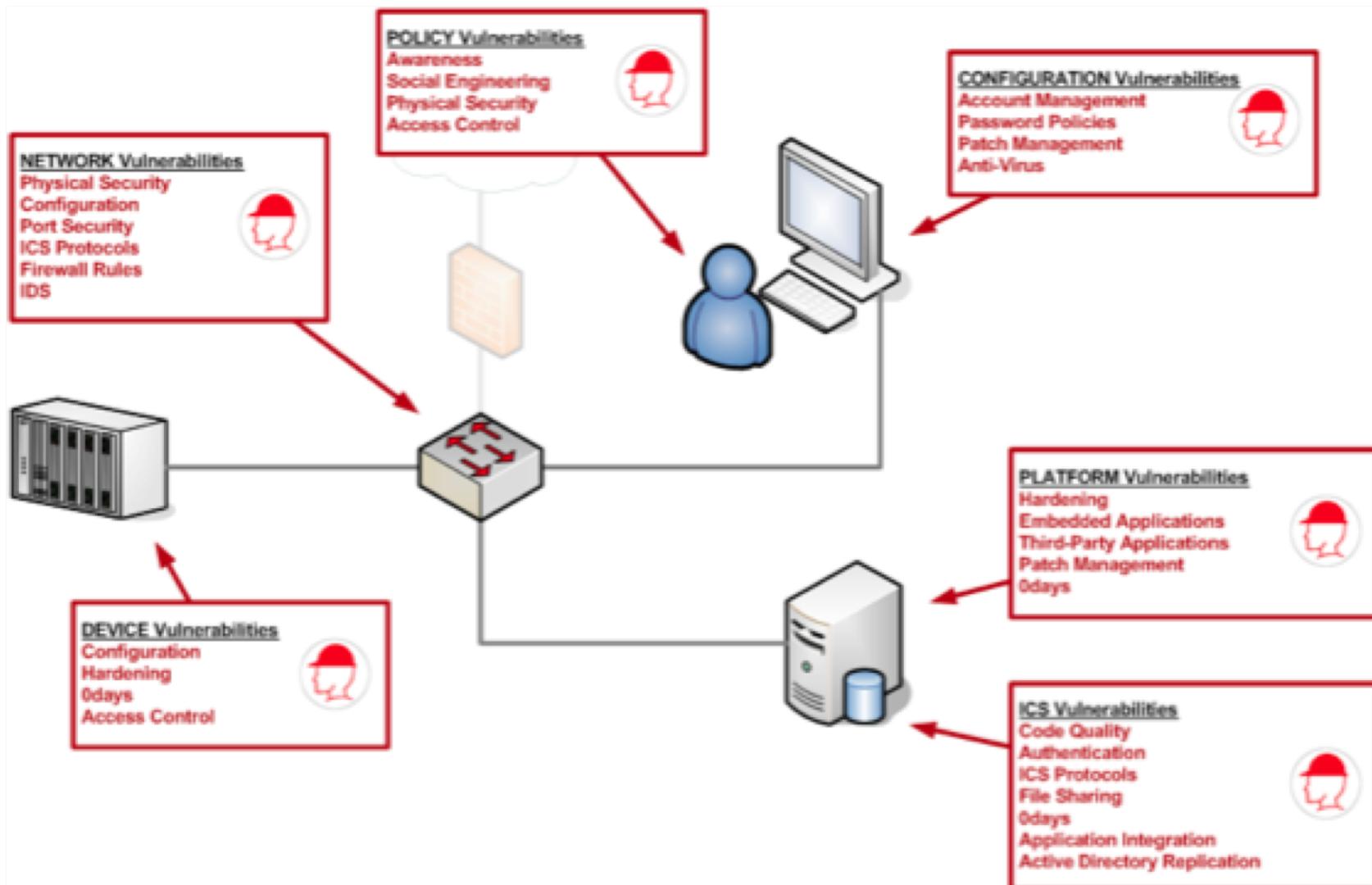
# Threat

- **threat**
  - An expression of an intention to inflict pain, injury, evil, or punishment.
  - An indication of impending danger or harm.
  - One that is regarded as a possible danger; a menace
- A threat is any attempt to compromise information, system, or network resources
- They can originate from anywhere, any time
- They take advantage of operating system, application, protocol, and psychological vulnerabilities
- They leverage all methods of entry to a system
- They can steal information, destroy data, deny access to servers, shut down embedded devices

# Vulnerability

- Weaknesses in a system
- Vulnerabilities are inherent in complex systems, they will always be present
- The majority of vulnerabilities are the result of poor coding practices
  - Lack of error checking
- Vulnerabilities are the gateway by which threats are manifested
- Vulnerabilities fall into two categories:
  - Known, those you can protect against
  - Unknown or “zero day”

# Vulnerabilities



# DID APPROACHES

---

# DiD Approaches

- Several approaches to DiD
- **Uniform protection**
  - <http://www.sans.edu/research/security-laboratory/article/367>
- **Protected enclaves**
  - <http://www.sans.edu/research/security-laboratory/article/372>
- **Information centric**
  - <http://www.sans.edu/research/security-laboratory/article/321>
- **Threat vector**
  - <http://www.sans.edu/research/security-laboratory/article/threat-vector-did>

# Uniform Protection DiD

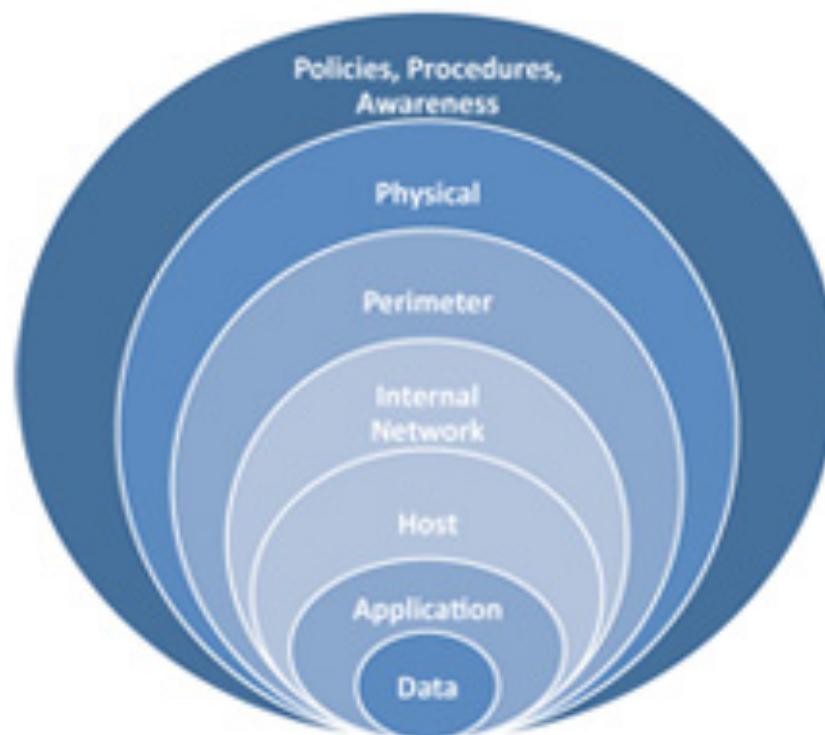
- Most common approach
- Firewall, VPN, IDS, Anti-Virus ...
- Same level of protection for all parts of the organisation
- No consideration for company critical assets

# Protected Enclaves

- Assets that require additional protection are segmented from the rest of the internal organization
- Restricting access to critical segments
- System of VPNs
- Internal Firewalls
- VLANs and ACLs

# Information centric DiD

- Identify critical assets and provide layered protection
- Data is accessed by applications
- Applications reside on hosts
- Hosts operate on networks



Layers of Defense in Depth

# Threat vector DiD

- The threat requires a vector to cross the vulnerability
- Stop the ability of the threat to use the vector
  - USB Thumb Drives – Disable USB
  - Floppy Drives – Disable
  - Auto Answer Modems – Digital phone PBX

# INFOSEC PROCESS - PDR



# Prevention

- Security measures to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional.
- Prevention phase:
  - security policies
  - controls
  - process
- First objective – determine **what** must be protected

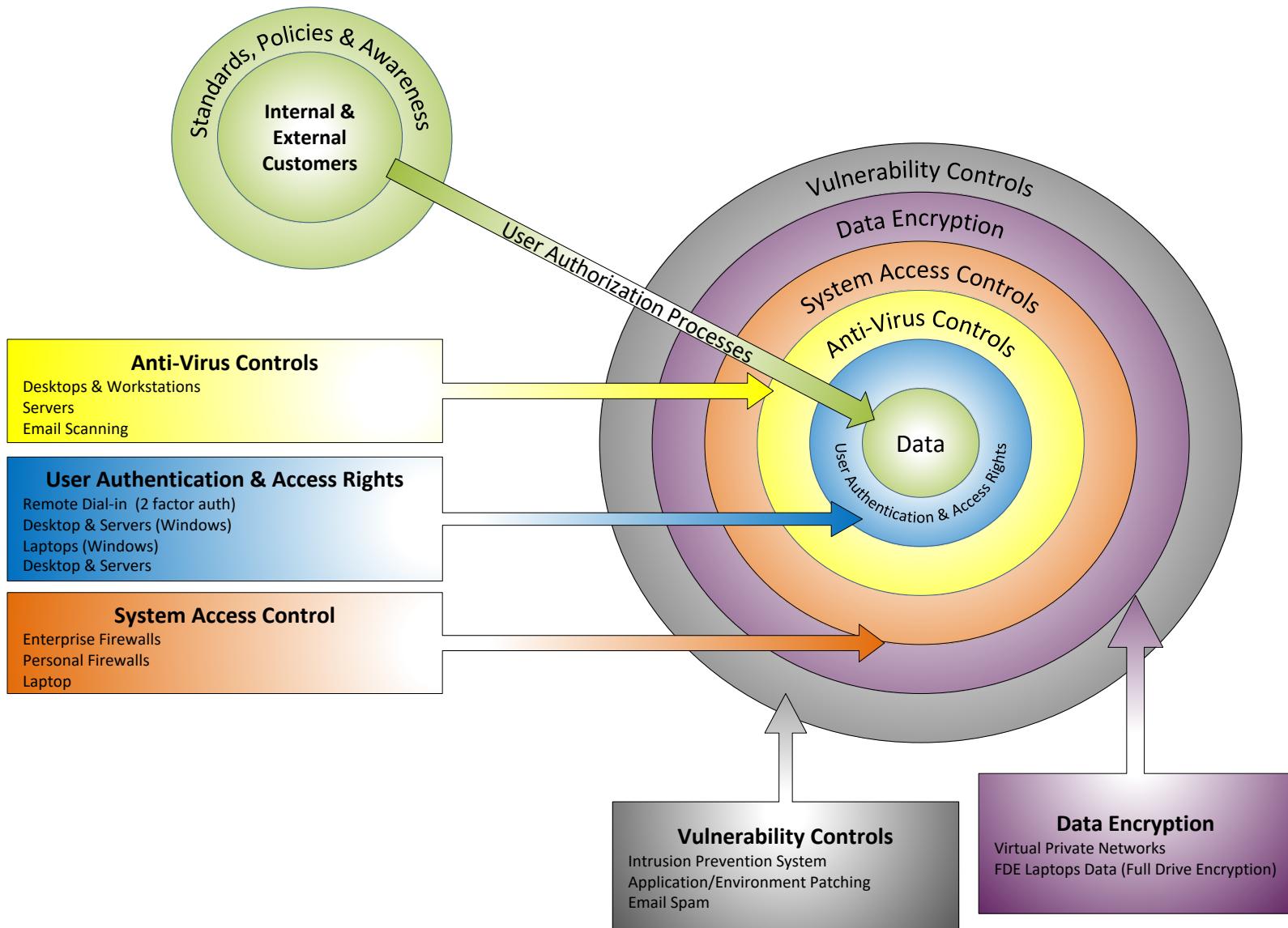
# Detection

- *“Prevention is ideal but Detection is a must”*
- Detection of a system compromise is extremely critical
- No matter the level of protection, you will be compromised (all it takes is a great level of motivation and skill)
- Timely detection and notification of a compromise
- Intrusion detection tools should be strategically placed at the network and application levels

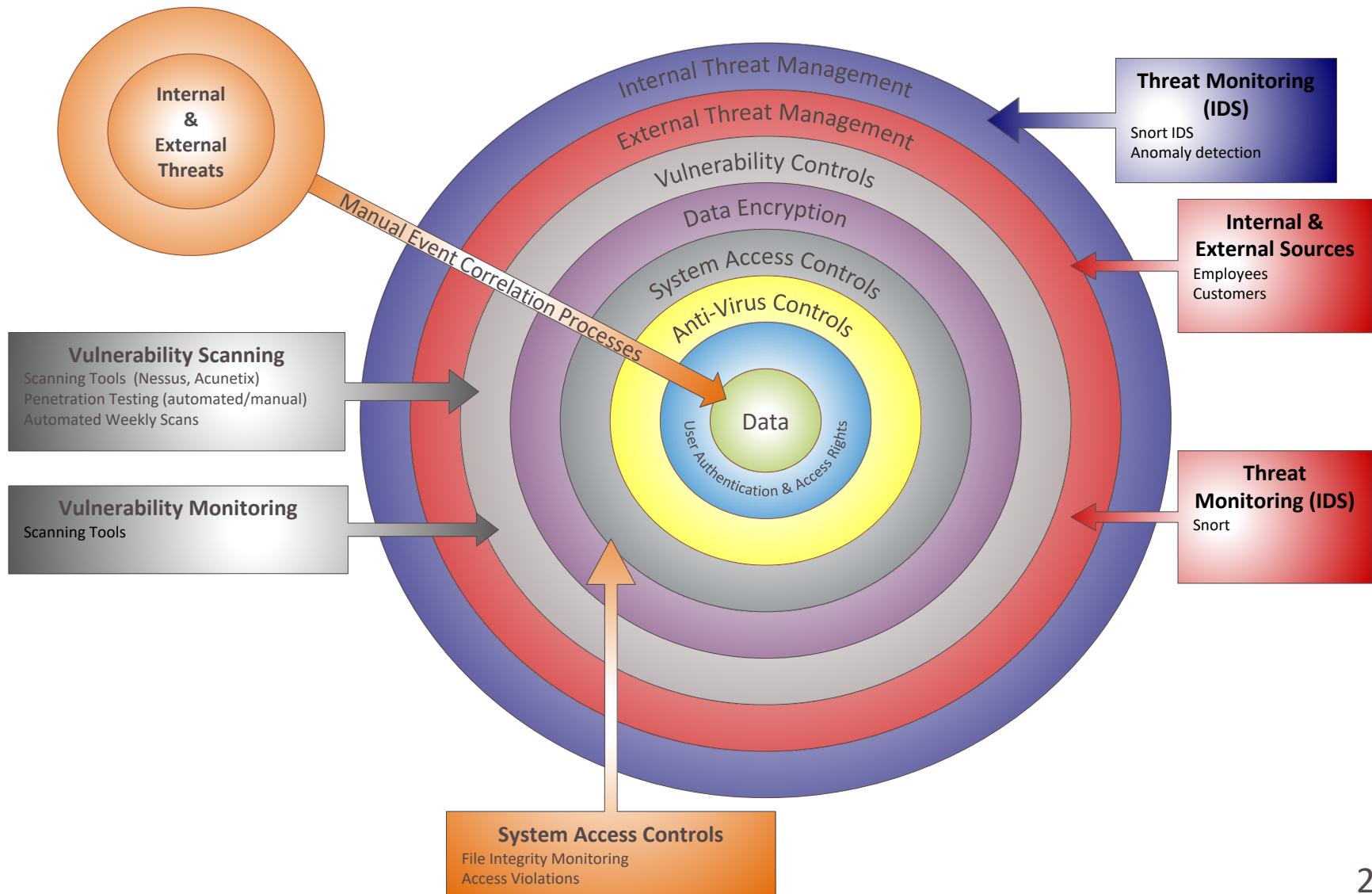
# Response

- For the detection process to have any value there must be a timely response
- You need to plan in advance how to respond to an incident
- Developing a policy while under attack is a recipe for disaster
- The response plan should be written and ratified by senior management
- A Computer Security Incident Response Team (**CSIRT**) should be established with specific roles and responsibilities identified.

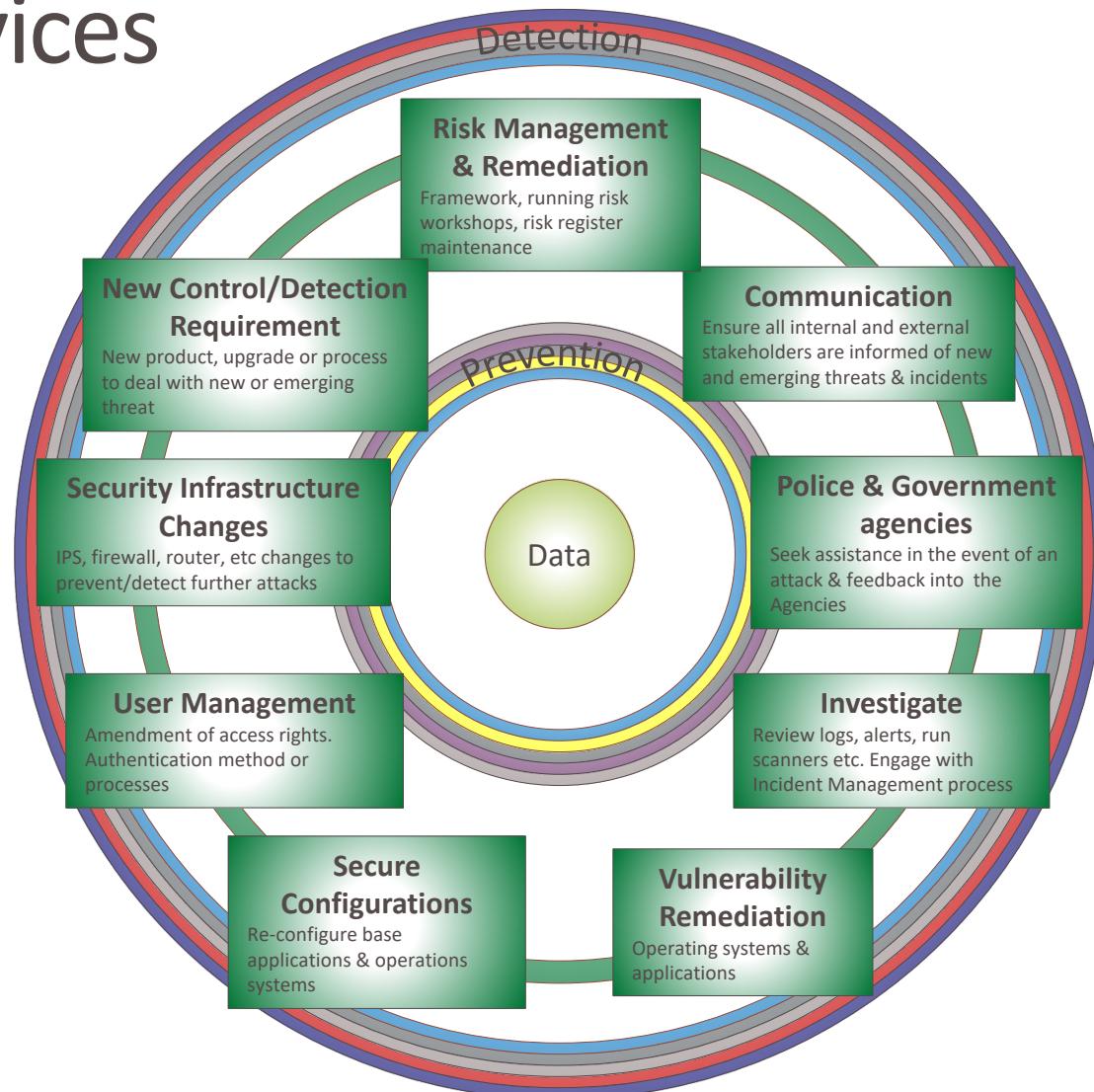
# Prevention Services



# Detection Services



# Response Services



# 20 CRITICAL CONTROLS

---

# SANS 20 Critical Security Controls

- 1: Inventory of Authorized and Unauthorized Devices
- 2: Inventory of Authorized and Unauthorized Software
- 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- 4: Continuous Vulnerability Assessment and Remediation
- 5: Malware Defenses
- 6: Application Software Security
- 7: Wireless Access Control
- 8: Data Recovery Capability
- 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- 11: Limitation and Control of Network Ports, Protocols, and Services
- 12: Controlled Use of Administrative Privileges
- 13: Boundary Defense
- 14: Maintenance, Monitoring, and Analysis of Audit Logs
- 15: Controlled Access Based on the Need to Know
- 16: Account Monitoring and Control
- 17: Data Protection
- 18: Incident Response and Management
- 19: Secure Network Engineering
- 20: Penetration Tests and Red Team Exercises

# SANS 20 Critical Security Controls (1)

- **Inventory of Authorized and Unauthorized Devices**
  - Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
- **Inventory of Authorized and Unauthorized Software**
  - Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
- **Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
  - Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

# SANS 20 Critical Security Controls (2)

- **Continuous Vulnerability Assessment and Remediation**
  - Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
- **Malware Defenses**
  - Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.
- **Application Software Security**
  - Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

# SANS 20 Critical Security Controls (3)

- **Wireless Access Control**
  - The processes and tools used to track/control/prevent/correct the security use of wireless local area networks, access points, and wireless client systems.
- **Data Recovery Capability**
  - The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
- **Security Skills Assessment and Appropriate Training to Fill Gaps**
  - For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

# SANS 20 Critical Security Controls (4)

- **Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**
  - Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
- **Limitation and Control of Network Ports, Protocols, and Services**
  - Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

# SANS 20 Critical Security Controls (5)

- **Controlled Use of Administrative Privileges**
  - The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
- **Boundary Defense**
  - Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
- **Maintenance, Monitoring, and Analysis of Audit Logs**
  - Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

# SANS 20 Critical Security Controls (6)

- **Controlled Access Based on the Need to Know**

- The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

- **Account Monitoring and Control**

- Actively manage the life-cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

- **Data Protection**

- The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

# SANS 20 Critical Security Controls (7)

- **Incident Response and Management**

- Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

- **Secure Network Engineering**

- Make security an inherent attribute of the enterprise by specifying, designing, and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers.

- **Penetration Tests and Red Team Exercises**

- Test the overall strength of an organization's defenses (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

# **SECURITATEA IN SISTEMELE IT**

---

## **INCIDENT HANDLING FOUNDATIONS**

Tudor Blaga



**UNIVERSITATEA TEHNICĂ**  
DIN CLUJ-NAPOCA

# Who is the new guy?

## Vlad Cristea

SysAdmin

Network Admin

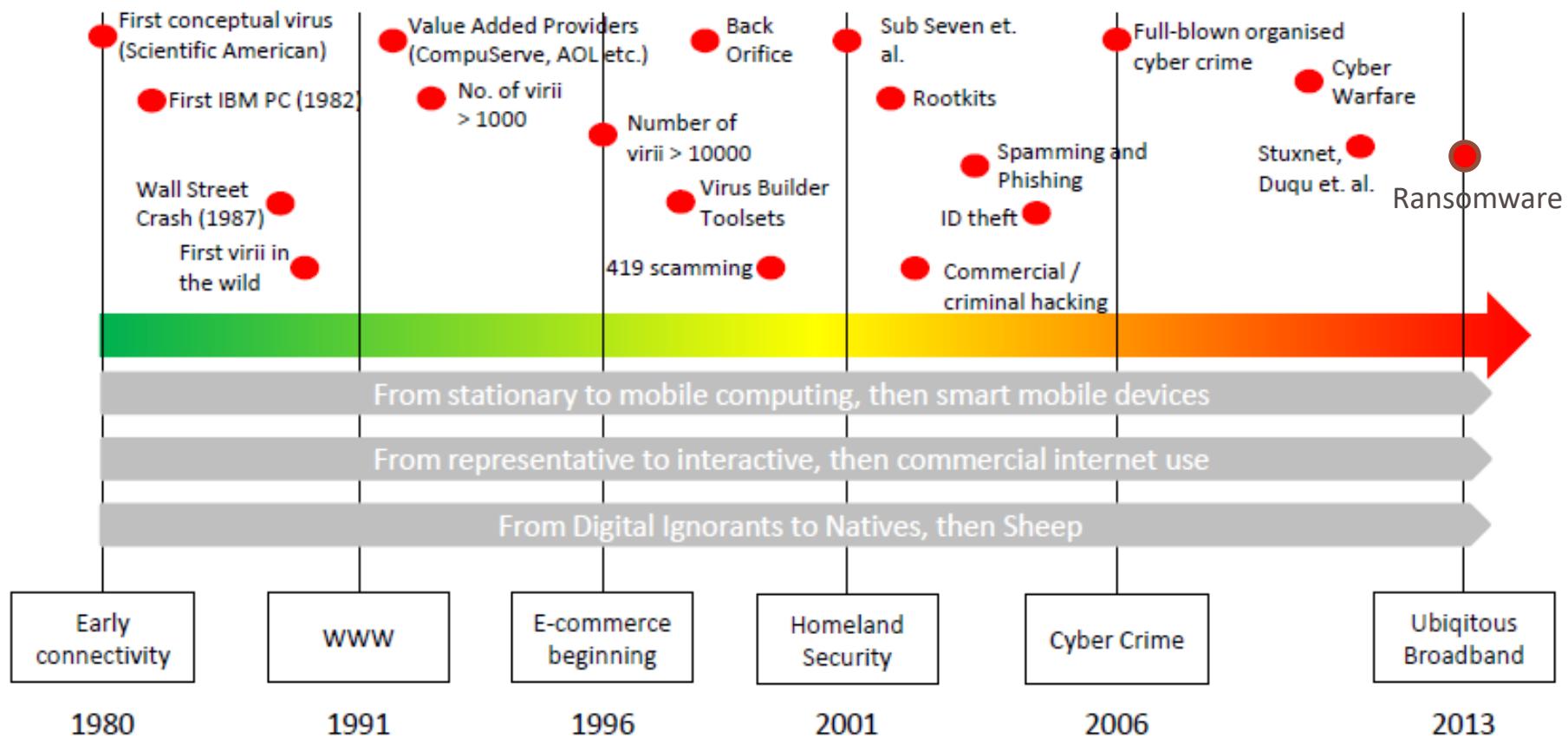
Threat Intelligence Engineer

Security Analyst

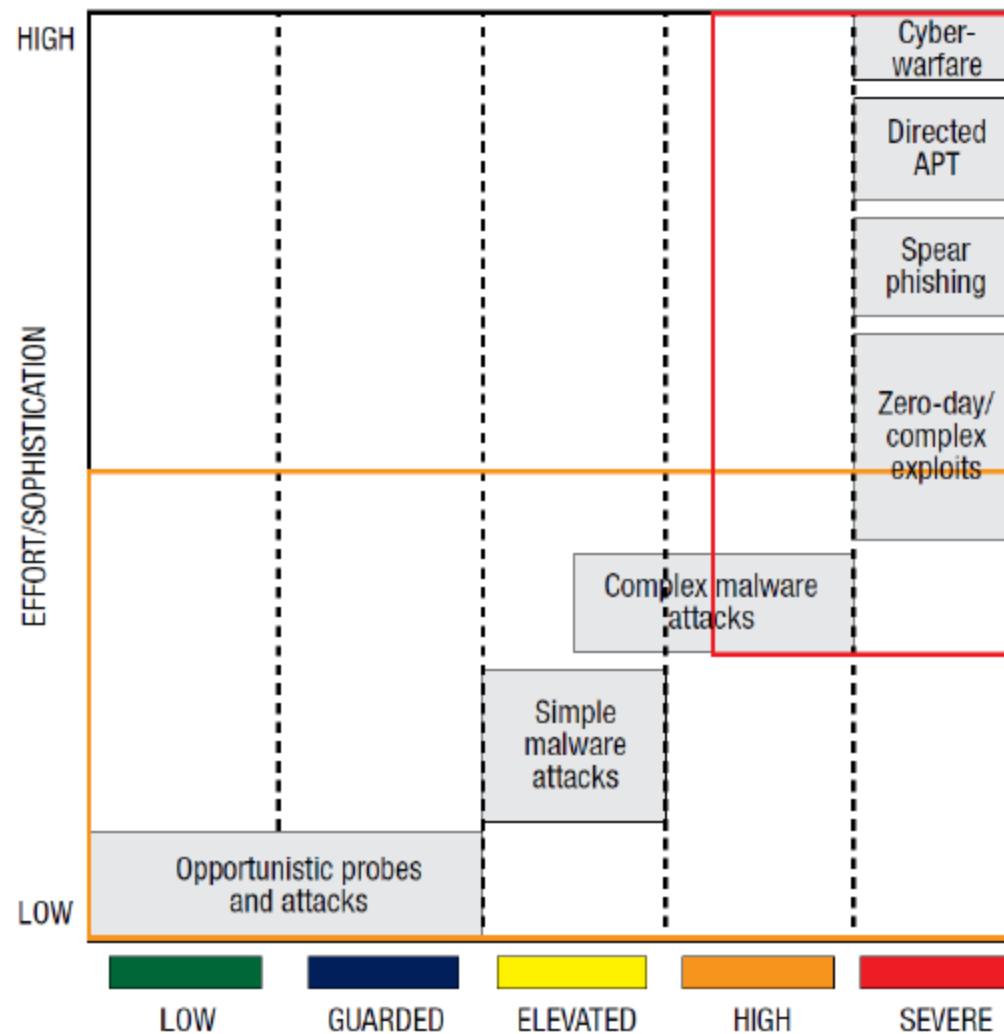
Incident response



# Cybercrime / Cyberwarfare



# Categories of attacks



# Cyber attack actors and impacts

**Table 1. Cyber threat actors and impacts: Heat map for the manufacturing sector**

Actors \ Impacts	Financial theft/fraud	Theft of IP or strategic plans	Business disruption	Destruction of critical infrastructure	Reputation damage	Threats to life/safety	Regulatory
Organized criminals	High	High	High	High	Moderate	High	Low
Hactivists	Low	High	High	High	High	Low	High
Nation-states	Low	High	High	High	High	High	Low
Insiders/partners	High	Very high	High	Low	High	Moderate	Very high
Competitors	Low	High	High	Low	High	Moderate	Very high
Skilled individual hackers	High	High	Moderate	Moderate	Moderate	High	Moderate

KEY ■ Very high ■ High ■ Moderate ■ Low

Source: Deloitte, "Cybersecurity: A prudent approach," October 30, 2015.

# Stuxnet 2007



**Type of attack:** Custom malware, airgap hopping, USB C2

**Impact:** Nuclear facility stops production and replace centrifuges

**Cause:** Lack of monitoring and alerting

**Threat actor:** Nation state (probably USA + Israel)

**Reason:** CyberWarfare

# Target 2013



**Type of attack:** VPN account takeover, lateral movement and POS malware

**Impact:** 40m CCs, 100m records accessed, CEO resigned

**Cause:** Lack of monitoring and general security controls

**Threat actor:** Criminal Organization

**Reason:** Financial Gain

# Sony hack 2014



**Type of attack:** Custom malware, backdoor, destructive tools

**Impact:** Most PCs destroyed, 100TB data leaked, 47m records

**Cause:** Lack of monitoring and alerting

**Threat actor:** Nation state (probably North Korea)

**Reason:** CyberWarfare

# Equifax 2017



**Type of attack:** Web exploit and lateral movement

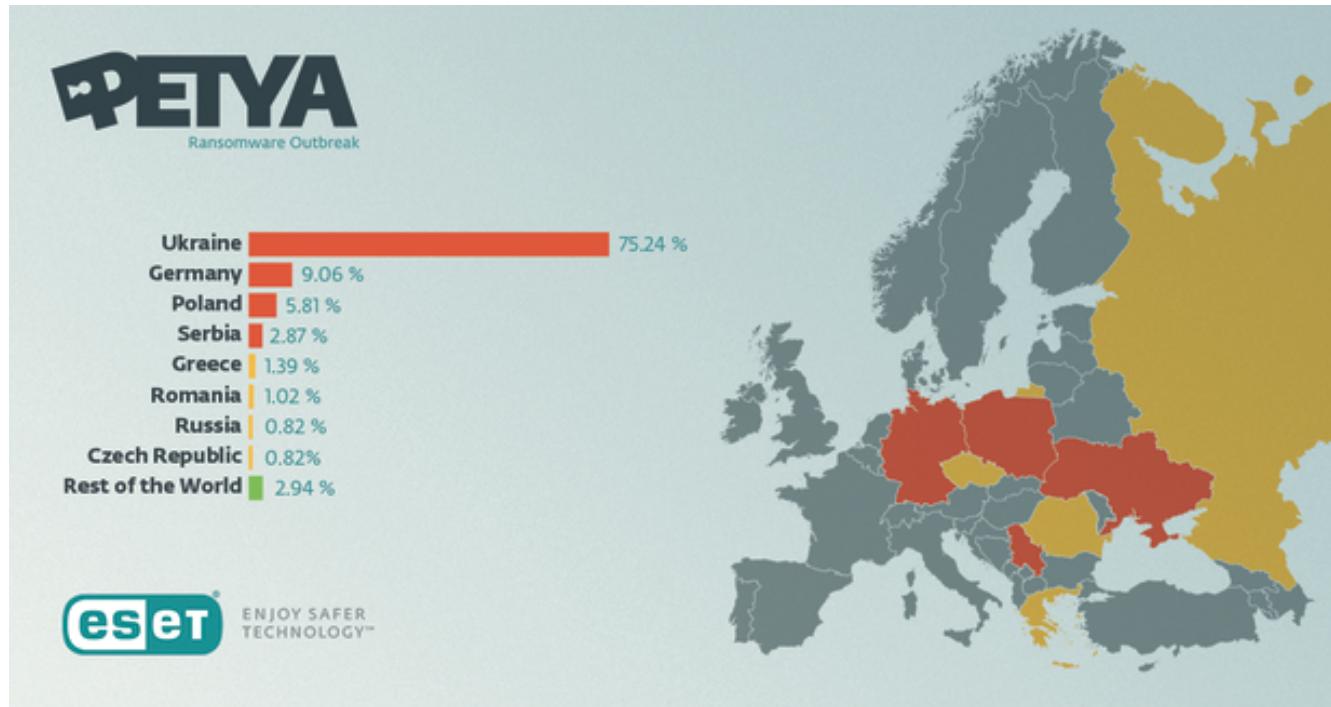
**Impact:** ~145m records stolen

**Cause:** Unpatched vulnerability and lack of alerting

**Threat actor:** Criminal organization

**Reason:** Financial gain

# NotPetya 2017



**Type of attack:** Supply chain infection and ransomware deployment

**Impact:** Companies close operations, data exfiltration, full compromise

**Cause:** Trusted update chain exploited and used to deploy malware

**Threat actor:** Nation state (probably Russia)

**Reason:** CyberWarfare

# Marriott 2018



**Type of attack:** Malware (opened by a security analyst on a machine that had access to Marriott's internal email 😊)

**Impact:** ~383 records stolen + ~5m passports

**Cause:** Unpatched vulnerability and lack of alerting

**Threat actor:** Nation state (probably China)

**Reason:** Cyberwarfare

# Bonus slide: Facebook 2018



**Type of attack:** Web exploit, stolen access token using “view as” functionality

**Impact:** ~30m users (2018 hack)

**Cause:** Bug in application which allowed users to “view as” anyone

**Threat actor:** Unknown

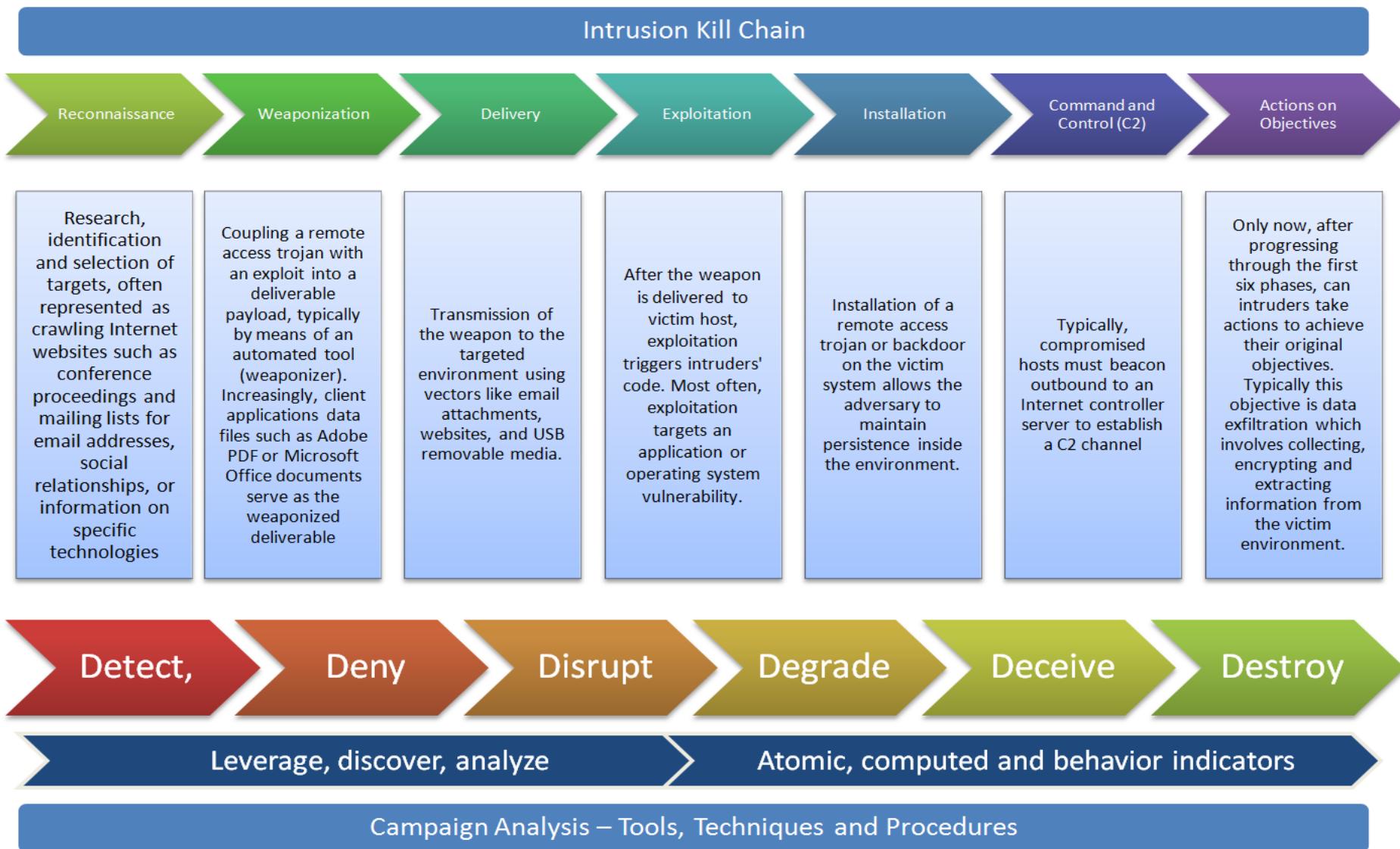
**Reason:** Unknown

# APT – Advanced Persistent Threat

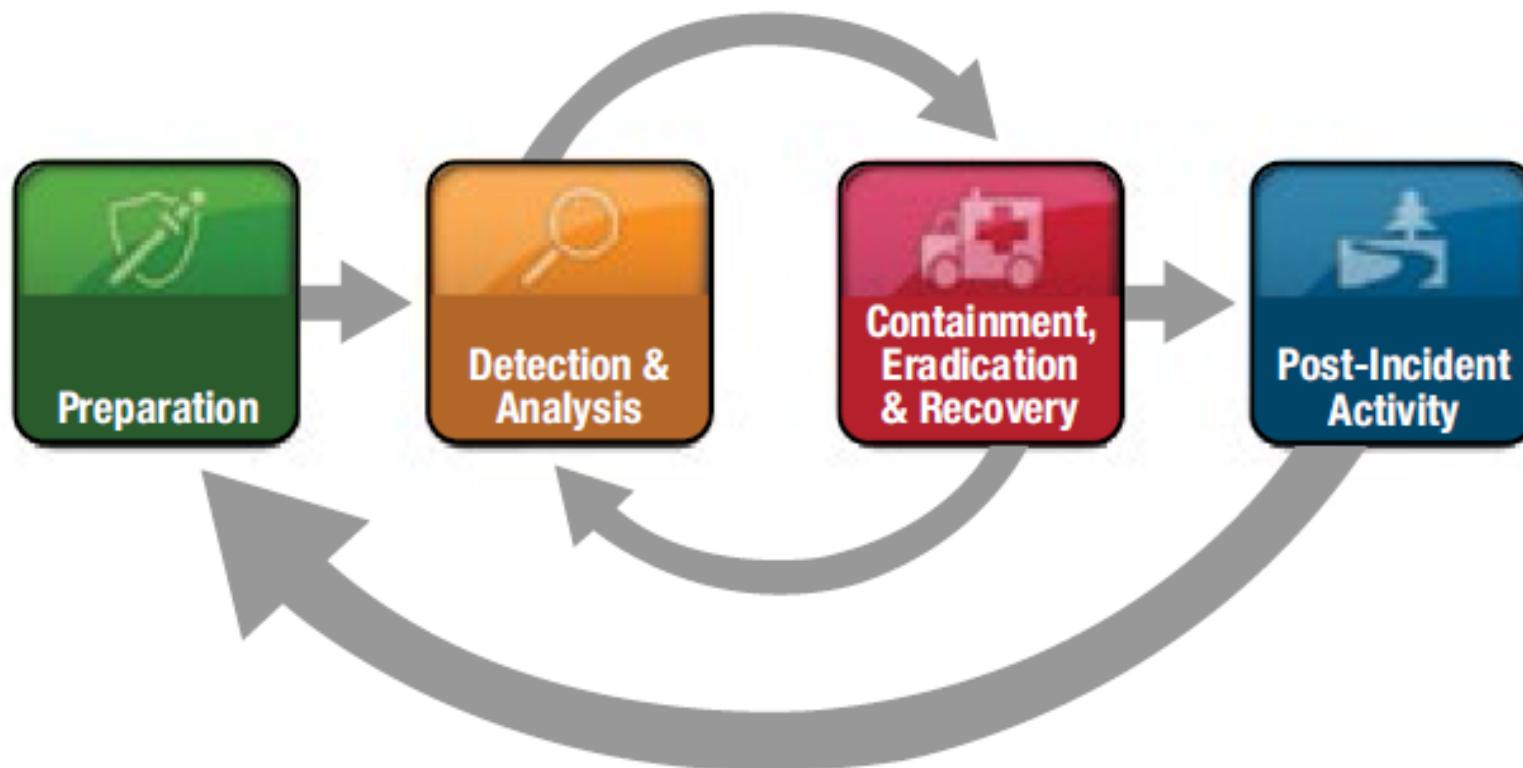
- NIST SP 800-53 R4 [5] defines the APT as:

“An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders’ efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.”

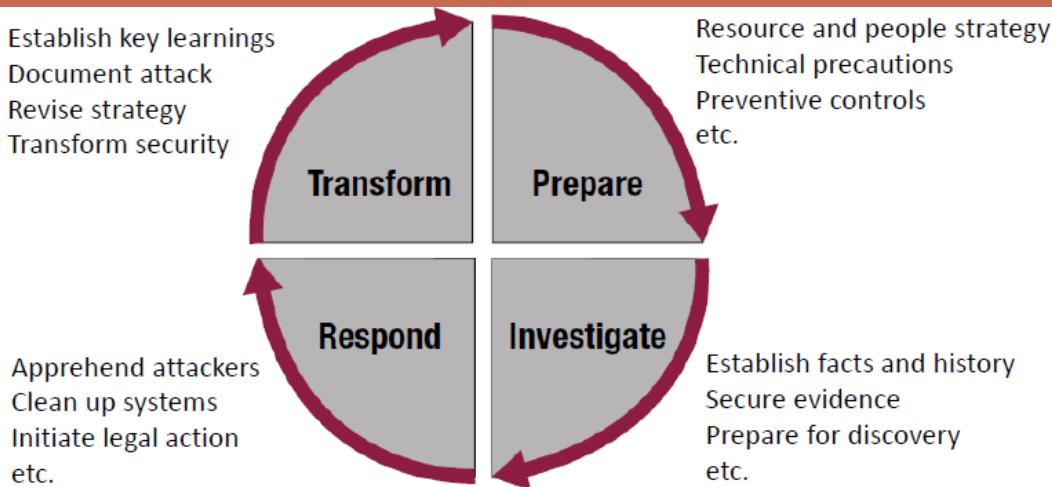
# APT attack internals



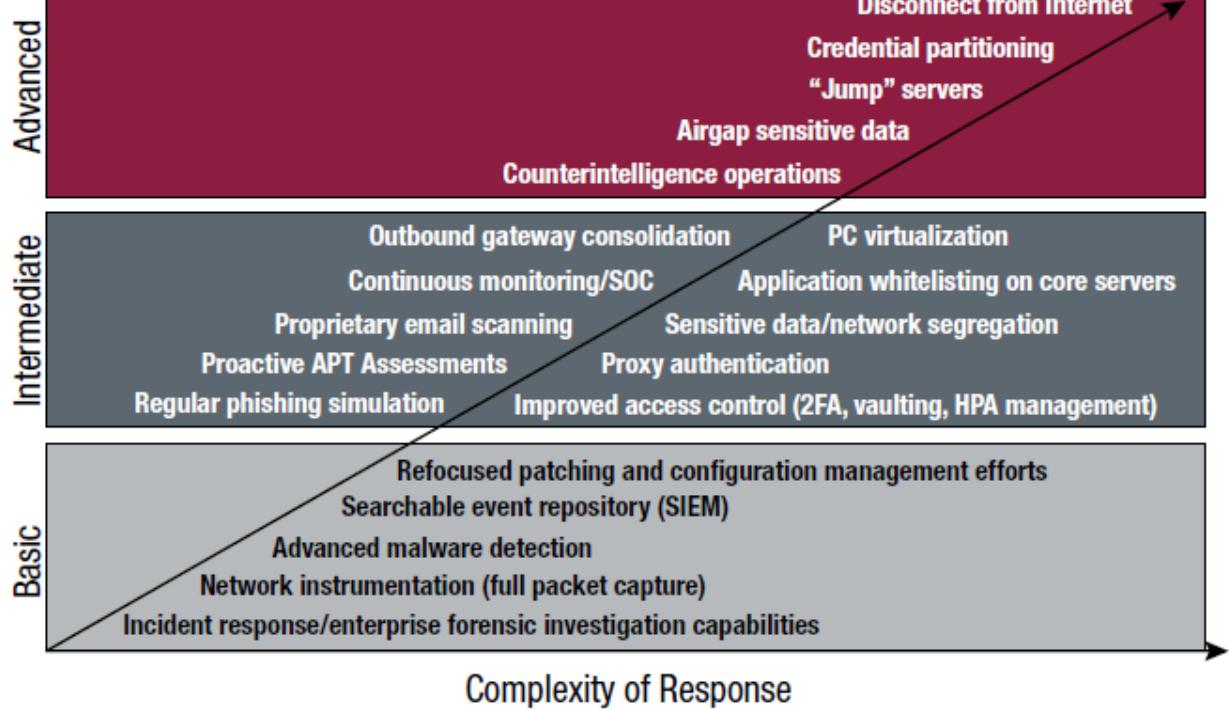
# The Incident Response Life Cycle From NIST SP 800-61



Source: Cichonski, Paul; Tom Millar; Tim Grance; Karen Scarfone; *Computer Security Incident Handling Guide*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Revision 2, USA, August 2012.



Source: TCS



SOC = Security operations center  
 2FA = Two-factor authentication

HPA = High profile asset  
 SIEM = Security information and event management

# Tooling capabilities

Capability (People, Process, Technology)	Minimum	Preferred
Host-level activity awareness	<ul style="list-style-type: none"><li>Logs from end-point software agents (e.g., antivirus)</li><li>Native OS logging (e.g., Microsoft Windows®)</li></ul>	<ul style="list-style-type: none"><li>Host-based intrusion detection</li><li>Remote enterprise forensic analysis</li><li>Agent-based, live memory analysis</li></ul>
Network-level activity awareness	<ul style="list-style-type: none"><li>Network flow data (e.g., layer 3)</li><li>Proxy logs</li><li>Firewall logs</li></ul>	<ul style="list-style-type: none"><li>Network intrusion detection logs</li><li>Full packet capture at all egress points</li><li>SSL inspection</li></ul>
Search	Decentralized log searches on a per-system basis: <ul style="list-style-type: none"><li>Local logging</li><li>Manual retrieval</li><li>Limited automation</li></ul>	<ul style="list-style-type: none"><li>Centralized aggregation of searchable log data</li><li>Event correlation (e.g., SIEM)</li></ul>
Digital forensics	<i>Ad hoc</i> , local	<ul style="list-style-type: none"><li>Remote enterprise (acquisition)</li><li>Case management systems</li></ul>
Malware analysis	<ul style="list-style-type: none"><li>Dynamic malware analysis</li><li>Basic static and automated analysis</li></ul>	<ul style="list-style-type: none"><li>In-depth static code analysis</li><li>Reverse engineering</li></ul>
Threat intelligence	<i>Ad hoc</i> , open source research	<ul style="list-style-type: none"><li>Subscription-based</li><li>Business partner information sharing</li><li>Repeatable, automated integration</li></ul>
Vulnerability identification	Enterprise application inventory	Enterprise vulnerability identification

# Incident Eradication

- Do not start eradication before forensics and evidence collection have been completed
- Target your eradication effort. Where compromised systems are taken offline, they may well run for a while for experimental purposes
- Wiping and rebuilding systems is a good idea, but it may prevent key learnings
- Restoring to factory default is tempting, but it may re-open the floodgates
- Recovering from a major incident may be an opportunity for re-architecting and reconfiguring (stuff you've always wanted to do)

## Incident Containment / Eradication / Remediation

- Change passwords, credentials
- Rebuild IAM, opsys authentication
- Block or filter known ports of entry
- Use honeypots and tarpits as appropriate
- Rebuild affected platforms from the ground up
- Wipe MBR / get new hardware
- Reset and rebuild network layer
- Blackout all hardware

# Ok, what about the proactive side?

## Threathunting!

- DNS Logs – entropy, zero variance queries, suspicious domains
- Traffic flow – statistical deviation
- Traffic anomalies – least seen domains
- Impossible traveler – VPN vs local login
- Rogue devices – weird MAC
- Honeyword /honeypot – who's trying to login as Administrator or CashflowServer
- Authentication attempts – multiple attempts with different users from same host

# Threat Intelligence

- Earlier detection, higher level of confidence
- Ongoing information flow about known attack patterns, vulnerabilities etc.
- Available from a number of sources (public, domain, commercial)
- Examples: various CERTs, security alliances (see RTA), security advisories by European institutions

# OSINT Techniques

<http://www.exploit-db.com/google-dorks/>

The screenshot shows the homepage of the Google Hacking Database. At the top left, it says "Google Hacking Database". Below that is a dropdown menu labeled "Select category:" with "sensitive Directories" selected. The menu also includes options like "Footholds", "Files containing usernames", "Web Server Detection", "Vulnerable Files", "Vulnerable Servers", "Error Messages", "Files containing juicy info", "Files containing passwords", "sensitive Online Shopping Info", "Pages containing network or vulnerability data", "Pages containing login portals", "Various Online Devices", and "Advisories and Vulnerabilities". To the right of the menu, there's a large "GOOGLE HACKING-DATABASE" logo. Below the logo, there's some text about Google's collection of hacking techniques and a search bar. At the bottom, there are two examples of search queries: "search for Cisco IOS images Author: fdisk..." and "Google search for Pix/Asa images Author: fdisk...".

# OSINT Techniques

Topsy.com – alert for search terms

The screenshot shows the Topsy.com homepage with a search bar containing 'hack government'. Below the search bar, there's a navigation bar with tabs: SOCIAL SEARCH, SOCIAL ANALYTICS, and SOCIAL TRENDS. On the left, a sidebar displays 'Latest Results' with timeframes and counts: Past 1 Hour (0), Past 1 Day (27), Past 7 Days (742), Past 12 Days (1.3K), Past 30 Days (1.8K), All Time, and Specific Range. A 'Everything' tab is selected. The main content area shows a summary for the 'Past 30 Days': 1,751 tweets, Topsy Sentiment Score: 40, and a timeline chart for the past 30 days. Below this, a tweet from 'Vision Implementer @tyrese' is displayed, followed by another tweet from 'WikiLeaks @wikileaks'.

The screenshot shows the Topsy.com homepage with a teal header containing 'SOCIAL SEARCH', 'SOCIAL ANALYTICS', and 'SOCIAL TRENDS'. In the top right corner, there's a 'TOPSY PRO LOGIN' button. The main title 'TOPSY' is in orange at the top center. Below it, the tagline 'Search and Analyze the Social Web.' is displayed. A navigation bar below the tagline includes 'EVERYTHING', 'LINKS', 'TWEETS', 'PHOTOS', 'VIDEOS', and 'INFLUENCERS'. A search bar with a magnifying glass icon is present. At the bottom, a banner features the text 'ALL TWEETS' and 'SINCE 2006' with a Twitter logo.

## Google Alerts

The screenshot shows the Google Alerts interface. At the top, there's a blue header with the word 'Alerts' and a sub-instruction 'Monitor the web for interesting new content'. Below this is a search bar with the placeholder 'Create an alert about...'. The main content area shows an alert for 'Wikileaks Releases German Spyware' with a link to techcrunch.com. To the right, there are sections for 'Alert suggestions' (News Sections like Entertainment, Science) and 'Companies' (Tesco, Sainsbury's).

# OSINT Techniques

HavelBeenPwned.com “Check if you have an account that has been compromised in a data breach”

GoofBay – Ebay typo search

HackNotifier.com – identify if email addresses have been compromised

SearchIRC.com – IRC Search

The screenshot shows the HavelBeenPwned.com website. At the top, there is a large blue button with the text '';--have i been pwned?'. Below it, a sub-header reads 'Check if you have an account that has been compromised in a data breach'. A search bar contains the email address 'p[REDACTED]@yahoo.com'. To the right of the search bar is a button labeled 'pwned?'. Below the search bar, the text 'Oh no — pwned!' is displayed in a large white font on a dark background. Underneath, a smaller message states 'Pwned on 4 breached sites and found no pastes (subscribe to search sensitive breaches)'. At the bottom of the page, there is a navigation bar with links like 'Home', 'About', 'Contact', and 'Help'.



The screenshot shows the SearchIRC website. The main heading is 'SearchIRC'. Below it, there is a search bar with the text 'hack site' and a 'go' button. The page title is 'Searching through 109,102 channels'. A navigation bar at the top includes 'Hack Site', 'IRC', 'Search', 'Help', and 'About'. The main content area displays search results for 'Displaying results 1 - 15 (of 841) matching **hack site**. Process time'. The results are listed as follows:

1. irc:// #symfony-dev New!  
Users: [progress bar]  
Network: Fayntic  
Review: There are no reviews of this channel  
Topic: It's Community **Hack** Day! Read everything you need on http://
2. irc:// #hackndev New!  
Users: [progress bar]  
Network: Fayntic  
Review: There are no reviews of this channel  
Topic: Hack&Dev http://hackndev.com | Speak \_english\_ | We hac patches against arm:devel | Useful links: http://marex.hackn installer? ping Sleep\_Walker
3. irc:// #sbhackers New!  
Users: [progress bar]  
Network: Fayntic  
Review: There are no reviews of this channel  
Topic: Hackity hack hack

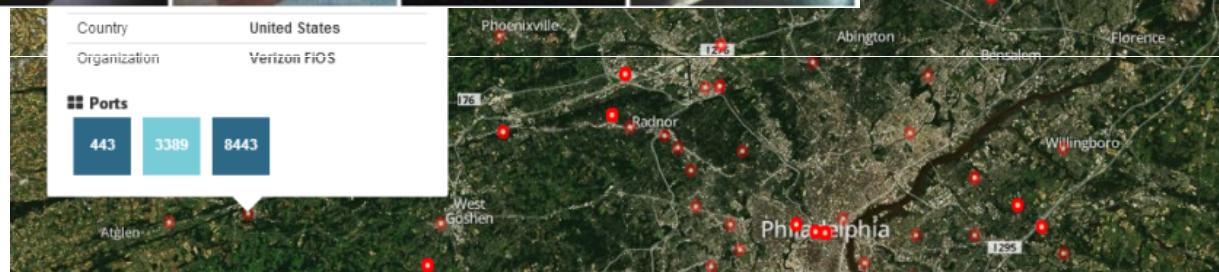
At the bottom left, there is a sidebar with the text 'Click on the channel name to join the chat using our java client. Click on the irc:// before the name to join the chat with your dedicated IRC client. Don't have an IRC client installed? There are plugins available for firefox.' and a link 'If you'd like to add channel stats to your website, click here'. A 'Please visit' section at the bottom right includes links to 'Cruise Guide' and 'IRC'.

# OSINT Techniques

[www.shodan.io](http://www.shodan.io) – search for computers or devices rather than websites – e.g. search for webcams based on a GPS location



Below is a map of the globally exposed routers that contain a backdoor



# Offensive OSINT

In the next slides, you will see two instances of information gathering made exclusively by using passive sources.

No port scans, no accessing of the websites, nothing that leaves a trace for the victim to see

The first one was not very successful, but the 2<sup>nd</sup> is pretty interesting and scary from a security perspective.

# Case 1

Brazilian company: Let's see what can we find about them

The image shows two side-by-side screenshots of web pages. The left page is from 'HURRICANE ELECTRIC INTERNET SERVICES' and the right page is from 'bgp.he.net'. Both pages are displaying WHOIS and DNS information for a domain.

**HURRICANE ELECTRIC INTERNET SERVICES (Left):**

- Quick Links:** BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, Bogon Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, Contact Us.
- Domain Information:** domain: se[REDACTED]ses[REDACTED].a.com.br, owner: Ser[REDACTED]s Es[REDACTED] Ltda, owner-c: Ser[REDACTED]T31, admin-c: Ser[REDACTED]T31, tech-c: Ser[REDACTED]T31, billing-c: Ser[REDACTED]T31, nserver: ns1.se[REDACTED]ses[REDACTED].a.com.br 17[REDACTED]4, nsstat: 20171108 AA, nslastaa: 20171108, nserver: ns2.se[REDACTED]ses[REDACTED].a.com.br 17[REDACTED]0, nsstat: 20171108 AA, nslastaa: 20171108, created: 20030320 #1147272, changed: 20170927, expires: 20220320, status: published, nic-hdl-br: Ser[REDACTED]T31, person: Ser[REDACTED]s Es[REDACTED] LTDA, created: 20110406, changed: 20170906.
- Navigation:** DNS Info, Website Info, IP Info, Whois.

**bgp.he.net (Right):**

- Quick Links:** BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, Bogon Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, Contact Us.
- Domain Information:** domain: se[REDACTED]ses[REDACTED].a.com.br, mname: se[REDACTED]ses[REDACTED].a.com.br rname: lucas.s[REDACTED]ses[REDACTED].a.com.br, serial: 2017250501, refresh: 300, retry: 300, expire: 300, minimum: 300.
- Start of Authority:** mname: se[REDACTED]ses[REDACTED].a.com.br rname: lucas.s[REDACTED]ses[REDACTED].a.com.br, serial: 2017250501, refresh: 300, retry: 300, expire: 300, minimum: 300.
- Nameservers:** ns1.se[REDACTED]ses[REDACTED].a.com.br, ns2.se[REDACTED]ses[REDACTED].a.com.br.
- Mail Exchangers:** relay.gr[REDACTED].a.com.br(0).
- TXT Records:** v=spf1 a mx a:intranet.se[REDACTED]ses[REDACTED].a.com.br a:exchange.se[REDACTED]ses[REDACTED].a.com.br a:srvpf01.se[REDACTED]ses[REDACTED].a.com.br ip4:17[REDACTED]54/32 ip4:17[REDACTED]20/32 -all.
- A Records:** 18[REDACTED]70.

Both pages include social media sharing icons for Twitter and Facebook.

# Case 1

Brazilian company: Oddities

The image shows two screenshots of the Hurricane Electric BGP Toolkit website, comparing WHOIS and DNS data for a specific domain.

**Left Screenshot (WHOIS):**

- Quick Links:** BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, Bogon Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, Contact Us.
- Domain:** s[REDACTED]-s-e[REDACTED].a.com.br
- WHOIS Data:**

domain:	s[REDACTED]-s-e[REDACTED].a.com.br
owner:	S[REDACTED]s E[REDACTED]a Ltda
owner-c:	S[REDACTED]31
admin-c:	S[REDACTED]31
tech-c:	M[REDACTED]4
billing-c:	S[REDACTED]31
nserver:	ns1.s[REDACTED]se[REDACTED].a.com.br
nsstat:	20171107 AA
nslastaa:	20171107
nserver:	ns2.s[REDACTED]se[REDACTED].a.com.br
nsstat:	20171107 AA
nslastaa:	20171107
created:	19970221 #30643
changed:	20170927
expires:	20220221
status:	published
nic-hdl-br:	S[REDACTED]1
person:	S[REDACTED]s E[REDACTED]a LTDA
created:	20110406
changed:	20170906
nic-hdl-br:	M[REDACTED]4
person:	M[REDACTED]s
created:	20060926
changed:	20120229
- Social Media:** Twitter and Facebook icons.

**Right Screenshot (DNS):**

- Quick Links:** BGP Toolkit Home, BGP Prefix Report, BGP Peer Report, Exchange Report, Bogon Routes, World Report, Multi Origin Routes, DNS Report, Top Host Report, Internet Statistics, Looking Glass, Network Tools App, Free IPv6 Tunnel, IPv6 Certification, IPv6 Progress, Going Native, Contact Us.
- Domain:** s[REDACTED]-s-e[REDACTED].a.com.br
- DNS Info:** DNS Info, Website Info, IP Info, Whois.
- Start of Authority:** mname: srvpf01.s[REDACTED]-s-e[REDACTED].a.com.br, rname: srvpf01.s[REDACTED]-s-e[REDACTED].a.com.br, serial: 26, refresh: 300, retry: 300, expire: 300, minimum: 300.
- Nameservers:** ns1.s[REDACTED]se[REDACTED].a.com.br, ns2.s[REDACTED]se[REDACTED].a.com.br.
- Mail Exchangers:** exchange.s[REDACTED]se[REDACTED].a.com.br(10).
- TXT Records:** v=spf1 mx include:s[REDACTED]se[REDACTED].a.com.br -all.
- A Records:** 18 [REDACTED] 70.

Updated 08 Nov 2017 16:28 PST © 2017 Hurricane Electric

# Case 1

Brazilian company: Let's see what else do they have around

The screenshot shows a web browser interface with two tabs and a sidebar.

**Top Tab:** https://identipy.com/180.209  
Content: Main nameservers

- ns2.servername.a.com.br
- ns1.servername.a.com.br
- exchange.servername.a.com.br

**Second Tab:** https://domreaper.com/www/servername-a.com.br.html  
Content: Target

- srvpf01.servername-a.com.br

**Sidebar:**

- 180.209 ns2.servername.a.com.br
- 180.210 intranet.servername.a.com.br
- 180.211 ts.servername.a.com.br
- 180.212 voip.servername.a.com.br
- 180.213 ts2.servername.a.com.br

# Case 1

Brazilian company: Port scans

The image shows two screenshots of the ViewDNS.info Port Scanner tool. Both screenshots have a URL of `viewdns.info/portscan/?host=s[REDACTED]ses[REDACTED].com.br` in the address bar.

**Screenshot 1 (Left):**

- Tools Bar:** Tools, API, Research, Data
- Page Title:** ViewDNS.info > Tools > Port Scanner
- Description:** This web based port scanner will test whether common ports are open or down on a specific server.
- Ports Scanned:** 21, 22, 23, 25, 80, 110, 139, 143, 445, 1433, 1
- Domain / IP Address:** [Input Field] GO
- Port Scan Results:** Port scan results for s[REDACTED]ses[REDACTED].com.br  
=====
- Legend:**
  - ✓ - port is OPEN
  - ✗ - port is CLOSED
- Table:** A table showing port numbers, services, and status (OPEN or CLOSED).

PORT	Service	Status
21	FTP	✓
22	SSH	✓
23	Telnet	✗
25	SMTP	✗
53	DNS	✗
80	HTTP	✓
110	POP3	✗
139	NETBIOS	✗
143	IMAP	✗
443	HTTPS	✓
445	SMB	✗
1433	MSSQL	✗
1521	ORACLE	✗
3306	MySQL	✗
3389	Remote Desktop	✗

**Screenshot 2 (Right):**

- Tools Bar:** Tools, API, Research, Data
- Page Title:** ViewDNS.info > Tools > Port Scanner
- Description:** This web based port scanner will test whether common ports are open or down on a specific server.
- Ports Scanned:** 21, 22, 23, 25, 80, 110, 139, 1433, 1
- Domain / IP Address:** [Input Field] GO
- Port Scan Results:** Port scan results for s[REDACTED]ses[REDACTED].com.br  
=====
- Legend:**
  - ✓ - port is OPEN
  - ✗ - port is CLOSED
- Table:** A table showing port numbers, services, and status (OPEN or CLOSED).

PORT	Service	Status
21	FTP	✓
22	SSH	✓
23	Telnet	✗
25	SMTP	✗
53	DNS	✗
80	HTTP	✓
110	POP3	✗
139	NETBIOS	✗
143	IMAP	✗
443	HTTPS	✓
445	SMB	✗
1433	MSSQL	✗
1521	ORACLE	✗
3306	MySQL	✗
3389	Remote Desktop	✗

# Case 1

## Targeting the users

Screenshot of a web browser showing a JSON response from <https://hacked-emails.com/api?q=do%00las@se%00se%00a.com.br>. The response includes a table of results and a PasteBin link.

0:	<td>found</td> <td>do%00las@se%00se%00a.com.br</td>	found	do%00las@se%00se%00a.com.br
1:	<td>X%00O</td> <td>a guest</td>	X%00O	a guest

The PasteBin link (<https://astebin.com/e%00Pa>) shows the raw HTML of the table rows. A red arrow points to the MD5 hash value in the second row.

ASTEBIN + new paste trends API tools faq C

Save Copy

```
status: "found"
query: "do%00las@se%00se%00a.com.br"
results: 2
data:
  0:
    title: "mpst.net.br"
    author: "anon"
    verified: false
    date_created: "2017-06-05T00:00:00+00:00"
    date_leaked: "2017-06-05T00:00:00+00:00"
    emails_count: 30779094
    details: "https://hacked-emails.com/leak/anon-mpstnetbrspamlist2"
    source_url: "#"
    source_lines: 211366166
    source_size: 7445672117
    source_network: "darknet"
    source_provider: "anon"
  1:
    title: "X%00O"
    author: "a guest"
    verified: false
    date_created: "2016-04-20T00:00:00+00:00"
    date_leaked: "2016-04-20T00:00:00+00:00"
    emails_count: 2521
    details: "https://hacked-emails.com/leak/pb-e%00Pa"
    source_url: "http://pastebin.com/e%00Pa"
    source_lines: 12732
    source_size: 360205
    source_network: "clearnet"
    source_provider: "pastebin"
```

We found 1 hashes! [Timer: 719 m/s] Please find them below...

MD5 Hashes:
2d4%003ad010d4107ea493d49d

2d4%003ad010d4107ea493d49d MD5 : 210317



ate in our database, basically, it's a MD5 cracker / decryption tool.  
e August 2007.  
ked / decrypted. NOTE that space character is replaced with [space]:

**BEST PASSWORD EVER**

# Case 2

## A bank in South Africa

SHODAN org:"Bank of [REDACTED]"

Explore Downloads Reports Enterprise Access Contact Us

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 471

TOP COUNTRIES South Africa 471

TOP SERVICES HTTPS 188  
HTTP 93  
NTP 39  
IKE-NAT-T 30  
IKE 30

TOP ORGANIZATIONS Bank of [REDACTED] 471

TOP OPERATING SYSTEMS Windows 7 or 8 1

TOP PRODUCTS Microsoft IIS httpd 41  
Microsoft HTTPAPI httpd 21  
IBM HTTP Server 19  
ntpd 16  
Apache httpd 16

SSL Certificate

Issued By:  
- Common Name: Symantec Class 3 Secure Server CA - G4  
- Organization: Symantec Corporation  
Issued To:  
- Common Name: [REDACTED] bank  
- Organization: [REDACTED] Bank of [REDACTED]

HTTP/1.1 200 OK  
Server: Go Home WebServer  
Date: Thu, 09 Nov 2017 10:59:25 GMT  
Content-type: text/html  
Last-modified: Tue, 13 Jul 2004 09:53:53 GMT  
Content-length: 112  
Etag: W/"70-40F3b131"  
X-frame-options: SAMEORIGIN

Supported SSL Versions  
TLSv1, TLSv1.1, TLSv1.2

HTTP/1.0 302 Found  
Location: [REDACTED]  
Server: BigIP  
Connection: Keep-Alive  
Content-Length: 0

VPN (IKE)  
Initiator SPI: e5f858a0876af576  
Responder SPI: 0000000000000000  
Next Payload: Notification (N)

19 17 19 39 19 98

Details [REDACTED] vpn

# Case 2

```
1 IP,Port,Banner,Timestamp,Hostnames,Country,City,Operating System,Organization
2 19 [REDACTED].17,500,"VPN (IKE)
3
4 Initiator SPI: e5f858a0876af576
5 Responder SPI: 0000000000000000
6 Next Payload: Notification (N)
7 Version: 1.0
8 Exchange Type: Informational
9 Flags:
10   Encryption: False
11   Commit: False
12   Authentication: False
13 Message ID: df9cfeb6
14 Length: 40",2017-11-09T22:10:15.439304,,S[REDACTED],,[REDACTED] Bank of [REDACTED]
15 19 [REDACTED].23,23,"CC
16 *****
```

Find result - 11 hits

Search "cisco smart" (11 hits in 1 file)

```
C:\Users\Vlad\AppData\Local\Temp\7z00B872CAC\shodan_data.csv (11 hits)
Line 119: 19 .19,4786,Cisco Smart Install Client active,2017-11-09T17:16:49.362561,,Sou
Line 120: 19 .19,4786,Cisco Smart Install Client active,2017-11-09T16:57:29.711327,,Sou
Line 472: 19 .19,4786,Cisco Smart Install Client active,2017-11-08T16:08:25.379704,,Sou
Line 876: 19 .19,4786,Cisco Smart Install Client active,2017-11-08T05:41:29.283457,,Sou
Line 948: 19 .19,4786,Cisco Smart Install Client active,2017-11-08T01:39:46.902707,,Sou
Line 1151: 19 .19,4786,Cisco Smart Install Client active,2017-11-07T13:23:53.041177,,Sou
Line 1507: 19 .19,4786,Cisco Smart Install Client active,2017-11-06T14:38:54.451639,,Sou
Line 1597: 19 .19,4786,Cisco Smart Install Client active,2017-11-06T06:24:59.235452,,Sou
Line 2414: 19 .19,4786,Cisco Smart Install Client active,2017-10-30T17:14:45.088579,,Sou
Line 2585: 19 .19,4786,Cisco Smart Install Client active,2017-10-30T01:37:22.482338,,Sou
Line 3989: 19 .19,4786,Cisco Smart Install Client active,2017-10-10T07:36:37.920079,,Sou
```

Search ",23," (12 hits in 1 file)

C:\Users\Vlad\AppData\Local\Temp\7z00B872CAC\shodan\_data.csv (12 hits)

```
Line 15: 19 .3,23,"CC
Line 1564: 19 .11,23,"C
Line 1610: 19 .194,23,"C
Line 1705: 19 .181,23,"C
Line 2019: 19 .254,23,"C
Line 2440: 19 .33,23,"@
Line 2826: 19 .1,23,"C
Line 2924: 19 .186,23,"CC
Line 3078: 19 .134,23,"C
Line 3368: 19 .9,23,"C
Line 3634: 19 .1,23,"CCC
Line 3787: 19 .189,23,"C
```

Search ",22," (3 hits in 1 file)

C:\Users\Vlad\AppData\Local\Temp\7z00B872CAC\shodan\_data.csv (3 hits)

```
Line 1364: 19 .194,22,"SSH-1.99-Cisco-1.25
Line 2701: 19 .253,22,"SSH-1.99-Cisco-1.25
Line 2990: 19 .33,22,"SSH-1.99-Cisco-1.25
```

# Case 2

<https://github.com/Sab0tag3d/SIET>

## SIET

### Smart Install Exploitation Tool

Cisco Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches. You can ship a switch to a location, place it in the network and power it on with no configuration required on the device.

You can easily identify it using nmap: nmap -p 4786 -v 192.168.0.1

This protocol has a security issue that allows:

1. Change tftp-server address on client device by sending one malformed TCP packet.
2. Copy client's startup-config on tftp-server exchanged previously.
3. Substitute client's startup-config for the file which has been copied and edited. Device will reboot in defined time.
4. Upgrade ios image on the "client" device.
5. Execute random set of commands on the "client" device. IS a new feature working only at 3.6.0E and 15.2(2)E ios versions.

All of them are caused by the lack of any authentication in smart install protocol. Any device can act as a director and send malformed tcp packet. It works on any "client" device where smart install is enabled. It does not matter if it used smart install in the network or not.

Confirm from vendor: <https://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20170214-smi>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-smi>

Slides: <https://2016.zeronights.ru/wp-content/uploads/2016/12/CiscoSmartInstall.v3.pdf>

This simple tool helps you to use all of them.



# Cool Tools

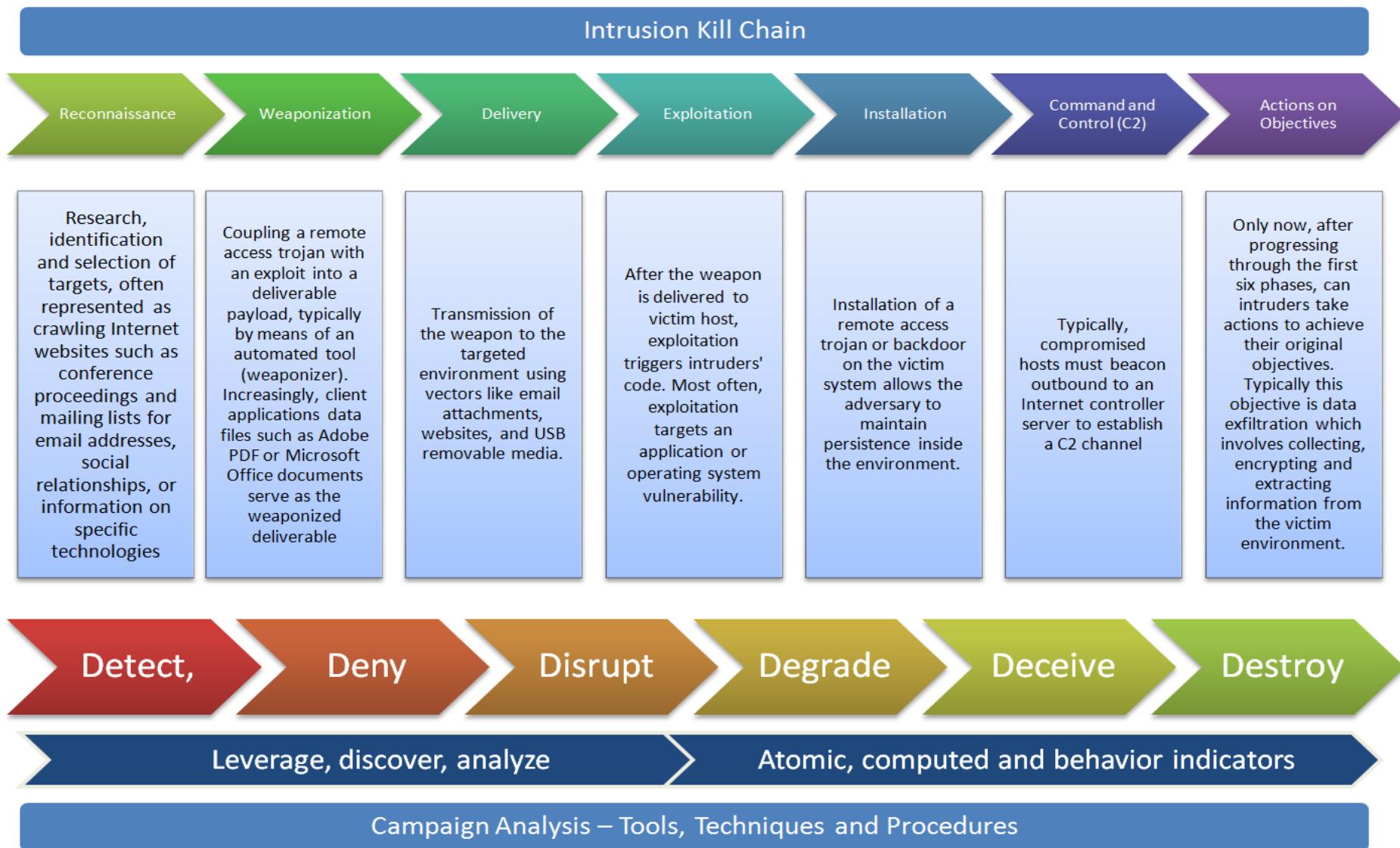
Shodan.io

Inteltechniques.com

Google.com

Notepad++

# APT attack internals



# Organizational response

Acknowledge  
and Report

- Prepare a comprehensive and truthful statement acknowledging the attack
- Prepare evidence for mandatory reporting
- Show that you a) know what happened and b) know how to deal with it
- Avoid «holding statements» and PR blurb

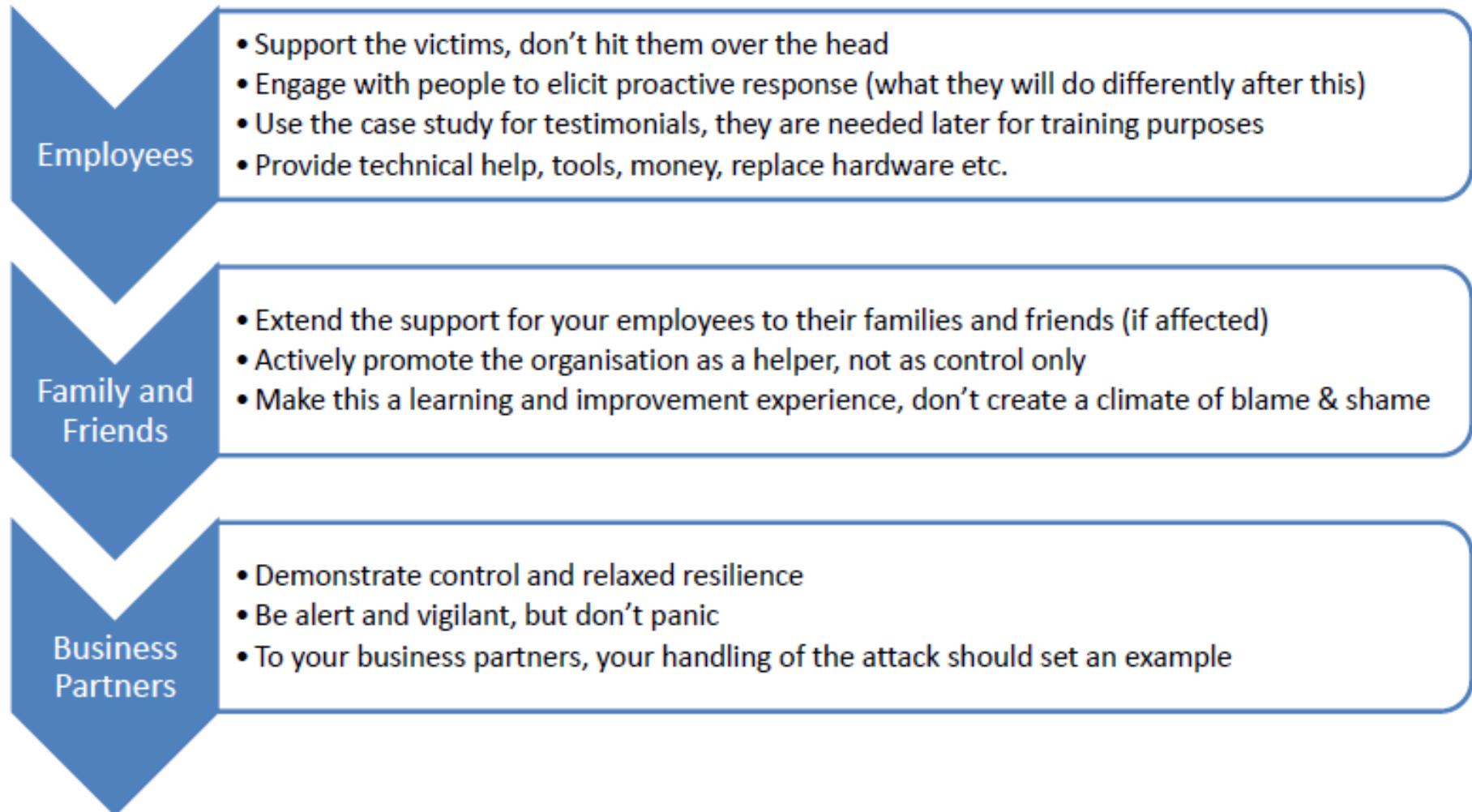
Stay in  
Charge

- Actively engage media, using an appropriate (!) and trained (!! ) spokesperson
- Prepare statements in non-tech language that outline progress in investigation and eradication
- Communicate internally – nothing worse than outsiders knowing more than insiders

Sell the  
Learnings

- Prepare a case study that demonstrates success
- Always admit that you are learning from this
- Make learning and improvement a public priority
- Avoid the blame game

# Social Response



# Thank you

# Q/A

# **SECURITATEA IN SISTEMELE IT**

---

## **NETWORK SECURITY**

Sl.dr.ing Tudor Mihai BLAGA

- **Secure Network Design**
  - **“The Grand Design”**
  - **Network Attacks**
  - **Firewalls**
  - **Network Security Devices**
- 

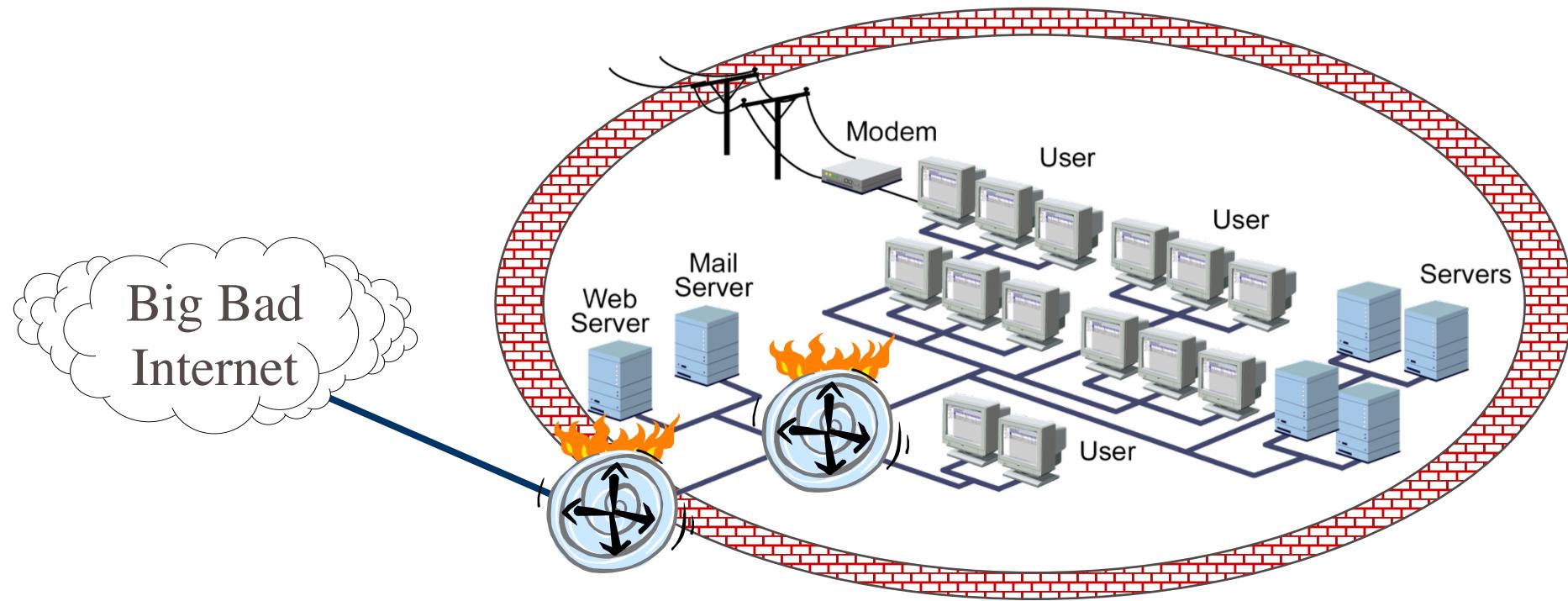
# AGENDA

# SECURE NETWORK DESIGN

---

# Crunchy Network Design

- Most networks focus on perimeter defense



# Network Design Objectives

- access from internal network to Internet
- protect internal network from external attacks
- defense-in-depth – tiered architecture
- control flow of information between systems

# Application Tiers

## Presentation tier

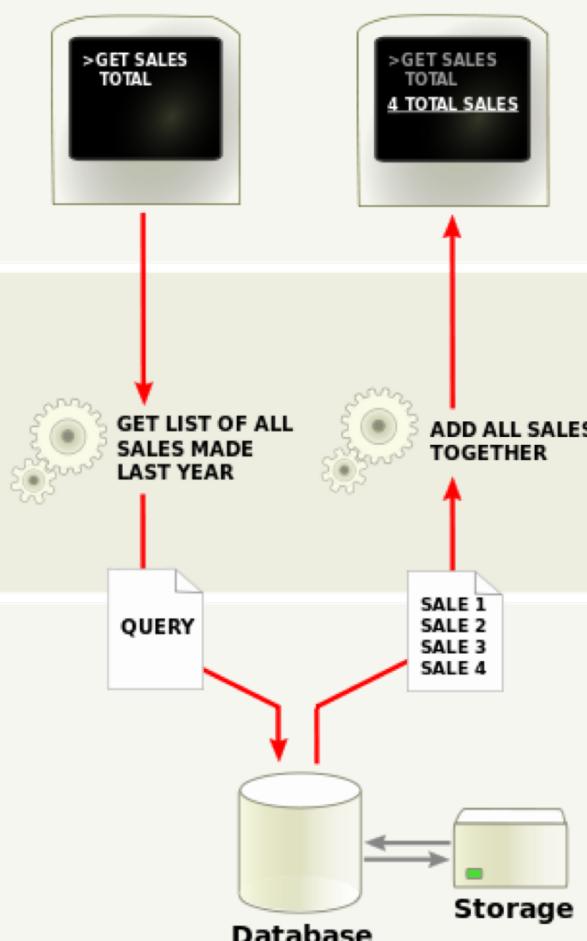
The top-most level of the application is the user interface. The main function of the interface is to translate tasks and results to something the user can understand.

## Logic tier

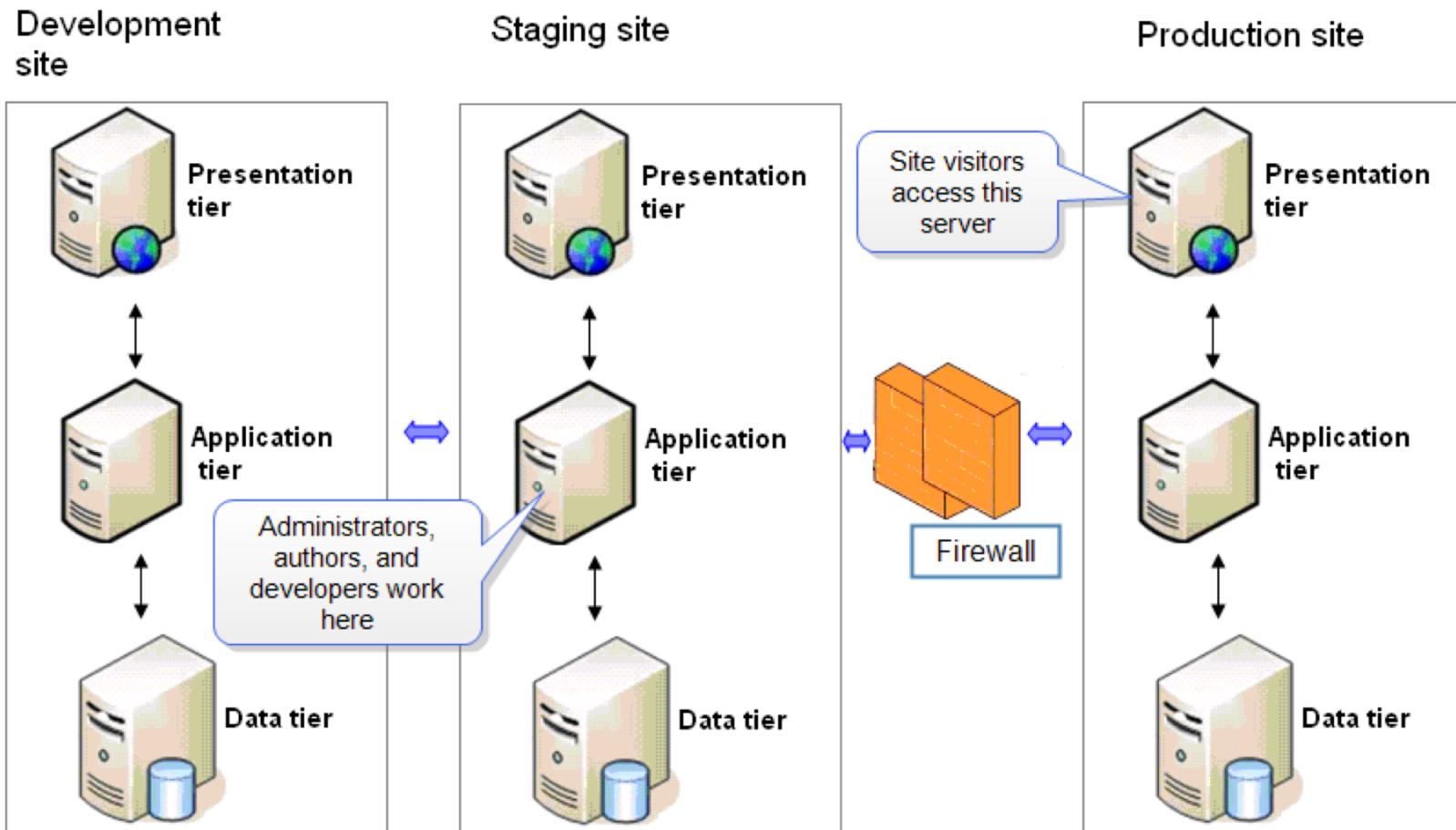
This layer coordinates the application, processes commands, makes logical decisions and evaluations, and performs calculations. It also moves and processes data between the two surrounding layers.

## Data tier

Here information is stored and retrieved from a database or file system. The information is then passed back to the logic tier for processing, and then eventually back to the user.



# Application Tiers



# Network Sections

- Public
  - resources on the Internet
  - cannot be trusted
- Semi-public
  - DMZ – Demilitarised Zone
  - Web, Mail, DNS servers
  - Must be reachable from the Internet
  - Might have access to the Internet
- Middleware – separate DMZ from private network
- Private
  - internal systems
  - Information should be protected

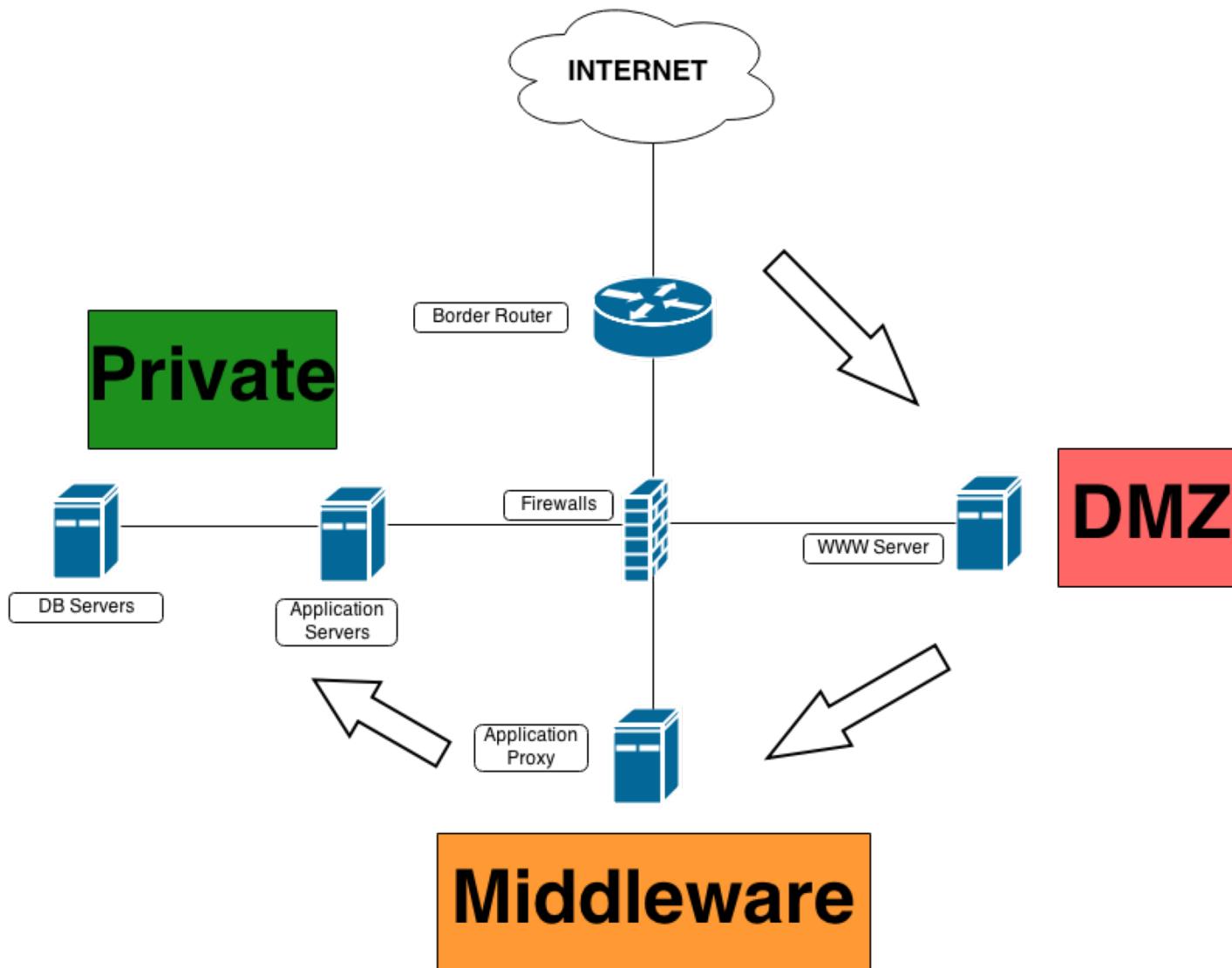
# Firewall Placement

- Where should we place it?
- Location where it can control access/restrict traffic that crosses boundaries of network sections:
  - from private systems to the Internet
  - from private systems to semi-public servers
  - from semi-public servers to the Internet
  - from the Internet to semi-public servers
- Ensure that outbound traffic is legitimate
- Control inbound connections
- Block inbound connections to private systems

# “THE GRAND DESIGN”

---

# Secure Network Design



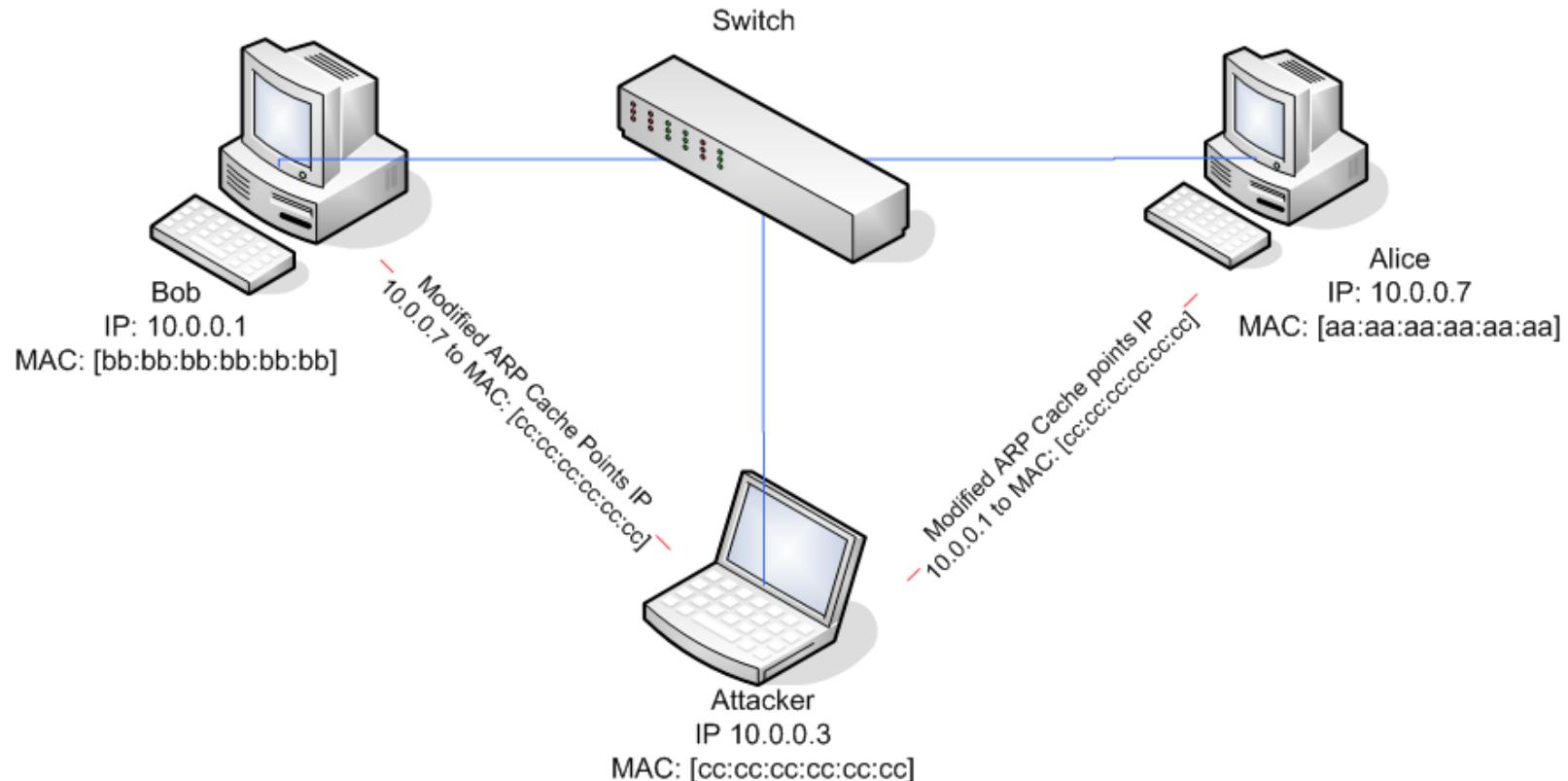
# NETWORK ATTACKS

---

# Security Flaws in IP

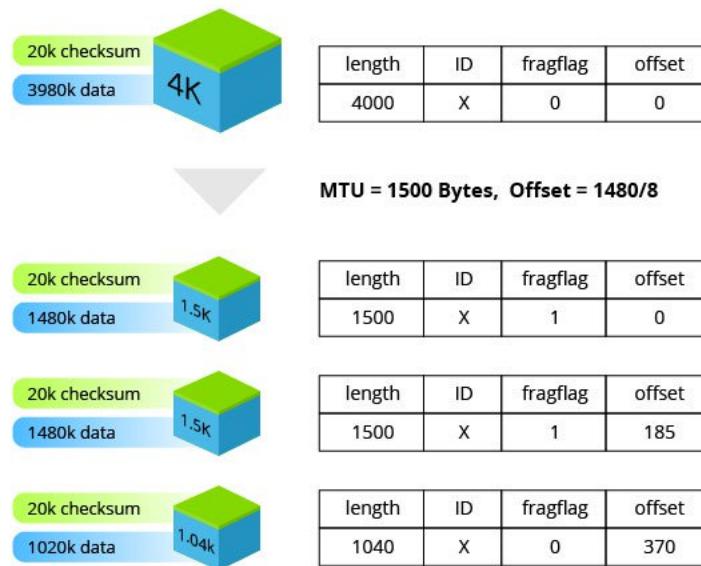
- The IP addresses are filled in by the originating host
  - Address spoofing
- Using source address for authentication
  - r-utilities (rlogin, rsh, rhosts etc..)
- IP fragmentation attack
  - End hosts need to keep the fragments till all the fragments arrive
- Traffic amplification attack
  - IP allows broadcast destination

# ARP Spoofing – Man-in-the-middle



# IP Fragmentation - 1

## IP Fragmentation and Reassembly (Example)



**Length** - The size of the fragmented datagram

**ID** - The ID of the datagram being fragmented

**Fragflag** - Indicates whether there are more incoming fragments

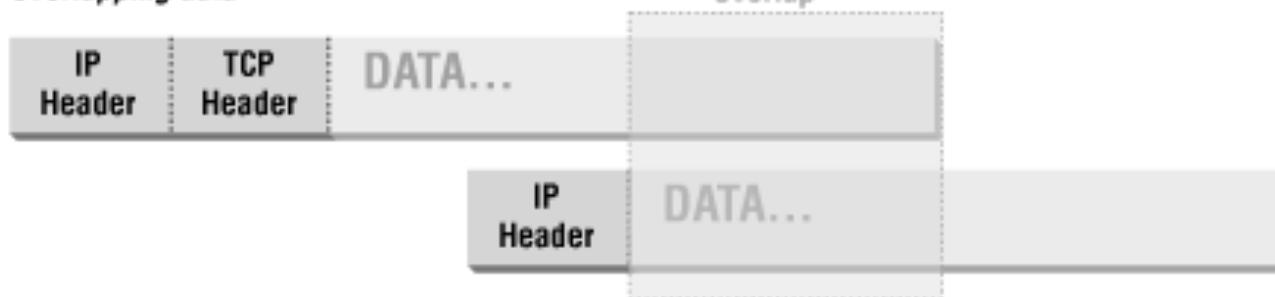
**Offset** - Details the order the fragments should be placed in during reassembly

# IP Fragmentation - 2

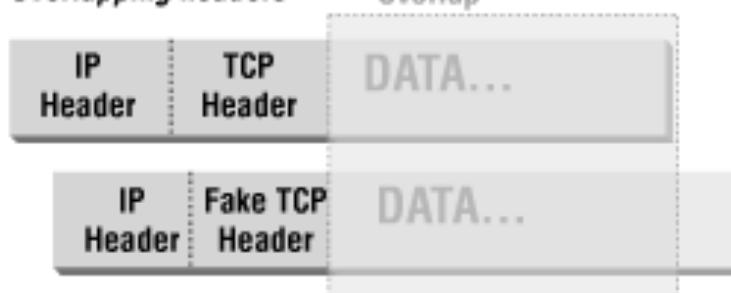
*Normal*



*Overlapping data*

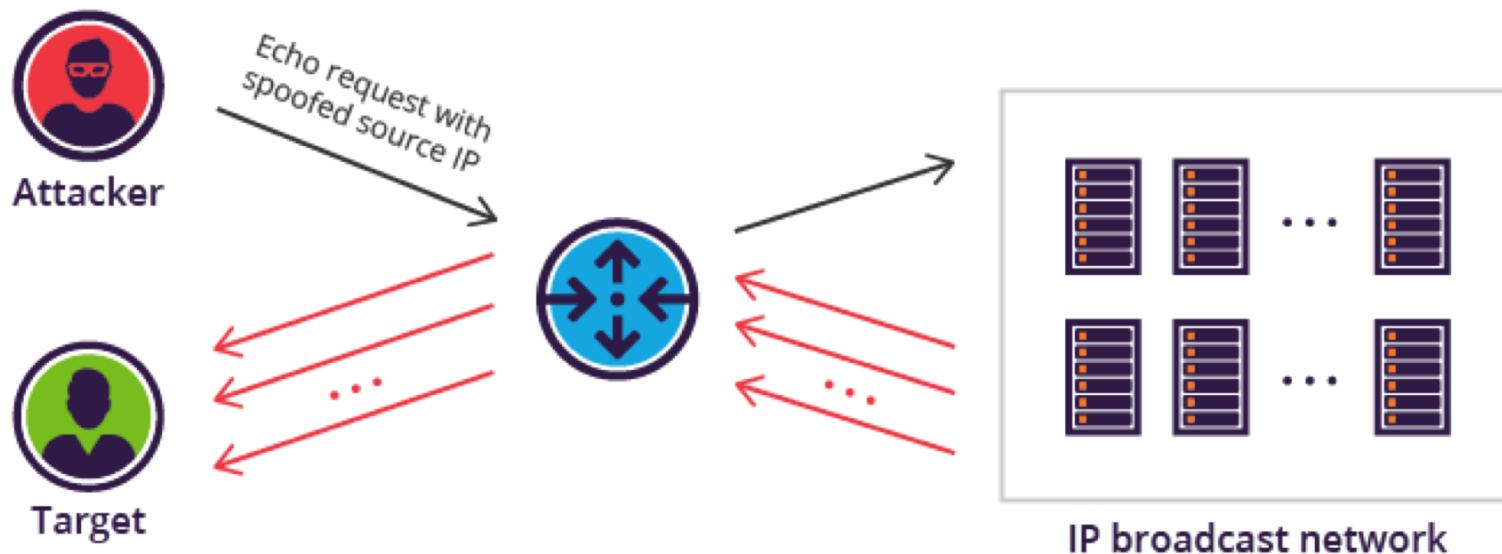


*Overlapping headers*



# Ping Flood & Smurf Attack

- IP Directed Broadcast

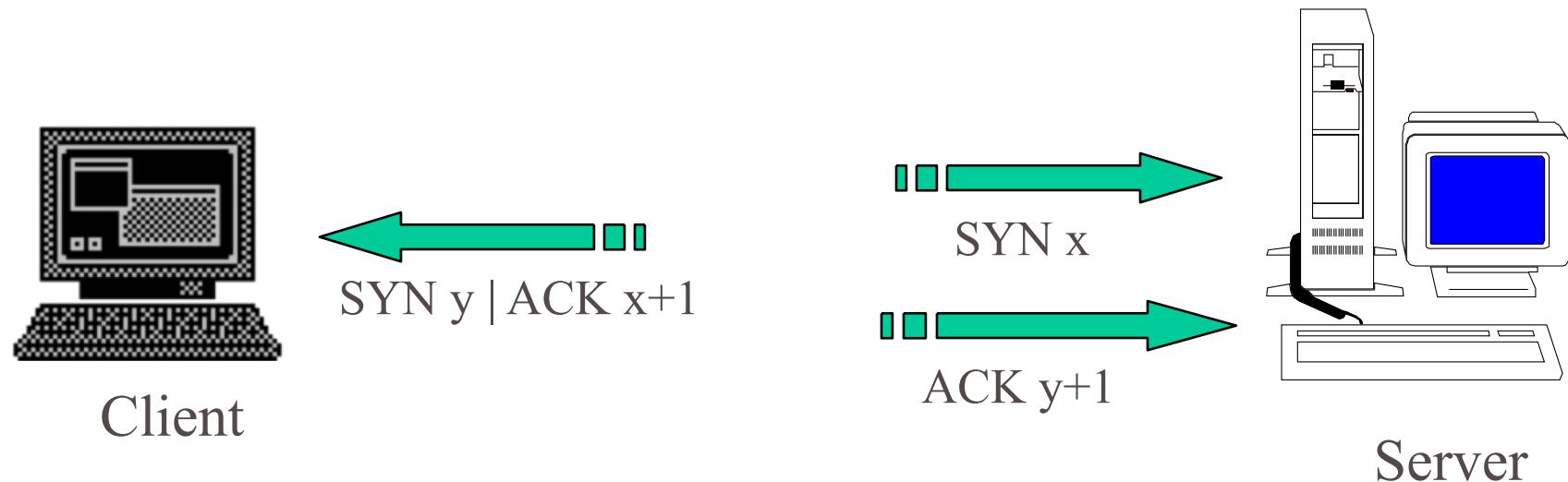


[source: Imperva]

# Ping of Death

- <https://www.youtube.com/watch?v=Y8kUGCiA6Y>

# TCP Attacks - 1



## Issues?

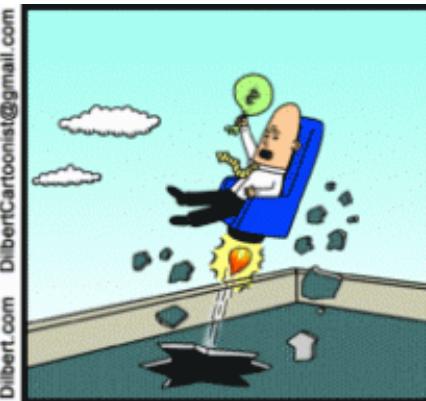
- Server needs to keep waiting for ACK  $y+1$
- Server recognizes Client based on IP address/port and  $y+1$

# TCP Attacks - 2

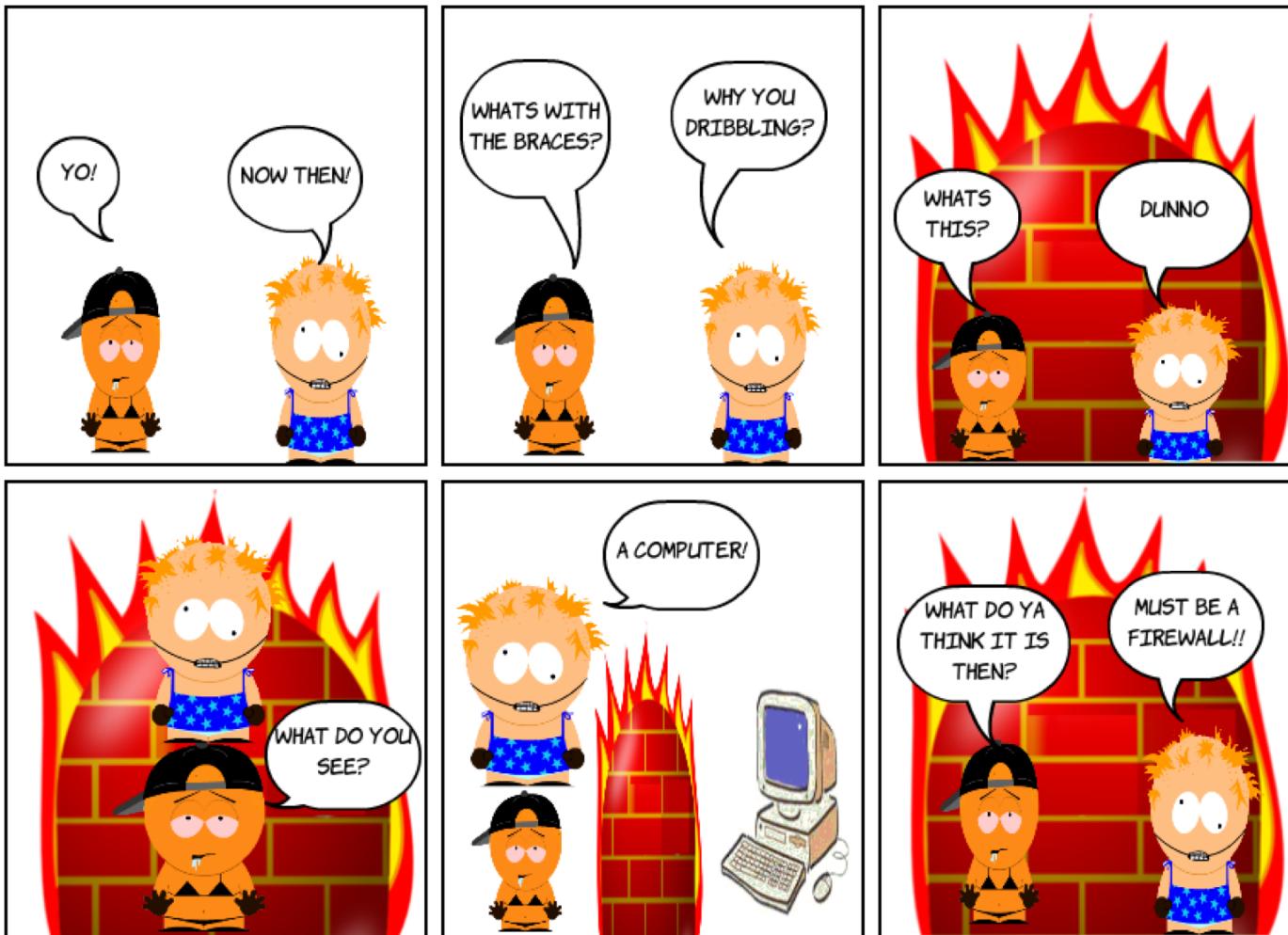
- TCP SYN Flooding
  - Exploit state allocated at server after initial SYN packet
  - Send a SYN and don't reply with ACK
  - Server will wait for 511 seconds for ACK
  - Finite queue size for incomplete connections
  - Once the queue is full it doesn't accept requests
- TCP Session Hijack
  - TCP packet valid based on: Address/Port/Sequence Number in window
  - How to get sequence number?
    - Sniff traffic
    - Guess it - Many earlier systems had predictable ISN
  - Inject arbitrary data to the connection
- TCP RST Attack
  - Tear down connection

# FIREWALLS

---



# Firewall



# Firewall Evolution

Packet Filtering -> Very Basic Filtering at L3|L4

Block/Allow

Packet Headers(Port|Protocol|Address)

Stateful Packet Filtering -> Basic Filtering at L3|L4

Block/Allow

Packet Headers(Port|Protocol|Address) + State

Application Gateway -> Advanced Filtering using Application Proxies at L7

Block/Allow/Inspect/Analyze

Communication State | Communications Information | User-level authentication

Stateful Inspection -> Medium Filtering at L3|L4|L7

Block/Allow/Inspect

Packet Headers(Port|Protocol|Address) + State + Partial Application Layer

UTM -> Control and Clean Traffic from Threats at L2|L3|L4|L5|L6|L7

Block/Allow/Shape/Detect/Prevent

Packet Headers(Port|Protocol|Address) + State + Medium Application Layer + Content + Signature + Flow + Partial User

NGFW -> Monitor, Manage and Clean Traffic from Threats meaningless of port and protocol at L2|L3|L4|L5|L6|L7

Block/Allow/Shape/Detect/Prevent/Identify/Monitor

Packet Headers(Port|Protocol|Address) + State + Deeper Application Layer + Content + Signature + Flow + Application + User

Specialized Application firewalls -> Advanced Protection at L7

Web Application Firewalls

Database Firewalls

# NETWORK SECURITY DEVICES

---

# Intrusion Detection System

- Passive sniffer – capture traffic
- Detects events of interest on the network
- Uses signature, anomaly or application/protocol analysis
- Signature analysis
  - Perform pattern matching
  - Rules indicate criteria in packets => events of interest
  - Rules applied to packets as they are received by IDS
  - Alerts are created when
- Security Analyst – alerts
  - **True Positive**/False Positive
  - **True Negative**/False Negative
- Network Based / Host Based

# IPS, Honeypots, ...

- IPS – Intrusion Prevention System
  - Stops attacks on the system and network (not only an alert)
  - Must be “in-line” of traffic path
  - Not a replacement for firewall, IDS, patching, ...
  - Cannot identify as many attacks as IDS (due to risk of false-positives)
- Honeypot
  - Server, virtual server, ... (not a production system)
  - No authorized activity on an honeypot
  - Understand how attackers break into a system
  - Identify attack traffic so that defense measures can be improved
  - Advanced technique!!!

# Security Best Practices in AWS

Stefan Mihail Magda  
Tudor Blaga

# Outline

- Introduction to Cloud Computing and AWS
- AWS responsibilities models
- Security Best Practices in AWS
- Security monitoring tools in AWS
- Security Incidents

# Introduction

- **Cloud Computing:**

- the end user has access to a shared pool of configurable computing resources
- The resources can be provisioned or released quickly with minimal management and effort from the end-user
- The access is granted through graphical web interfaces, CLI, APIs

# Introduction

- **Services Types:**

- *(SaaS) Software as a Service*
- *(PaaS) Platform as a Service*
- *(IaaS) Infrastructure as a Service*

# Introduction

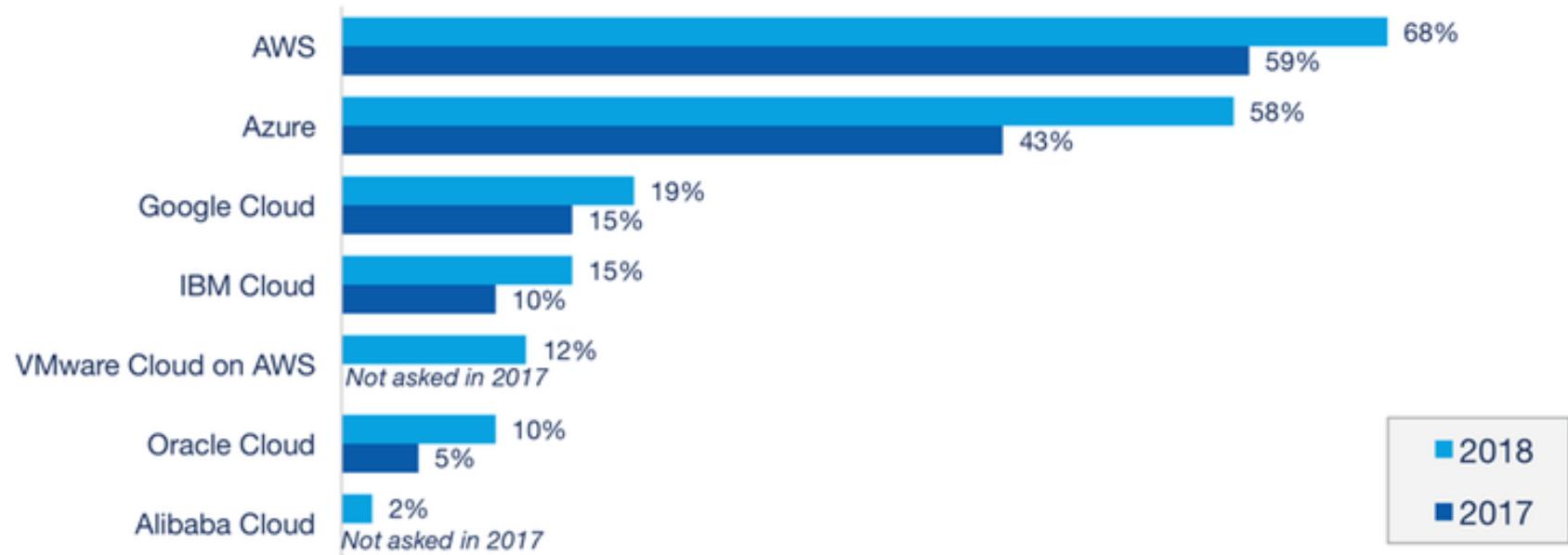
- **Trends :**

- infrastructure trends are more and more directed to be implemented in cloud, being it Private, Public or Hybrid
- more companies are migrating from private cloud adoption and embracing the services offered by many public providers, thus optimizing the costs

# Introduction

## Enterprise Public Cloud Adoption 2018 vs. 2017

% of Respondents Running Applications



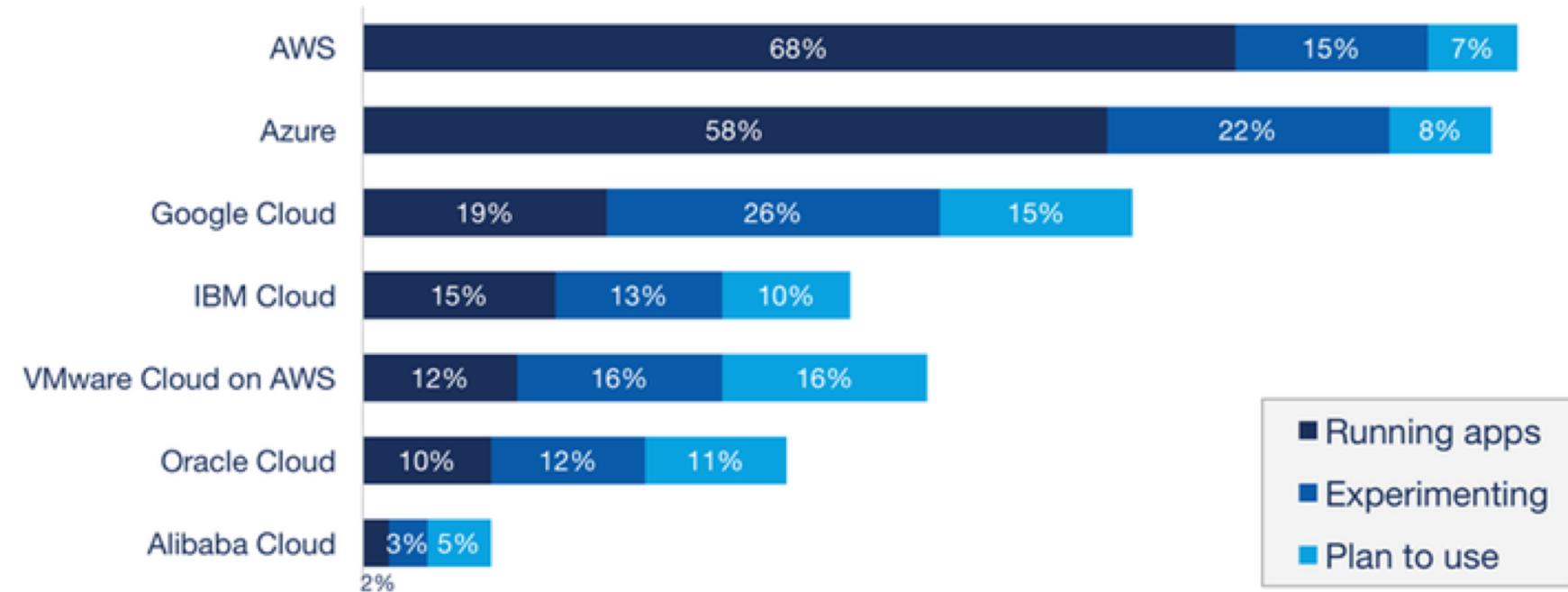
Source: RightScale 2018 State of the Cloud Report

**RIGHTSCALE**

# Introduction

## Enterprise Public Cloud Adoption

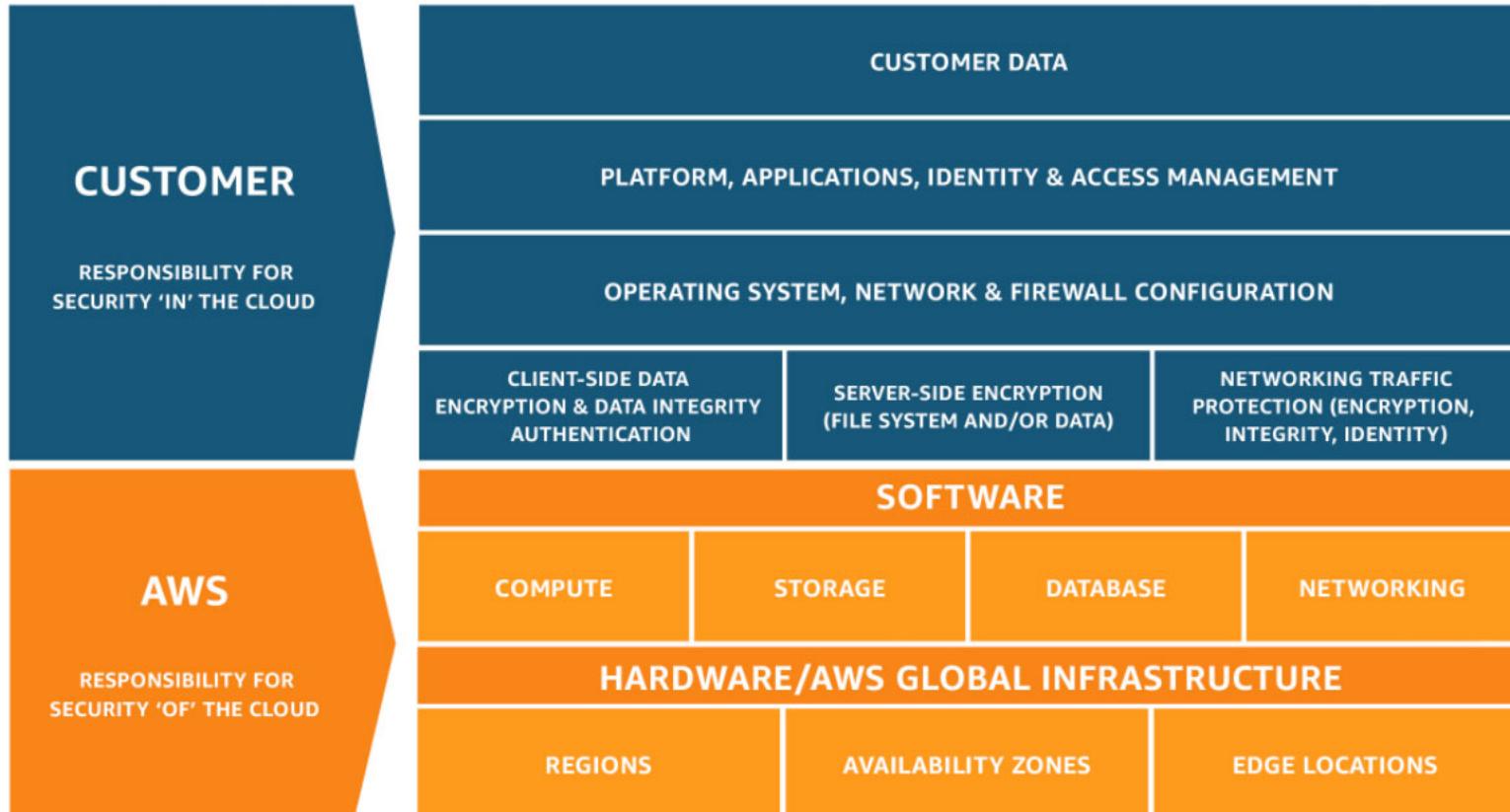
% of Respondents Running Applications



Source: RightScale 2018 State of the Cloud Report

# AWS responsibilities models

# AWS responsibilities models



# AWS responsibilities models

- **Inherited Controls:**
  - Physical and Environmental controls
- **Shared Controls:**
  - Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest OS and applications.
  - Configuration Management – AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
  - Awareness & Training - AWS trains AWS employees, but a customer must train their own employees.
- **Customer Specific:**
  - Service and Communications Protection or Zone Security which may require a customer to route or zone data within specific security environments.

# Quiz

- Q: Preventing or detecting when an AWS account has been compromised?
- A: Customer

# Quiz

- Q: Configuring AWS services (except AWS Managed Services) in a secure manner
- A: Customer

# Quiz

- Q: Ensuring network security (DoS, MITM, port scanning)
- A: Customer, AWS

# Quiz

- Q: Restricting access to AWS services or custom applications to only those users who require it
- A: Customer

# Quiz

- Q: Ensuring AWS and custom applications are being used in a manner compliant with internal and external policies
- A: Customer, AWS

# Quiz

- Q: Protecting against AWS zero day exploits and other vulnerabilities
- A: AWS

# Quiz

- Q: Providing environmental security assurance against things like mass power outages, earthquakes, floods, and other natural disasters
- A: AWS

# Quiz

- Q: Configuring AWS Managed Services in a secure manner
- A: AWS

# Quiz

- Q: Database patching
- A: AWS for RDS, Customer for EC2

# Security Best Practices in AWS

# Security Best Practices in AWS

- Securing IAM (Identity Access Management)

- Root account (used only in case of emergencies):

- Enable MFA
    - Disable or revoke any assigned access keys
    - Define a breaking glass procedure



IAM Users



Roles &  
Groups



IAM  
Permissions



MFA Token

# Security Best Practices in AWS

- Securing IAM (Identity Access Management)

- IAM Users and service accounts

- Enable MFA
- Assign users to groups least privilege
- Do not assign access keys for users

# Security Best Practices in AWS

- Securing IAM (Identity Access Management)
  - IAM Users and service accounts
    - Enable MFA
    - Assign users to groups least privilege
    - Do not assign access keys for users
    - Define a strong password policy
      - Min 10 characters
      - Alpha-numeric and symbols required
      - Expire after 90 days and prevent reuse
  - Note: If possible integrate the AWS Accounts with an SSO provider

# Security Best Practices in AWS

- Securing IAM – Least Privilege Model
- IAM Policies:
  - AWS Managed Policies
  - Customer Manager Policies
  - JSON format

# Security Best Practices in AWS

- **Version** – Specify the version of the policy language that you want to use.
- **Statement** – Use this main policy element as a container for the following elements. You can include more than one statement in a policy.
- **Sid** – Include an optional statement ID to differentiate between your statements.
- **Effect** – Use Allow or Deny to indicate whether the policy allows or denies access.
- **Principal** – Indicate the account, user, role, or federated user to which you would like to allow or deny access. If you are creating a policy to attach to a user or role, you cannot include this element. The principal is implied as that user or role.
- **Action** – Include a list of actions that the policy allows or denies.
- **Resource** – Specify a list of resources to which the actions apply.
- **Condition (Optional)** – Specify the circumstances under which the policy grants permission.

# Security Best Practices in AWS

## S3\_ReadOnly

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "s3:Get*",  
8         "s3>List*"  
9       ],  
10      "Resource": "*"  
11    }  
12  ]  
13 }
```

## S3\_FullAccess

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": "s3:*",  
7       "Resource": "*"  
8     }  
9   ]  
10 }
```

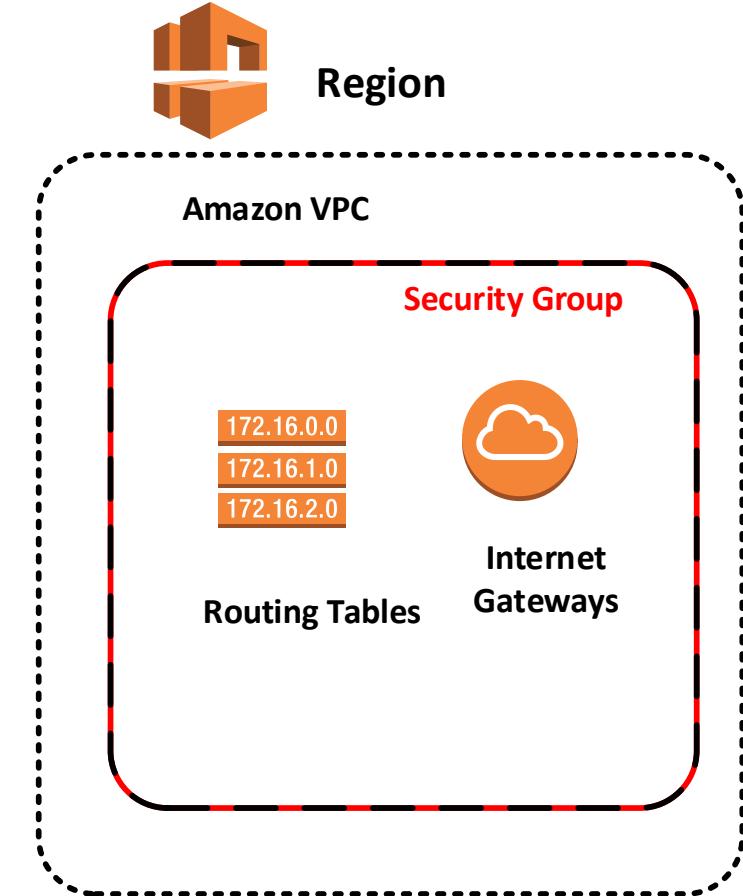
# Security Best Practices in AWS

- Securing VPC (Virtual Private Cloud)

- VPC Components:

- VPC CIDR
- Subnets
- Network ACLs
- Security Groups
- Routing tables
- Endpoints
- Gateways (Internet, EgressOnly, VPN)

EgressOnly, VPN)



# Security Best Practices in AWS

- Securing VPC (Virtual Private Cloud)

Identify used/ unused Regions

## 1. Unused Regions

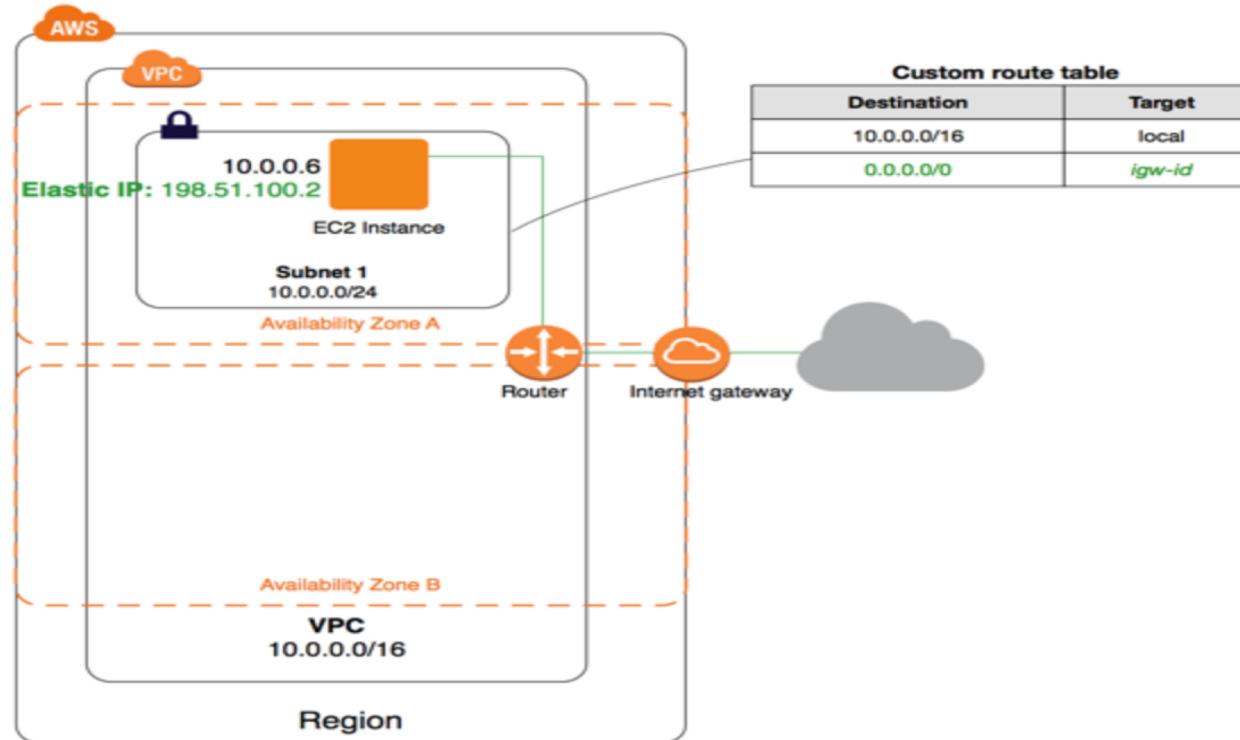
- Unset “Auto-assign Public IP” flag
- Remove default route to Internet Gateway
- Restrict egress traffic in Security Groups
- Deny All traffic at NACL level
- Remove any routing table entries
- Enable VPC FlowLogs

# Security Best Practices in AWS

- Securing VPC (Virtual Private Cloud)
  - 2. Used Regions:
    - Unset “Auto-assign Public IP” flag
    - Remove default route to Internet Gateway
    - Restrict ingress/egress traffic in Security Groups to used services only
    - Restrict ingress/egress traffic in NACLs to used protocols and ports only
    - Use AWS Endpoints for to communicate with AWS services (Using AWS backbone)
    - Enable VPC FlowLogs

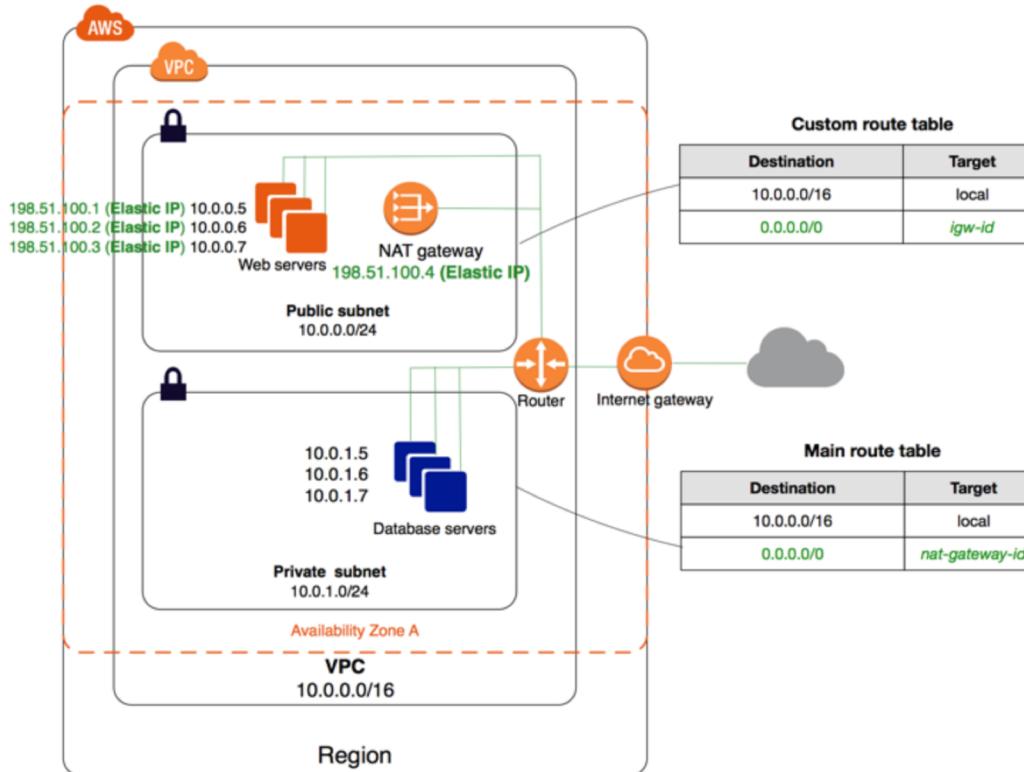
# Security Best Practices in AWS

- Securing VPC (Virtual Private Cloud)
  - Public subnets only



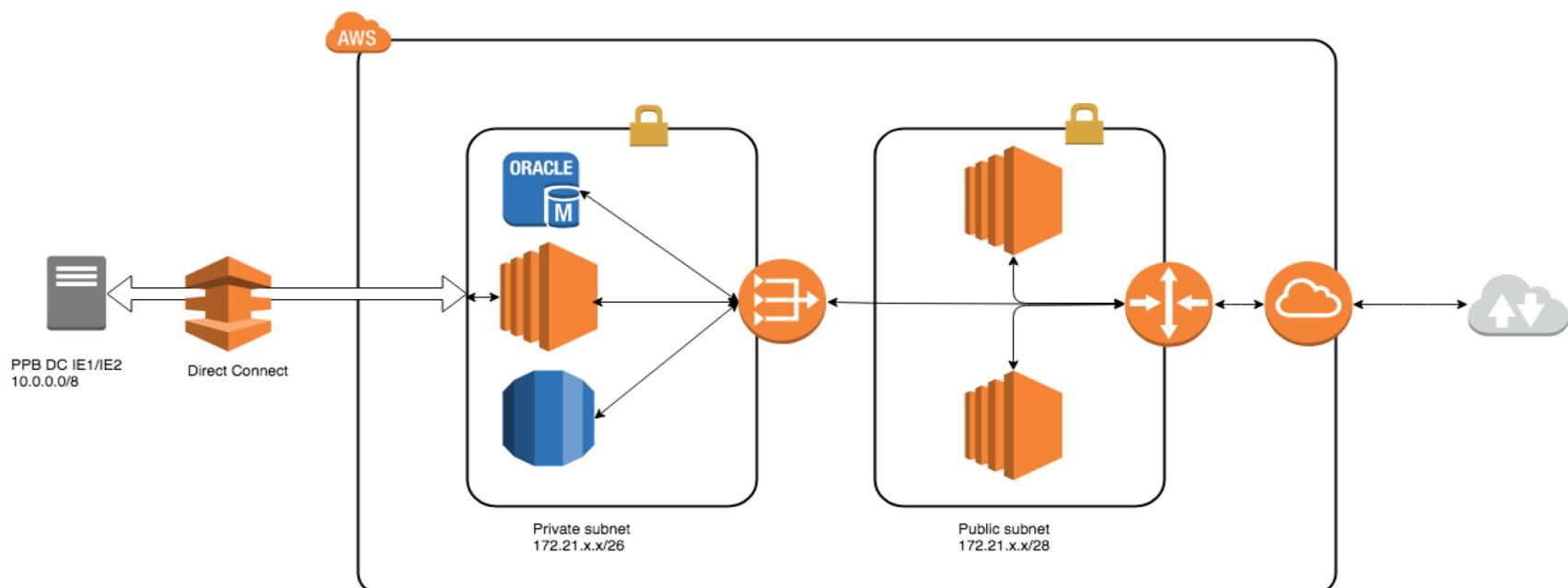
# Security Best Practices in AWS

- Securing VPC (Virtual Private Cloud)
  - Private & Public subnets



# Security Best Practices in AWS

- Securing VPC (Virtual Private Cloud)
  - DirectConnect (VPN) & Private & Public subnets



# Security Best Practices in AWS

- Compute(EC2) , storage and databases security
  - Always encrypt them (CMS, KMS) (i.e EC2, EBS, RDS)
  - S3 (Server-Side Encryption, Client-Side Encryption)
  - Restrict access to required IPs/ subnets only (SG, NACL)
  - Assign Public IPs only when required
  - Do not make an S3 bucket or object public
  - Update/ Upgrade OS and applications on a regular basis
  - Restrict access using IAM policies
  - Enable access logs

# Security Best Practices in AWS

- Secure Logging
  - Enable VPC Flow Logs
  - Enable CloudTrail
  - Enable AWS Config
  - Enable ELB/ALB logging
  - Set S3 bucket versioning and access logging
  - Use centralized logging for multiple accounts



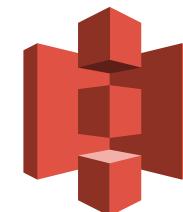
**Amazon CloudWatch**



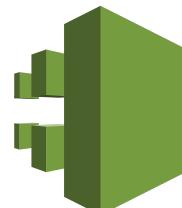
**AWS Config**



**VPC flow logs**



**Amazon S3**



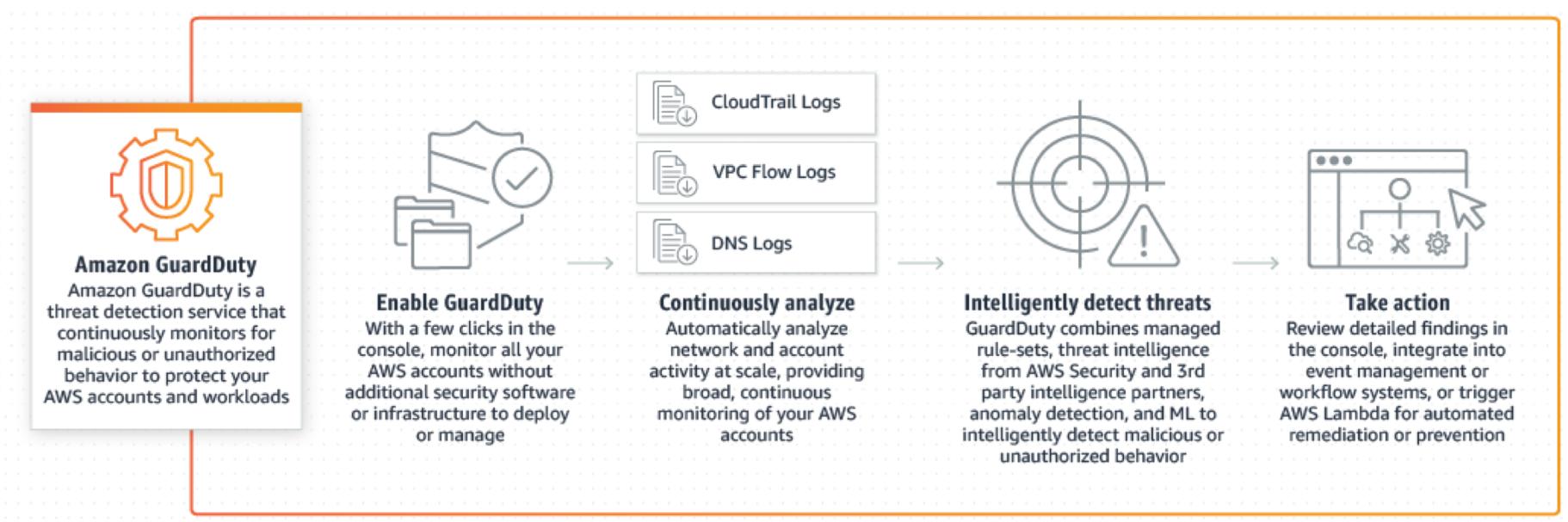
**AWS**

**CloudTrail**

# Security Monitoring Tools in AWS

# Security Monitoring Tools in AWS

## AWS GuardDuty



# Security Monitoring Tools in AWS

## AWS GuardDuty

### Current findings

Showing 59 of 59

26

31

2

**Actions** 

Saved filters

No saved filters

 *Include and exclude filter options are available on certain finding attributes in the details*

<input type="checkbox"/>	Finding	Last seen	Count
<input type="checkbox"/>	 [SAMPLE] Bitcoin-related domain queries from EC2 instance i-999999... [SAMPLE] EC2 instance i-99999999 communicating with known XorD...	2017-11-09 16:00:04 (9 days ago)	1
<input type="checkbox"/>	 [SAMPLE] Bitcoin-related domain name queried by EC2 instance i-99... [SAMPLE] IAM User GeneratedFindingUserName logged into the AW...	2017-11-09 16:00:04 (9 days ago)	1
<input type="checkbox"/>	 [SAMPLE] API GeneratedFindingAPIName was invoked from a Kali Li... [SAMPLE] Credentials for instance role GeneratedFindingUserName ... [SAMPLE] EC2 instance involved in RDP brute force attacks. [SAMPLE] Reconnaissance API GeneratedFindingAPIName was invo...	2017-11-09 16:00:04 (9 days ago)	1
<input type="checkbox"/>	 [SAMPLE] Blackholed domain name queried by EC2 instance i-99999... [SAMPLE] API GeneratedFindingAPIName was invoked from a known...	2017-11-09 16:00:04 (9 days ago)	1
<input type="checkbox"/>	 [SAMPLE] Unusual EC2 instance i-99999999 type launched.	2017-11-09 16:00:04 (9 days ago)	1

# Security Monitoring Tools in AWS

## AWS Inspector

- = There is an Inspector Agent running on the EC2 machines hosting the application which monitors for:
  - Common Vulnerabilities and Exposures
  - Network Security Best Practices
  - Authentication Best Practices
  - Operating System Security Best Practices
  - Application Security Best Practices
  - PCI DSS 3.0 Assessment

# Security Monitoring Tools in AWS

## AWS Inspector

**Define an assessment**

An assessment is the process of discovering potential security issues (findings) through the analysis of your application's behavior against selected rule packages. [Learn more.](#)

**Assessment name\***

**Rule packages\***  ×  
 ×  
 ▼

Amazon Inspector assesses the application against selected rule package(s). [Learn more.](#)

**Duration\***  ▼

The default Amazon Inspector assessment duration is 24 hours. You can modify the duration, but note that assessments with longer durations can deliver fuller sets of findings.

**\*Required** [Cancel](#) [Previous](#) **Next**

# Security Monitoring Tools in AWS

## AWS Inspector

### Amazon Inspector - Findings

Inspector findings are potential security issues discovered during Inspector's assessment of the specified application. [Learn more](#).

[Add/Edit attributes](#)

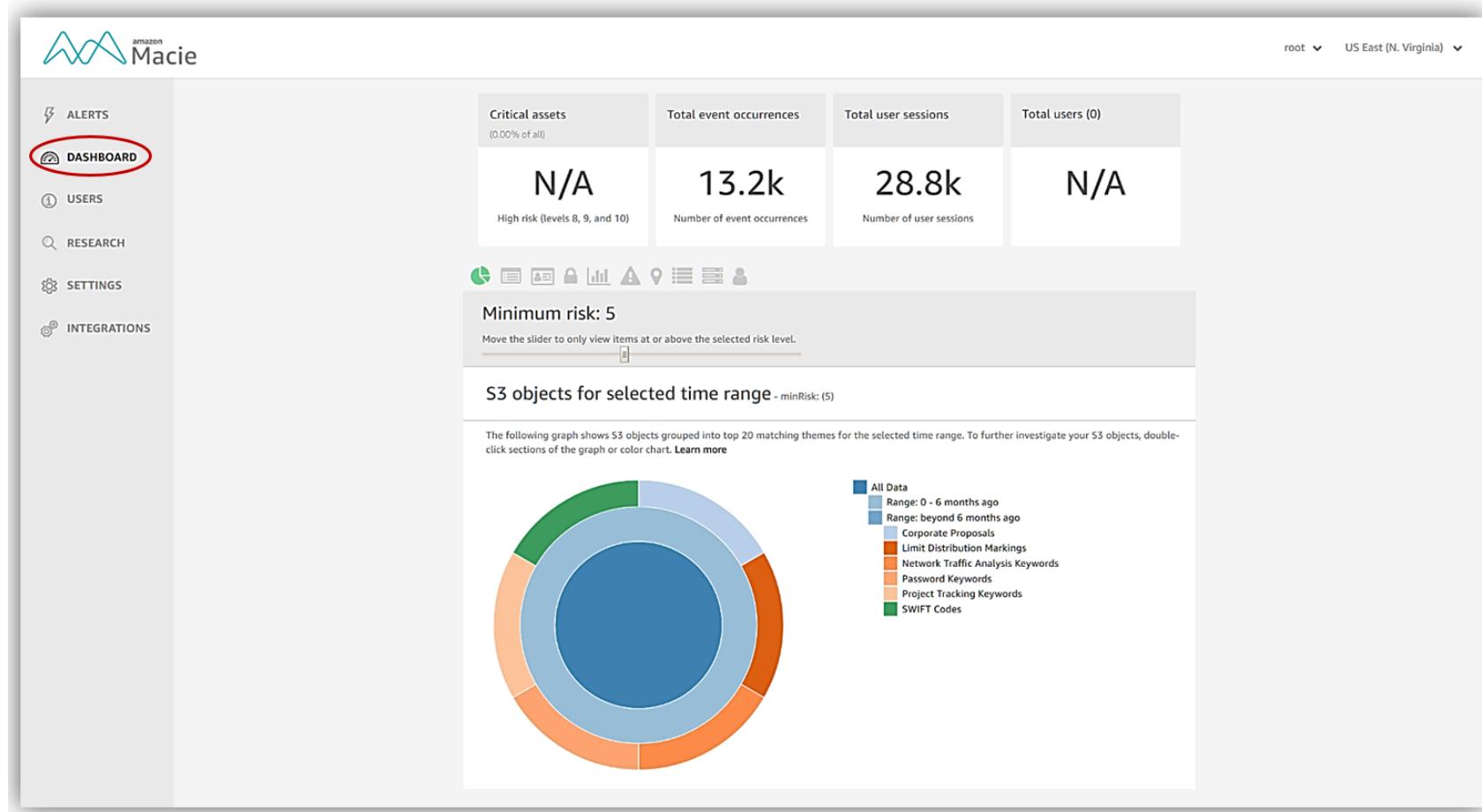
Last updated on September 24, 2015 4:12:42 PM (20m ago)



Viewing 1-10 of 24					
	Severity	Application	Assessment	Rule package	Finding
<input type="checkbox"/>	High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	Instance i-aac4c46f is configured without a password.
<input type="checkbox"/>	High ⓘ	Customer Processing	Comprehensive-Assessment	Common Vulnerabilities and Exposures	Instance i-aac4c46f is vulnerable to known security issues.
<input type="checkbox"/>	High ⓘ	Customer Processing	Comprehensive-Assessment	Authentication Best Practices	No password complexity mechanism is present.
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Initial app	PCI DSS 3.0 Readiness	Instance i-aac4c46f was found to be compliant with PCI DSS 3.0.
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Initial app	PCI DSS 3.0 Readiness	The machine i-aac4c46f was found to be compliant with PCI DSS 3.0.
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Comprehensive-Assessment	Operating System Security Best Practices	No potential security issues found.
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	The machine i-aac4c46f was found to be compliant with PCI DSS 3.0.
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Comprehensive-Assessment	Network Security Best Practices	No potential security issues found.
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Comprehensive-Assessment	PCI DSS 3.0 Readiness	Instance i-aac4c46f was found to be compliant with PCI DSS 3.0.
<input type="checkbox"/>	Informational ⓘ	Customer Processing	Initial app	PCI DSS 3.0 Readiness	A machine with Instance ID i-aac4c46f was found to be compliant with PCI DSS 3.0.

# Security Monitoring Tools in AWS

## AWS Macie



The screenshot shows the AWS Macie dashboard. On the left sidebar, the 'DASHBOARD' option is selected and highlighted with a red circle. The main area displays various metrics and a donut chart.

Critical assets (0.00% of all)	Total event occurrences	Total user sessions	Total users (0)
N/A	13.2k	28.8k	N/A

Below the metrics, there is a section titled 'S3 objects for selected time range - minRisk: (5)'. It includes a note: 'The following graph shows S3 objects grouped into top 20 matching themes for the selected time range. To further investigate your S3 objects, double-click sections of the graph or color chart.' A 'Learn more' link is provided.

The donut chart is divided into several segments, each representing a different theme. The legend on the right lists the categories:

- All Data
- Range: 0 - 6 months ago
- Range: beyond 6 months ago
- Corporate Proposals
- Limit Distribution Markings
- Network Traffic Analysis Keywords
- Password Keywords
- Project Tracking Keywords
- SWIFT Codes

## AWS Trusted Advisor

Trusted Advisor free checks

- Checking the Security Groups for unrestricted permissions
- Checking the IAM service for password policies if the root account MFA
- Detects if the EBS or RDS snapshots are marked as public.

### Paid Checks

- Checks S3 buckets have no loose permissions.
- Checks CloudTrail is on.
- Checks ELB listeners use good SSL policies.
- Checks if SSL certs will expire soon.
- Checks if IAM keys have been rotated in the past 90 days.

## Trusted Advisor Dashboard



### Cost Optimization



0 ✓ 0 ▲ 0 !

### Performance



1 ✓ 0 ▲ 0 !

### Security



5 ✓ 0 ▲ 0 !

### Fault Tolerance



0 ✓ 0 ▲ 0 !

# Security Monitoring Tools in AWS

## AWS Trusted Advisor

### Recommended Actions

 <a href="#">Security Groups - Specific Ports Unrestricted</a>	Refreshed: 9 minutes ago Previous status: Green	 
<p>Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.</p> <p>0 of 2 security group rules allow unrestricted access to a specific port.</p>		
 <a href="#">IAM Use</a>	Refreshed: 9 minutes ago Previous status: Green	 
<p>Checks for your use of AWS Identity and Access Management (IAM).</p> <p>At least one IAM user has been created for this account.</p>		
 <a href="#">MFA on Root Account</a>	Refreshed: 9 minutes ago Previous status: Green	 
<p>Checks the root account and warns if multi-factor authentication (MFA) is not enabled.</p> <p>MFA is enabled on the root account.</p>		
 <a href="#">Service Limits</a>	Refreshed: 9 minutes ago Previous status: Green	 
<p>Checks for usage that is more than 80% of the service limit.</p> <p>0 of 55 items have usage that is more than 80% of the service limit.</p>		
 <a href="#">Amazon EBS Public Snapshots</a>		 
<p>Checks the permission settings for your Amazon Elastic Block Store (Amazon EBS) volume snapshots and alerts you if any snapshots are marked as public.</p> <p>0 EBS snapshots are marked as public.</p>		

# Security Monitoring Tools in AWS

## Scout2

Scout2   Compute ▾   Database ▾   Management ▾   Messaging ▾   Network ▾   Security ▾   Storage ▾   Regions ▾   Filters ▾   Help ▾

### Dashboard

Summary:

Service	# of Rules	# of Findings	# of Checks
Cloudformation	1	0	0
CloudTrail	5	0	44
CloudWatch	0	0	0
EC2	21	45	474

# Security Monitoring Tools in AWS

## Scout2

Scout2   Compute ▾   Database ▾   Management ▾   Messaging ▾   Network ▾   Security ▾   Storage ▾   Regions ▾   Filters ▾   Help ▾

### EC2 Dashboard

<b>Default security groups in use</b>  • Security groups checked: 16 • Security groups flagged: 0	<b>Non-empty rulesets for default security groups</b>  • Rulesets checked: 32 • Rulesets flagged: 28	<b>DNS port open to all</b>  • Rules checked: 20 • Rules flagged: 0
<b>MongoDB port open to all</b>  • Rules checked: 20 • Rules flagged: 0	<b>MsSQL port open to all</b>  • Rules checked: 20 • Rules flagged: 0	<b>MySQL port open to all</b>  • Rules checked: 20 • Rules flagged: 0
<b>NFS port open to all</b>  • Rules checked: 20 • Rules flagged: 0	<b>Oracle DB port open to all</b>  • Rules checked: 20 • Rules flagged: 0	<b>PostgreSQL port open to all</b>  • Rules checked: 20 • Rules flagged: 0
<b>RDP port open to all</b>  • Rules checked: 20 • Rules flagged: 0	<b>SMTP port open to all</b>  • Rules checked: 20 • Rules flagged: 0	<b>SSH port open to all</b>  • Rules checked: 20 • Rules flagged: 2

# Security Monitoring Tools in AWS

## Security Monkey

It consists in 3 components:

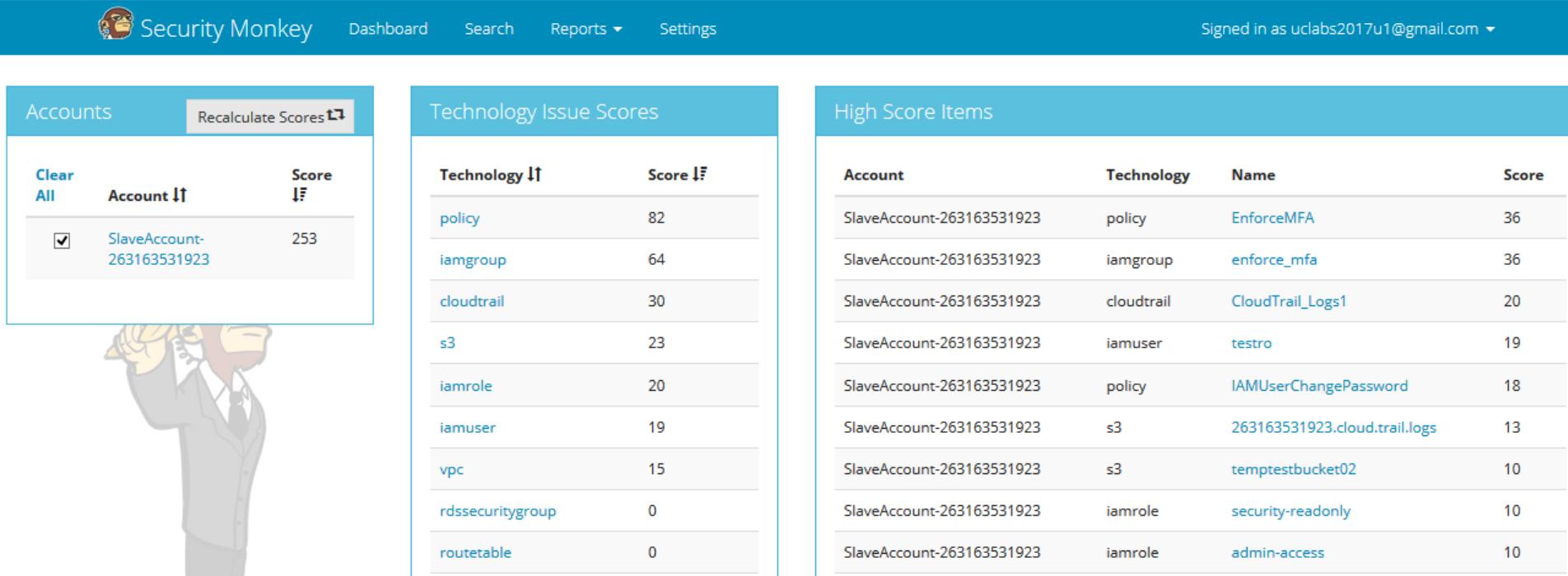
**The watcher** component monitors a given account by slurping the configuration. It is able to detect and record changes on any services configuration, storing them on the database.

**The auditor** compares the previously slurped AWS configuration against best practices or custom administrator rules. After the comparison it label each change or configuration based on a risk model (1 = Low risk, 10 = High risk), helping the administrator to focus his attention on the most important issues that need to be fixed.

**The notify-er** component enables a user or group of users to receive alerts when a particular resource has changed or when a security deviation happened

# Security Monitoring Tools in AWS

## Security Monkey



The screenshot shows the Security Monkey interface with three main panels:

- Accounts:** Displays a table with one account listed: SlaveAccount-263163531923 (Score: 253). Includes a "Clear All" button and a "Recalculate Scores" button.
- Technology Issue Scores:** Displays a table of technology issues and their scores:
 

Technology	Score
policy	82
iamgroup	64
cloudtrail	30
s3	23
iamrole	20
iamuser	19
vpc	15
rdssecuritygroup	0
routetable	0
- High Score Items:** Displays a table of high-scored items across different accounts and technologies:
 

Account	Technology	Name	Score
SlaveAccount-263163531923	policy	EnforceMFA	36
SlaveAccount-263163531923	iamgroup	enforce_mfa	36
SlaveAccount-263163531923	cloudtrail	CloudTrail_Logs1	20
SlaveAccount-263163531923	iamuser	testro	19
SlaveAccount-263163531923	policy	IAMUserChangePassword	18
SlaveAccount-263163531923	s3	263163531923.cloud.trail.logs	13
SlaveAccount-263163531923	s3	temptestbucket02	10
SlaveAccount-263163531923	iamrole	security-readonly	10
SlaveAccount-263163531923	iamrole	admin-access	10

# Security Monitoring Tools in AWS

## Security Monkey

Security Monkey    Dashboard    Search    Reports ▾    Settings    Signed in as uclabs2017u1@gmail.com ▾

Search		Items							Actions					
									AutoRefresh	false	Refresh Now	Export	⚙️	1-15 of 15
Region	Filter	Select	Active	Technology	Account	Account Type	Region	Name	Issues	Score	First Seen	Last Modified		
eu-west-1		<input type="checkbox"/>	<input checked="" type="checkbox"/>	s3	SlaveAccount-263163531923	AWS	eu-west-1	temptestbucket02	3	10	7/6/17 6:52 PM	7/6/17 6:52 PM		
		<input type="checkbox"/>	<input checked="" type="checkbox"/>	s3	SlaveAccount-263163531923	AWS	eu-west-1	263163531923.cloud.trail.logs	3	13	7/6/17 6:52 PM	7/6/17 6:52 PM		
		<input type="checkbox"/>	<input checked="" type="checkbox"/>	rdssecuritygroup	SlaveAccount-263163531923	AWS	eu-west-1	default	0	0	7/6/17 6:52 PM	7/6/17 6:52 PM		
		<input type="checkbox"/>	<input checked="" type="checkbox"/>	routetable	SlaveAccount-263163531923	AWS	eu-west-1	rtb-4a516f2d	0	0	7/6/17 6:51 PM	7/6/17 6:51 PM		
		<input type="checkbox"/>	<input checked="" type="checkbox"/>	vpc	SlaveAccount-263163531923	AWS	eu-west-1	None (vpc-2cea4b4b)	0	0	7/6/17 6:50 PM	7/6/17 6:50 PM		

# Security Incidents

# Security Incidents

# References

1. Cloud Computing Trend: <http://www.righscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey>
2. CIS Amazon Web Services Foundations  
[https://d0.awsstatic.com/whitepapers/compliance/AWS\\_CIS\\_Foundations\\_Benchmark.pdf](https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf)
3. AWS Security Best Practices  
[https://d0.awsstatic.com/whitepapers/Security/AWS\\_Security\\_Best\\_Practices.pdf](https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf)
4. Amazon Web Services documentation: <http://docs.aws.amazon.com>
5. Amazon Web Services security products: <https://aws.amazon.com/products/security/>
6. Security Monkey documentation: [https://github.com/Netflix/security\\_monkey](https://github.com/Netflix/security_monkey)

# Security in IT Systems: Linux Security (C7)

Gabriel Lazăr

November 21, 2014

## 1 Keeping system secure with updates

## 2 System services

## Keeping system secure with updates

# Intro

- staying *up-to-date*: critical issue for keeping your O.S. secure
- new exploits are being discovered & distributed every day
- widespread, automated attacks - targeting *unpatched* systems
- vendors / software authors release patches to correct these problems
- new patches / software versions may impact the functionality of the O.S.
- some patches require reboot / downtime
- while needed, patches should be tested first on a non-production system

# The Linux Operating System (*Distribution*):

- the Linux kernel
- software collection
- installer

## Software management:

- applications: distributed as *packages* in distribution specific format
- third-party repositories (packages in similar format)
- manual source code download, compilation and installation

# Example 1

- classic method
- most difficult way

## Installing software from source

```
$ wget http://ftp.gnu.org/pub/gnu/wget/wget-1.16.tar.xz
$ tar -xvf wget-1.16.tar.xz
$ cd wget-1.16
$ ./configure --prefix=/usr/local
$ make
$ sudo make install
```

## Example 1 (cont.)

*Advantages:*

- can decide what precise software version (and patches) to install
- can customize every build feature (enable/disable functionality)

*Problems:*

- manual patching on (security) updates
- manual installation of dependencies (software libraries or tools on which wget depends)
- uninstall process: prone to errors (`make uninstall` target may be poorly written)
- untracked files, spread through filesystem paths

## Example 2:

A couple of terms:

- rpm - RedHat Package Manager
- yum - Yellowdog Updater Modified - “an interactive, rpm based, package manager” (yum manual page)

Installing a **package** (RedHat/Fedora/CentOS *distribution*)

```
$ sudo yum install wget
```

## Example 2: (cont.)

### *Advantages:*

- easy installation, update, uninstall process
- dependencies are automatically handled
- official package repositories can be trusted (if signed)
- files are tracked

### Removing a package (RedHat):

```
$ sudo yum remove wget
```

## Example 2: (cont.)

### Tracking package files:

```
$ rpm -ql wget
/etc/wgetrc
/usr/bin/wget
/usr/share/doc/wget-1.14
/usr/share/doc/wget-1.14/AUTHORS
/usr/share/doc/wget-1.14/COPYING
/usr/share/doc/wget-1.14/MAILING-LIST
/usr/share/doc/wget-1.14/NEWS
/usr/share/doc/wget-1.14/README
/usr/share/doc/wget-1.14/sample.wgetrc
/usr/share/info/wget.info.gz
...
$ whereis wget
wget: /bin/wget /usr/bin/wget /usr/share/man/man1/wget.1.gz
$ rpm -qf /bin/wget
wget-1.14-5.fc18.i686
```

## Example 2: (cont.)

*Issues:*

- can't choose an exact software version
- can't easily enable/disable desired features (no building control)
- can't *go back* to previous package versions, most of the time (due to dependencies version requirements)

## Summary:

- keep your Linux distribution updated
- follow the Linux security advisory sites/mailing lists for your distro
- use pre-compiled software from trusted repositories when possible
- check for signs of tampering:

```
$ sudo rpm -Va  
S.5....T.  c /etc/vimrc  
...
```

## Tasks:

- ① Document the format of the `rpm -Va` output lines
- ② In a RedHat-compatible distribution, how can you remove unused packages, which were installed as dependencies of other packages (since then, removed)?
- ③ Find out relevant security related sites and mailing lists for a Linux distribution of your choice

## System services

## Intro:

- Goal: minimize number of running system services
- Why? To protect against potential threats (not yet reported or discovered)
- Run only services that your system needs, disable all others
- Possible operations:
  - enable/disable
  - configure options in order to tighten security
- Services: mail, file transfer, remote login, web server, network print services etc.

# 1. Linux services, the classic way: System V init scripts (*daemons*)

- created almost 30 years ago at AT&T Bell Labs
- now, replaced by `systemd` service (see next section) in almost all Linux distributions
- Services (daemons) are started/stopped when the Linux system enters or leaves a certain system state (called `runlevel`).

# System V init scripts

Typical runlevels in an older CentOS distribution:

```
$ less /etc/inittab
...
# Default runlevel. The runlevels used are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have netwo
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
...
```

## System V init scripts (cont.)

- On Linux distros without a graphical interface (as above), the default runlevel (after boot) is 3 – Full multiuser mode
- If the Linux OS has a graphical interface (X Window System is installed), the default runlevel is instead 5 – X11 (the OS will boot directly into a graphical login)
- System services are started automatically at boot time by the system initialization process (`init` - “the father of all processes”)
- `init` works by parsing `/etc/inittab` and running scripts found in `/etc/rc.d` folder, according to a default or a desired runlevel.
- Each script can start or stop a service, query its status, reload (re-read) configuration files etc.

## Scripts layout (RedHat based distro)

```
$ cd /etc/rc.d
$ ls
init.d rc rc0.d rc1.d rc2.d rc3.d
rc4.d rc5.d rc6.d rc.local rc.sysinit
```

- `rc.sysinit` is a script run by `init` at system boot, *before* any other scripts (RedHat specific)
- `rc.local` is a customizable script run at system boot, *after* all runlevel specific (or default) scripts are started (RedHat specific)
- scripts for every installed service are placed under `init.d`
- in general, each such script responds to commands given in the following format:

```
<script_name> { start|stop|status|restart|reload }
```

## Example (script ‘skeleton’ / template file): I

```
#!/bin/bash
#
# chkconfig 35 90 12
# description: sample sys V daemon

# source function library
. /etc/rc.d/init.d/functions

# start service:
start() {
    # ... add commands here
}

# restart service:
stop() {
```

## Example (script ‘skeleton’ / template file): ll

```
# ... add commands here
}

# main switch:
case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    status)
        status <program_name>
        ;;
    restart|reload|condrestart)
        stop
        ;;
```

## Example (script ‘skeleton’ / template file): III

```
start
;;
*)
echo "Usage: $0 {start|stop|restart|reload|status}"
exit 1
esac
exit 0
```

# Working with services (daemons)

- How to manually control a service in RedHat-based distributions:

```
$ service network restart
```

- A more generic method:

```
$/etc/rc.d/init.d/network restart
```

- in a Debian-based distro, the `rc.d` folder is missing, so one would run instead:

```
$/etc/init.d/network restart
```

## Working with services (cont.)

**Note:** you should always use the distribution-specific way (there may be side-effects) of controlling a service

- Next: how does `init` know what services to start/stop when entering a specific runlevel?
- This is implemented using *symbolic links* in the folder `rcX.d`, where X = runlevel

## Example: services stopped (K) or started (S) when entering runlevel 3 |

```
$ cd /etc/rc.d
$ ls -l rc3.d
...
K10saslauthd -> ../init.d/saslauthd
K30postfix -> ../init.d/postfix
K50netconsole -> ../init.d/netconsole
K50vsftpd -> ../init.d/vsftpd
K75quota_nld -> ../init.d/quota_nld
K87restorecond -> ../init.d/restorecond
K89rdisc -> ../init.d/rdisc
S02lvm2-monitor -> ../init.d/lvm2-monitor
S08ip6tables -> ../init.d/ip6tables
S08iptables -> ../init.d/iptables
```

Example: services stopped (K) or started (S) when entering runlevel 3 ||

```
S10network -> ../init.d/network
S11auditd -> ../init.d/auditd
S12rsyslog -> ../init.d/rsyslog
S25blk-availability -> ../init.d/blk-availability
S25netfs -> ../init.d/netfs
S26udev-post -> ../init.d/udev-post
S55sshd -> ../init.d/sshd
S90crond -> ../init.d/crond
S99local -> ../rc.local
...
...
```

## Notes:

- each symbolic link points to a specific service script from `init.d`
- the name of each symbolic link starts with either 'S', or 'K'
- thus `init` knows to start or stop the specific service
- therefore, in order to disable a service, one could rename the symbolic link from the desired runlevel folder (`rcX.d`). E.g.:

```
$ cd /etc/rc.d/rc3.d/  
$ sudo mv S25netfs 00NOT-S25netfs
```

## Notes (cont.):

- **BUT**, one should always use the distribution-specific way! In this case, the `chkconfig` command:

```
$ sudo chkconfig netfs off --levels 35
```

- This automatically renames all symbolic links pertaining to the specified service (in this case, links to 'netfs' at runlevels 3 and 5 will start with the letter 'K')
- Note that all changes take effect only at the next reboot (or next time the desired runlevel is reached).
- To act "now", use the `service ... start` or `service ... stop` commands.

## xinetd: the super service

- xinetd (or its older name - inetd) is a service that can start/stop etc. other services as needed (which are thus not controlled directly by init)
- created to launch various network services on request.
- hides network complexity for such programs (which simply use stdin/stdout to receive or send data, and spawn copies of themselves to serve multiple clients at once)
- performance penalties (one process copy per active request)
- historical source of security problems
- if possible, *disable* it
- if not, configure it to filter the list of accepted host IPs

## In short:

- disable every service you don't need
- disable any unsecure/traditional service, if possible, or limit/filter its usage
- use SSH/SFTP/SCP instead of telnet/ftp.
- don't start a mail server, if you intend to send/receive emails and have *another* mail provider (most certainly you do)
- disable network facilities if you intend to use a service locally (e.g. printing)

## 2. Linux services, the new way: `systemd`

**Benefits** over System V init scripts:

- hotplug capable: assumes any resource can appear or disappear at any time.
- better tracking of system state (who owns what, what failed, all logs are captured etc.)
- improved modularity
- reduces number of order dependencies between daemons
- => (at least in theory) faster
- more 'cross-platform' - scripts can be written and distributed upstream.

# systemd: usage I

- ① List running units:

```
$ systemctl list-units
```

- ② List failed units:

```
$ systemctl --failed
```

- ③ Activate a unit immediately:

```
$ sudo systemctl {start|stop|restart|reload|status}  
<unit>
```

- unit: not only services, but also other types of entities: targets, device units, mount units etc. (see `systemd` manual page)

## systemd: usage II

- e.g. a ‘target’ is similar to the old ‘runlevel’.

To start in graphical mode at every boot, run:

```
$ sudo systemctl set-default graphical.target
```

To start in multi-user, text mode, with network enabled instead:

```
$ sudo systemctl set-default multi-user.target
```

To see only running services, filter the listing:

```
$ systemctl -t service
```

- To start a service/target by default at system boot, the unit must be *enabled*:

## systemd: usage III

```
$ sudo systemctl enable <unit>
```

(this takes effect at next computer restart)

- `systemctl` has its own logging system - `journalctl`. E.g., to show all messages for a specific unit:

```
# journalctl -u <unit>
```

# Task:

- write a simple service which sets up the default qdisc policy for an Ethernet network device

# Security in IT Systems: Linux Security (C8)

Gabriel Lazăr

November 28, 2014

## 1 Logging system messages

## 2 Limiting user access

## 3 Application

## Logging system messages

# Importance of good logging

- attacks can occur that leave no visible trace afterwards
- retrieving the logs:
  - manual: administrator task (tedious)
  - automatic: specialized programs (parse and offer summary)
- log to multiple destinations (machines, equipments):
  - attacker can remove evidence from local (compromised) files
  - 2nd copy of logs on secure machine: can find “diffs” -> evidence of attack
  - backup of messages, if local disk crashes

# Linux logging services (daemons)

- ① Classical solution: syslog Sys. V service
- ② Modern replacement: journalctl (with systemd)

## the syslog service

- service name: syslogd
- started at boot
- receives log messages from kernel and any other process
- distributes them to:
  - various files (local, or remote)
  - devices (e.g. printer: /dev/lp0)
  - terminal (messages are displayed almost in real time)

# The syslog service

- File: /etc/syslog.conf
- Terms: 'facility' & 'priority'
  - facility: every log message is tagged with a 'facility' value (system 'aspect' the process is attached to)
  - priority: reflects the severity/importance of each message
- Historical source of security bugs
  - drop-in replacements exists (improved services, enhanced functionality, backwards compatible)
  - example: CentOS 6 Linux system: rsyslog service (configure /etc/rsyslog.conf)

## Configuring the syslog service: facilities

name	description
kern	kernel errors
user	from user processes
mail	from mail server
cron	from cront/at jobs
daemon	other system daemons
auth	authentification warnings
authpriv	Linux specific (private auth. warnings)
local[0-7]	site specific

Table 1: Message facilities

## Configuring the syslog service: priorities

name	description
emerg	system is unusable
alert	take action immediately
crit	critical condition
err	general condition error
warn	system warning
notice	normal but important
info	FYI / information message
debug	debug / developer output

Table 2: Message priorities

# Configuring the syslog service: example

*Legend:*

- ‘.’ - log specified *and higher* priorities
- ‘.=’ - log only specified priority
- ‘-’ (before the log filepath) = don’t sync

sample: /etc/syslog.conf

```
# log kernel messages on console
kern.*                                /dev/console

# log most of messages of level 'info' and higher
*.info;mail.none;authpriv.none;cron.none  /var/log/messages

# auth priv msg go to specialized log
authpriv.*                               /var/log/secure

# mail msg -> special log
mail.*                                    -/var/log/maillog

# cron
cron.*                                   /var/log/cron

# emergency msg are logged everywhere
*.emerg                                  *
```



# Process logging with syslog

C code sample: logging user messages ('log.c')

```
1 #include <syslog.h>      // syslog() functions
2 #include <unistd.h>       // sleep()
3
4 int main(int argc, char* argv[])
5 {
6     int i;
7     openlog(argv[0], LOG_PERROR | LOG_PID, LOG_USER);
8     for (i = 0; i < 10; ++i)
9     {
10         syslog(LOG_DEBUG, "i = %d", i);
11         sleep(1);
12     }
13     closelog();
14     return 0;
15 }
```

## Process logging with syslog (cont.)

- since log priority is 'debug', the message won't be logged to any file
- to log debug messages, the syslog configuration file must be updated
- restart syslogd service after /etc/syslog is modified
- e.g. (for CentOS 'rsyslog' service):

create 'etc/rsyslog.d/user.conf' with the following content:

`user.debug -/var/log/user.log`

restart (r)syslog service:

```
# service rsyslog restart
```

## Process logging with syslog (cont.)

- build and run the above C code sample:

```
$ gcc log.c -o log  
$ ./log
```

- follow logged messages in real time on screen:

```
# tail -f /var/log/user.log
```

# Logging issues and solutions

- logs can grow until the file system fills up
- ill-behaved users can take advantage and flood system with log messages
- => it's important to 'rotate' log files on a regular basis:
  - move the old log file aside
  - start a new one
  - compress, move to external storage and/or discard oldest logs
- in Unix/Linux world, rotation is accomplished using two services:
  - ① logrotate - to rotate logs
  - ② cron - to schedule rotation actions through logrotate

# Log rotation with 'cron' & 'logrotate'

- see `man cron`, `man crontab` and `man logrotate`

cron: scheduling action: `/etc/cron.daily/logrotate`

```
#!/bin/sh

/usr/sbin/logrotate /etc/logrotate.conf >/dev/null 2>&1
EXITVALUE=$?
if [ $EXITVALUE != 0 ]; then
    /usr/bin/logger -t logrotate "ALERT exited abnormally with [$EXITVALUE]"
fi
exit 0
```

logrotate: configuration files

<code>/etc/logrotate.conf</code>	<i># main config (read the comments)</i>
<code>/etc/logrotate.d/&lt;name&gt;.conf</code>	<i># specific configs</i>

## 'logrotate' example

- Few keywords: rotate, daily, size, compresss, missingok, postrotate - cmd - endscript
- **Task:** create a log rotation config file for the above /var/log/user.log example

/etc/logrotate.d/fail2ban

```
...
/var/log/fail2ban.log {
rotate 7
missingok
compress
postrotate
    /usr/bin/fail2ban-client flushlogs 1>/dev/null || true
endscript
}
```

## History of logged-in users

- Files logging previous user access: ‘wtmp’, ‘btmp’

View previous logged in users:

```
# last  
# last -f /var/log/wtmp.0
```

View previous failed login attempts:

```
# lastb  
# lastb -f /var/log/btmp.0
```

## Limiting user access

# Controlling user access to a Unix/Linux system

- overview of the Unix/Linux account and password system
- interaction between user rights and file system attributes
- limit user access to system resources

# Users & passwords in Linux

- each user has an assigned username and password
- both are case-sensitive
- each username has a unique associated ID ( = user ID, 'UID')
- the operating system uses the UID internally, not the username
- users can also belong to one or more 'groups'
- information stored in:
  - /etc/passwd
  - /etc/shadow (encrypted password - 'hash')
  - /etc/group

# The superuser ('root')

- the administrator account in Unix/Linux: 'root'
- user ID for root: 0
- **any** account with UID 0 has superuser privileges
- attackers often try to create new UID 0 accounts to get root access to the system

## Becoming superuser

- ➊ login as 'root' (bad!)
- ➋ login as regular user and use the 'su' command
- ➌ limit access with sudo (fine-grained control) (see /etc/sudoers)
  - 'sudo' prompts users for *their* passwords (easier when administrators leave the company)
  - 'sudo' allows fine-grained access control - the admin may specify a list of specific commands that a given user may execute with superuser privileges.
  - better logging



## '/etc/password'

- public information: username, user ID, user main group, user's full name, path to home folder and default command shell

example:

```
...
tcpdump:x:72:72:::/sbin/nologin
domotica:x:1914:1914:/home/domotica:/bin/bash
...
```

## '/etc/shadow'

- private information! (file should be readable only for superuser)
- fields: username, encrypted password + various pieces of administrative information
- administrators use this file and a number of user accounting commands to configure:
  - password expiration and 'aging',
  - password history,
  - minimum password lengths,
  - force wide variety of character types,
  - check passwords against dictionary etc.
- to block a user, set an invalid encrypted password for that user, or/and:
- set a special command shell in '/etc/passwd':
  - `/sbin/nologin` (modern)
  - `/bin/false` (classic)

# Superuser commands for account management

- `useradd`, `adduser` (add, modify users - see the manual pages)
- `usermod` (modify user settings - e.g. add user to another group)
- `userdel`
- `passwd` (change password, lock/unlock user, set password related actions)

*Task:* Read the manual pages for all the above commands. Create a user, register him to an additional group and set a password expiration date.

## File permissions and ownership

- easiest way to see file attributes:

```
# cd /etc
# ls -l
...
drwxr-xr-x.  5 root root    4096 Nov 12 17:54 yum
-rw-r--r--.  1 root root     969 Oct 16 18:15 yum.conf
drwxr-xr-x.  2 root root    4096 Oct 16 18:15 yum.repos.d
```

file owner	group owner	everyone else
r w x	r - x	r - x

Table 3: file permissions

## File attributes and ownership

There are 3 sets of file 'rights': for the file owner (1st set), for people in the group that owns the file (2nd column) and for all others (3rd set)

- 'r': file is readable / directory contents can be listed
- 'w': file can be modified / files can be created/deleted in this directory
- 'x': file is executable / directory path can be 'traversed' to access a file
- To change file rights: 'chmod' command (see manual page)
- To change ownership: 'chown' command (see manual page)

## Other (special) rights:

- 'set-UID', 'set-GID': causes the file to be executed as the owner (or group owner) of the executable, instead of the user who runs it => different (usually elevated) privileges
- the 'sticky' bit: when set on a directory, only the owner of a given file may remove that file from the directory. (e.g. on /tmp)

---

file owner	group owner	everyone else
r w s	r - s	r - t

---

Table 4: special file permissions: setuid, setgid, sticky

# File attributes and system security

- avoid world-writable directories
- if world-writable directories must exist, set 'sticky' bit
- avoid setuid-ed programs! (make a list)

**Task:** use the 'find' command to create a list of: - all world-writable directories - all SUID/SGID files

## File system security

- The Linux logical file system is mapped on the physical file system
- Disk partitions are *mounted* at various points in the (logical) file system
- Each mount point can be created with different security options

```
[root@lab211a ~]# df
Filesystem      1K-blocks  Used   Available Use% Mounted on
/dev/sda2        32944956  1745564  29519216  6%   /
/dev/sda1        487652    106260   355792   23%  /boot
/dev/sda3        34137840  125568  32271472  1%   /home
```

to configure automatically mounted devices, edit:

/etc/fstab

## File system security (cont.)

- Mounting security options:
  - ‘ro’: file system is mounted read-only (nothing can be modified on this partition - e.g. good for preserving untouched system binaries)
  - ‘nosuid’: SUID/SGID program permission bits are ignored
  - ‘nodev’: Unix/Linux device files won’t work (only regular files/directories)
  - ‘noexec’: no binaries
- In a perfect world, all file-systems should be either mounted read-only, or ‘nosuid’

## File system security (cont.)

mount point	description	security
/	root partition	separate partition
/home	users partition	noexec,nodev,nosuid
/bin	system binaries	ro,nosuid
/lib	system libs	ro,nosuid
/var	fragmented (logs)	nosuid

Table 4: logical filesystem example with mounting options

# Application

# Practical tasks

- ① Limiting disk usage for system users with ‘quota’
- ② Blocking brute-force SSH attacks with dynamic firewall rules  
(‘fail2ban’)

# **SECURITATEA IN SISTEMELE IT**

---

## **INTRODUCTION TO INFORMATION SECURITY**

Cristian Serban  
Lucian Suta



## Agenda

- Common online threats
- How the web works
- Web vulnerabilities today
- Application Security tools
- SDLC program

## Samy [2005]

- An XSS worm that was designed to propagate across the MySpace social-networking site
  - It displayed the string "but most of all, samy is my hero" on a victim's MySpace profile page
  - When a user viewed that profile page, the payload would be planted on their own profile page
- Within just 20 hours from release, over one million users had run the payload
- myspace.com site became unavailable
- Samy Kamkar was sentenced to three years probation with only one computer, no Internet, 90 days community service, and 15-20.000 USD of restitution.

**myspace.com**  
a place for friends

Privacy | Help | SignUp

MySpace Search powered by Google

Home | Browse | Search | Invite | Film | Mail | Blogs | Favorites | Forum | Groups | Events | MySpace TV | Music | Comedy | Classifieds

Cool New Videos      75,195 uploaded today!

 Elephant Playing Darts  
Catch Of The Day

 Shaolin Monk Demonstration CT

 Ripe TV: Max Tour Stories  
Ripe TV

 Triple Backflip Off The Wall  
JonJonTV

Books      Forum      Mobile      Profile Editor  
 Blogs      Grade My Prof.      Movies      Ringtones NEW!  
 ChatRooms      Horoscopes      Music      Schools  
 Comedy      Impact NEW!      Music Videos      Sports  
 Downloads      Jobs      MySpaceIM      MySpace TV  
 Filmmakers      Latino      News NEW!      Weather

**myspaceim** >> download

**Member Login**

E-Mail:   
 Password:   
 Remember Me  
   
[Forgot your password?](#)  
[Login Trouble?](#)

**Find Your Friends on MySpace**

Check your [Gmail](#), [Yahoo!](#) and [AOL](#) contacts and find them on MySpace!

**Cool New People**

andy      Sheena      JASON

**MySpace Music**      [more music]

 **Mike Jones**  
Hip Hop / Rap  
Houston, TX

**EXCLUSIVE**

The Houston rapper returns with his strongest CLUB BANGER to date, "DROP & GIMME SO," featuring Hurricane Chris. The associated "booty shakin'" dance will surely be DROPPING at a club near you! Listen here first, exclusively on MySpace.

> Download Now

**MySpace Specials**

**Videos**      [more videos]

 **Forza Initial D Crossover**  
Takumi "Tak" Fujiwara's AE86 Trueno and Nakazato "Zack" Takehi's Skyline R32 on Ferza.  
 > Watch It Now!

http://mail.myspace.com/index.cfm?fuseaction=mail.friendRequests&Mytoken=[REDACTED]

The screenshot shows a MySpace inbox page with several annotations:

- KICK ASS**: Red arrow pointing to the "Mail Center" link.
- classemates.com**: Red arrow pointing to the "I graduated in:" section.
- I RULE**: Red arrow pointing to the "Friend Request Manager" link.
- PLEASE DONT PRESS CHARGES**: Red arrow pointing to the message content.
- MAD PHOTOSHOP SKILLS**: Red arrow pointing to the profile picture of the requester.
- SHE WANTS ME**: Red arrow pointing to the message content.

**Inbox**

- Saved**
- Trash**
- Bulletin**
- Friend Requests**
- Pending Requests**
- Event Invites**

**Fly Fishing Trip in Mexico**  
All inclusive package in Ascension Bay, Mexico, from US\$1,600... [www.pescamaya.com](http://www.pescamaya.com)

**Listing 1-10 of 919664**

	Date:	From:	Confirmation:
<input type="checkbox"/>	Oct 4, 2005 10:22 PM	 Online Now!	<b>PLEASE DONT PRESS CHARGES</b> Lulu the Loveable Freak wants to be your friend! <b>Approve</b> <b>Deny</b> <b>Send Message</b>
<input type="checkbox"/>	Oct 4, 2005 10:21 PM		AlysOnIt wants to be your friend! <b>Approve</b> <b>Deny</b> <b>Send Message</b>

## Project Chanology [2008]

- Anonymous is an international network of activists and hacktivists active since 2004
- In 2008, they used a tool called LOIC to launch a Distributed Denial-of-Service (DDOS) attack against the Church of Scientology
- Several people were arrested and convicted because they failed to conceal their IP addresses

PCWorld  
FROM IDG

AdChoices DDoS Scientology

Scientology Hack

### NEWS

#### Hackers Hit Scientology With Online Attack



By Robert McMillan

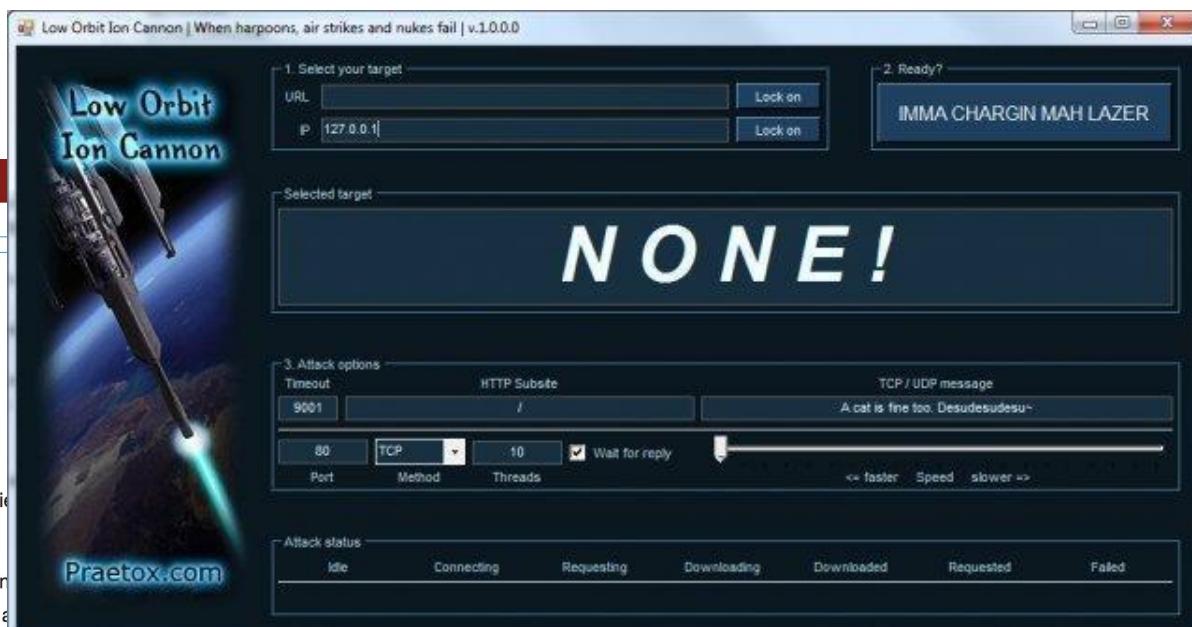
IDG News Service | JAN 26, 2008 12:26 PM PT

A group of hackers calling itself "Anonymous" has hit the Church of Scientology's website with an online attack.

The attack was launched January 19 by Anonymous, which is seeking religious freedom and to help "save people from Scientology by reversing the brainwashing," a statement on its [Web page](#) maintained by Anonymous.

Anonymous claims to have knocked the Church's Web site offline with a distributed denial-of-service attack, in which many computers bombard the victim's server with requests, overwhelming it with data in the hope of ultimately knocking the system offline. True to its name, Anonymous does not disclose the true identities of its members.

[ Further reading: [How to remove malware from your Windows PC](#) ]



## Royal Navy Website [2010]

- The site was temporarily unavailable
- A Romanian hacker TinKode reportedly exploited a SQL injection vulnerability and stole usernames and passwords of the site's administrators.
- For a while, the site displayed the message: "Unfortunately the Royal Navy website is currently undergoing essential maintenance. Please visit again soon."

The BBC News Technology header features the BBC logo, a sign-in link, and navigation links for News, Sport, Weather, iPlayer, TV, and Radio. Below the header is a large red banner with the words "NEWS TECHNOLOGY". Underneath the banner is a horizontal menu bar with links for Home, World, UK, England, N. Ireland, Scotland, Wales, Business, Politics, Health, Education, and Sci/E.

8 November 2010 Last updated at 13:04



## Royal Navy website attacked by Romanian hacker

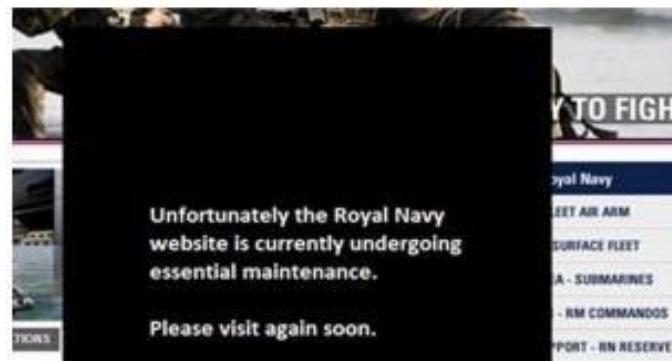
The Royal Navy's website has been hacked by a suspected Romanian hacker known as TinKode.

The hacker gained access to the website on 5 November using a common attack method known as SQL injection.

TinKode published details of the information he recovered, which included user names and passwords of the site's administrators.

A Royal Navy spokesperson confirmed the site had been compromised and said: "There has been no malicious damage."

They added that as a precaution the site has been "temporarily suspended" and that security teams were investigating how the hacker got access. They said no confidential information had been disclosed.



The Royal Navy website has been suspended while security teams investigate

### Related Stories

[Europe simulates total cyber war](#)  
[UK facing cyber](#)

## 50 Days of Lulz [2011]

- Lulzsec was a hacker group that was formed in May 2011 and was active until June
- During that time they hacked many websites including
  - Fox TV (leaking contact information for 73,000 contestants),
  - PBS, Sony Pictures,
  - a porn site (leaking e-mail addresses and passwords including three US military ones)
  - InfraGard (an organization associated with the FBI), US Senate, CIA
- The group relied on straight-forward techniques: remote file includes, SQL injection and XSS



## Adobe Breach [2013]

- Hackers steal details on 153 million customers and source code for Adobe Photoshop, Adobe Acrobat, Reader, ColdFusion
  - Passwords were encrypted with the same key
  - Encryption algorithm used ECB mode
- “we believe that the third party likely removed from our systems certain customer names, payment card expiration dates, encrypted payment card numbers, and other information relating to customer orders. In addition, the third party used our systems to decrypt some card numbers. We have not been able to confirm that any decrypted card numbers were removed as a result of this access to our systems.”

# Did your Adobe password leak? Now you and 150m others can check

Leak is 20 times worse than the company initially revealed, and could put huge numbers of peoples' online lives at risk



Adobe's HQ. The company leaked over 100m users' details. Photograph: PAUL SAKUMA/ASSOCIATED PRESS

Nearly 150 million people have been affected by a loss of customer data by Adobe, over 20 times more than the company admitted [in its initial statement last week](#).

Owing to the proliferation of Adobe products in use throughout the world, from the Flash browser plugin, to the Acrobat software used to create PDFs, to the AIR framework used to make software like Tweetdeck and the BBC iPlayer desktop application, many users have [Adobe](#) accounts which they have since forgotten about (including 50% of the Guardian technology desk).

## Equifax Breach [2017]

- Equifax is one of the three main credit reporting agencies in the US
- In September 2017 it announced that it lost **highly sensitive** personal and financial information for 143 million people
  - Social security numbers, birthdates, addresses
  - Credit card numbers
  - Documentation related to disputes
- The attack started in May and was only detected on July 29th
- In October, hackers manipulated the site to deliver fake Adobe Flash updates which infected computers with adware



The image shows the Equifax website's landing page for a cybersecurity incident. The background is dark red with white text and icons related to cybersecurity and consumer protection. At the top left is the Equifax logo. Top right links include "English | Español" and "Return to equifax.com ▾". The main title "Cybersecurity Incident & Important Consumer Information" is centered in large white font. Below it is an orange button labeled "Enroll Now". A subtext below the button reads "to Protect & Monitor Credit — FREE for everyone in the U.S." The background features faint icons of mobile phones, servers, checklists, and a computer monitor with a padlock.

[Home](#)    [Consumer Notice](#)    [Lock or Freeze](#)    [Announcements](#)    [FAQs](#)    [Contact](#)

Need help? [Contact Us](#)

## Am I Impacted?

If you have a U.S. Social Security number, you can see if your personal information has been impacted.

1. Click the “Am I Impacted?” button below
2. Provide your last name and the last six digits of your Social Security number and submit.

Anyone with a U.S. Social Security number can enroll in TrustedID Premier, even if your personal information was not impacted, for FREE through Wednesday, January 31, 2018.

Note: Because we do not store this information during this step, you may have to enter this information multiple times to validate your identity throughout the TrustedID Premier enrollment process.

[Am I Impacted?](#)

*On October 2, 2017, Equifax announced that additional consumers may have been impacted. To minimize confusion, Equifax will mail written notices to all of the additional potentially impacted U.S. consumers identified since the Sept. 7 announcement. The feature “Am I Impacted?” has been updated to reflect the additional impacted U.S. consumers.*

The screenshot shows a web browser displaying the homepage of the Universitatea Tehnică din Cluj-Napoca (University of Technology of Cluj-Napoca). The URL in the address bar is [www.utcluj.ro](http://www.utcluj.ro). The page features a dark header with the university's logo, name, and language links (ENGLISH, TELEFOANE, CONTACT, INTRANET). A search bar is also present in the header. Below the header, there is a large banner image showing three different views of a classical building with a red dome and a flag flying from its roof. The banner has four sections: 'UNIVERSITATEA' (with a logo), 'VREAU SA DEVIN STUDENT', and 'SUNT STUDENT'.

Burp Suite Professional v1.6.05 - licensed to Betfair [10 user license]

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding image content

#	Host	Method	URL	Params	Edited	Status	Length	MI
50	http://www.utcluj.ro	GET	/	<input type="checkbox"/>	<input type="checkbox"/>	200	30561	HT
52	http://www.utcluj.ro	GET	/static/skeleton.css	<input type="checkbox"/>	<input type="checkbox"/>	200	10158	CSS
53	http://www.utcluj.ro	GET	/static/Layout.css	<input type="checkbox"/>	<input type="checkbox"/>	200	2092	CSS
54	http://www.utcluj.ro	GET	/static/Styles.css	<input type="checkbox"/>	<input type="checkbox"/>	200	7142	CSS
55	http://www.utcluj.ro	GET	/static/skeleton_layout.css	<input type="checkbox"/>	<input type="checkbox"/>	200	2058	sc
56	http://www.utcluj.ro	GET	/static/base.css	<input type="checkbox"/>	<input type="checkbox"/>	200	9581	CSS
58	http://fonts.googleapis.com	GET	/css?family=Source+Sans+Pro:70...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	1729	CSS
59	http://www.utcluj.ro	GET	/static/js/jquery.flexslider.js	<input type="checkbox"/>	<input type="checkbox"/>	200	40817	sc

Request Response

Raw Headers Hex

```
GET / HTTP/1.1
Host: www.utcluj.ro
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCYQFjAA&url=http%3A%2F%2Fwww.utcluj.ro%2F&ei=2BJrVLzdBoHmywPa7ICQBw&usg=AFQjCNHfmfzlrpIwkEOYMJb3XTxWgmB_dQ&bvm=bv.79908130,d.bGQ
Connection: keep-alive
```

? < + > Type a search term 0 matches

Burp Suite Professional v1.6.05 - licensed to Betfair [10 user license]

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding image content

#	Host	Method	URL	Params	Edited	Status	Length	MI
50	http://www.utcluj.ro	GET	/			200	30561	HT
52	http://www.utcluj.ro	GET	/static/skeleton.css			200	10158	CS
53	http://www.utcluj.ro	GET	/static/Layout.css			200	2092	CS

Request Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK  
Date: Tue, 18 Nov 2014 09:35:18 GMT  
Server: Apache/2.2.22 (Ubuntu)  
Vary: Accept-Encoding  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=utf-8  
X-Pad: avoid browser bug  
Content-Length: 30305

<!DOCTYPE html>  
<!--if lt IE 7 --><html class="ie ie6" lang="ro"> </if>-->  
<!--if IE 7 --><html class="ie ie7" lang="ro"> </if>-->  
<!--if IE 8 --><html class="ie ie8" lang="ro"> </if>-->  
<!--if (gte IE 9) /!(IE)--><!--><html lang="ro"> <!-->

<head>  
 <meta charset="utf-8">  
 <title>Universitatea Tehnica din Cluj-Napoca</title>  
 <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">  
 <meta name="author" content="Tudor Trd, trd002200@gmail.com" />  
 <link href='http://fonts.googleapis.com/css?family=Source+Sans+Pro:700,200,600,400,300' rel='stylesheet' type='text/css'>  
 <link rel="stylesheet" href="/static/base.css">  
 <link rel="stylesheet" href="/static/skeleton.css">  
 <link rel="stylesheet" href="/static/skeleton\_layout.css">  
 <link rel="stylesheet" href="/static/Layout.css">  
 <link rel="stylesheet" href="/static/Styles.css">  
 <link rel="stylesheet" href="/static/Elements.css">  
 <!--if lt IE 9--><script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script><!--endif-->

?

<

+

>

Type a search term

0 matches

Response:

`Set-Cookie: value[; expires=date][; domain=domain][; path=path][; secure][; httponly]`

Request:

`Cookie: value`

Javascript:

`document.cookie="name=Nicholas; domain=nczonline.net; path=/";`



- |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|
| ① | ② | ③ | ④ | ⑤ | ⑥ | ⑦ | ⑧ |
|---|---|---|---|---|---|---|---|

scheme://	login.password@	address:	port	/path/to/resource	?query_string	#fragment	
-----------	-----------------	----------	------	-------------------	---------------	-----------	--

- ① Scheme/protocol name
  - ② Indicator of a hierarchical URL (constant)
  - ③ Credentials to access the resource (optional)
  - ④ Server to retrieve the data from
  - ⑤ Port number to connect to (optional)
  - ⑥ Hierarchical Unix path to a resource
  - ⑦ “Query string” parameters (optional)
  - ⑧ “Fragment identifier” (optional)
- ] “Authority”

The screenshot shows a web browser window with the URL <https://www.paypal.com/ro>. The browser's toolbar includes icons for back, forward, search, and various settings. A context menu is open on the right side of the screen.

The main content area displays the PayPal homepage for a user named "Cristian Serban". The navigation bar includes "My Account", "Send Payment", "Request Money", and "Merchant Ser...". Below the navigation bar are links for "Overview", "Top Up Account (Instantly)", "Withdraw", "History", and "Resoluti...".

A "Certificate" dialog box is overlaid on the page. The dialog has tabs for "General", "Details", and "Certification Path", with "General" selected. The "Certificate Information" section contains the following text:

**This certificate is intended for the following purpose(s):**

- Ensures the identity of a remote computer

\* Refer to the certification authority's statement for details.

**Issued to:** 2028.globalsign.com

**Issued by:** GlobalSign Organization Validation CA

**Valid from** 15/07/2009 **to** 15/07/2012

Buttons at the bottom of the dialog include "Issuer Statement", "Learn more about certificates", and "OK".

# OWASP Top 10 Application Security Risks

**2013**

1. Injection
2. Broken Authentication and **Session Management**
3. Cross-Site Scripting (XSS)
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. **Cross-Site Request Forgery (CSRF)**
9. Using Components with Known Vulnerabilities
10. **Unvalidated Redirects and Forwards**

**2017**

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. **XML External Entities (XXE)**
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. **Insecure Deserialization**
9. Using Components with Known Vulnerabilities
10. **Insufficient Logging and Monitoring**

## WebGoat

- A deliberately insecure web application
- Allows people to test common vulnerabilities found in Java-based applications
- We have an instance running at
  - <http://18.194.142.217/WebGoat>

# Injection

Injection vulnerabilities are caused by code that allows *user-supplied input* (coming from a possible attacker) to be *passed into an interpreter* (on the server side) *without verification*.

## Examples

- SQL injection
- OS command injection
- LDAP injection
- Spring Evaluation Language (SPEL) injection

## How to prevent

- Parameter validation (whitelisting, blacklisting)
- Parameter encoding (maybe not recommended, should be tied to interpreter)
- Parameter sanitization (remove invalid characters from input)
- Parameterized queries (for databases)

# Broken Authentication and Session Management

Broken authentication vulnerabilities are caused by flaws in code that implements login mechanisms, user accounts creation, logout mechanisms, account management (including password management and account recovery), etc. Session management vulnerabilities are caused by flaws in code which implement management of user sessions (including session timeout and invalidation).

## How to prevent

- Do not allow account enumeration
- Use hashes + salt for storing passwords
- Implement two-factor authentication (2FA)
- Use good random number generators for session ids
- Do not reuse session ids, invalidate session id upon logout (both cookies and database records)
- Session ids should be changed upon login (to prevent session fixation)
- Do not expose session ids in the URL

# Sensitive Data Exposure

This vulnerability has to do with a lack of protection of sensitive data.

Sensitive data can include

- Credit card information: number, name, expiration date, CVV
- Personal identifiable information (PII): customer name, address, telephone number, e-mail address, SSN or CNP
- Financial information
- Health information
- Identifiers: customer account name (used for logging in)
- Password

How to prevent

- Use strong hashing and encryption algorithms (both at rest and in transit)
- Store as little sensitive data as possible
- Do not put sensitive data in URLs (where they can be seen and logged)
- Disable autocomplete on pages that collect sensitive data
- Disable caching of pages that contain sensitive data
- Use external services (for authentication or credit card processing, for instance)

## Broken Access Control

This vulnerability has to do with a lack of protection of certain application functionality (on the server) which can result in a lack of protection of certain pages on the web application.

How to prevent

- Protect each instance of critical functionality.
- Use indirect object references (unique per user or per user session)
-

# Security Misconfiguration

Security misconfiguration vulnerabilities are vulnerabilities that are generated by a lack of proper configuration at any level in the software stack: operating system, web server, application server, libraries, frameworks, application.

How to prevent

- Configure firewall
- Disable applications that are not needed
- Change default passwords
- Etc.

# Cross Site Scripting (XSS)

Cross Site Scripting vulnerabilities are caused by code that *redirects user-supplied input* (coming from a possible attacker) *back to the browser without verification*. This code can be in both the server or the browser. XSS can be either *reflected* or *stored*.

## How to prevent

- Output encoding (should be contextual)
- Parameter validation (whitelisting, blacklisting)
- Parameter sanitization (remove invalid characters from input)

## Using Components with Known Vulnerabilities

Software is rarely built 100% from scratch. This vulnerability has to do with using third-party components (libraries, frameworks, services) that are known to have vulnerabilities. Components can include other components that can have their own vulnerabilities.

### How to prevent

- Make sure you have a list of all components that you are using (directly or indirectly, together with versions). Regularly verify whether there are known vulnerabilities to the particular components (and versions) you are using.
- Update component versions regularly.

## Cross Site Request Forgery (CSRF)

This vulnerability occurs when a website under attacker control forces the browser to make requests to a second website where the user has an account. The requests can be issued using images or Javascript. The attacker relies on the fact that the browser will automatically send cookies (including session-related ones) to the second site. Also, the user must have a currently valid session on the second website in order for an attack to succeed.

### How to prevent

- Protect sensitive actions by requiring a password or some other information.
- Include a hidden unique token in a form in the page. This token can be checked when the form is submitted. An attacker will not be able to embed such a token in the request that the browser automatically makes to your website.

## Unvalidated Redirects and Forwards

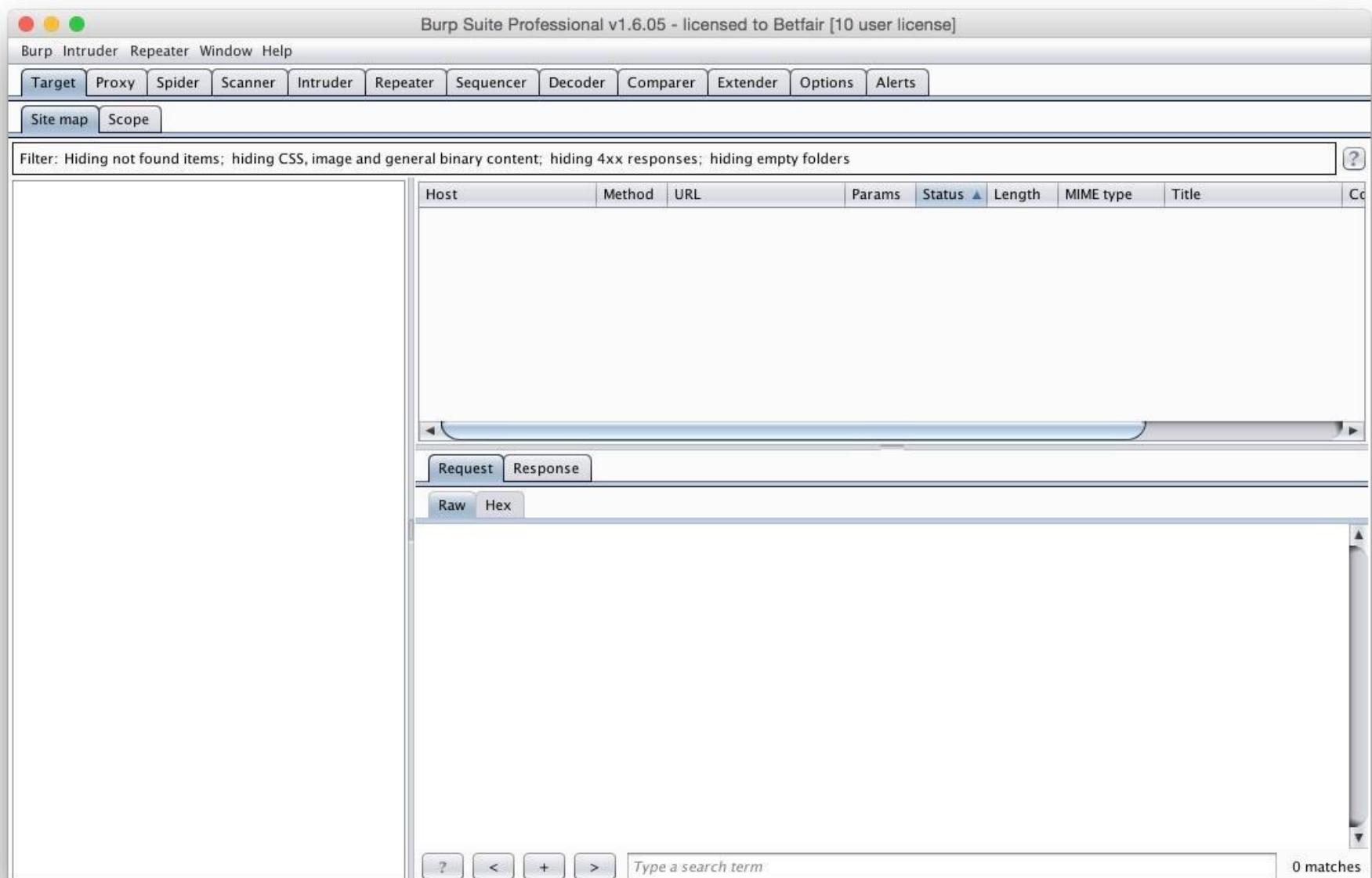
This vulnerability is caused by pages that redirect or forward users (using HTTP mechanisms) to other pages (whose location is determined by parameters that are not validated).

### How to prevent

- Avoid redirects and forwards.
- Avoid using parameters when determining where to redirect or forward to.
- Use indirection (have a whitelist of possible values that map to individual URLs).
- Validate URL parameters. For instance, you can make sure that the hostname in the URL is allowed.

## Burp

- An intercepting Proxy, which lets you inspect and modify traffic between your browser and the target web application.
- An application-aware Spider, for crawling content and functionality.
- An advanced web application Scanner, for automating the detection of numerous types of vulnerability.
- An Intruder tool, for performing powerful customized attacks to find and exploit unusual vulnerabilities.
- A Repeater tool, for manipulating and resending individual requests.
- A Sequencer tool, for testing the randomness of session tokens.



Acunetix Web Vulnerability Scanner (Consultant Edition)

File Actions Tools Configuration Help

New Scan Report Start URL: http://testhtml5.vulnweb.com:80/ Profile: Default Stop Pause

Tools Explorer

- Web Vulnerability Scanner
  - Web Scanner
- Tools
  - Site Crawler
  - Target Finder
  - Subdomain Scanner
  - Blind SQL Injector
  - HTTP Editor
  - HTTP Sniffer
  - HTTP Fuzzer
  - Authentication Tester
  - Compare Results
- Web Services
  - Web Services Scanner
  - Web Services Editor
- Configuration
  - Application Settings
  - Scan Settings
  - Scanning Profiles
- General
  - Program Updates
  - Version Information
  - Licensing
  - Support Center
  - Purchase
  - User Manual
  - AcuSensor

Scan Results

Scan Thread 1 (http://testhtml5.vulnweb.com:80/) Scanning

Alerts summary 28 alerts

acunetix threat level Level 3: High

Acunetix Threat Level 3  
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Total alerts found 28

High	18
Medium	3
Low	6
Informational	1

Target information http://testhtml5.vulnweb.com:80/

Statistics 17152 requests

Progress 65.10%

Activity Window

```
11.25 12:01:31, [high] Cross site scripting (verified) "/comment" on parameter "id"
11.25 12:01:32, [high] Cross site scripting (verified) "/report" on parameter "id"
11.25 12:01:32, [high] Cross site scripting (verified) "/" on parameter "username"
11.25 12:01:41, Open port 8443 - https-alt
11.25 12:01:52, Port scanning completed!
```

Application Log Error Log

Web Scanner Scanning 1 website(s) ... Number of websites left to scan : 1

## Automated Web Vulnerability Scanners

### **Acunetix Web Vulnerability Scanner - commercial**

- SQL Injection & Blind SQL Injection
- Cross-site Scripting (XSS)
- OWASP Top 10 and other vulnerabilities
- Automatic JavaScript analyzer for security testing of AJAX and Web 2.0 applications
- Login Sequence Recorder
- Scanning Scheduler
- Acunetix AcuSensor Technology



### ZAP'S FEATURES

- Open source
- Cross platform
- Easy to install
- Completely free
- Ease of use a priority
- Comprehensive help pages
- Fully internationalized
- Translated into a dozen languages
- Community based, with involvement actively encouraged
- Under active development by an international team of volunteers

### ZAP'S FUNCTIONALITY

- Intercepting proxy
- Traditional and AJAX spiders
- Active scanner
- Passive scanner
- Forced Browsing
- Fuzzer
- Dynamic SSL certificates
- Smart card support
- Web sockets support
- Authentication and session support
- Powerful REST based API
- Support for a wide range of scripting languages
- Automatic updating option
- Integrated and growing marketplace of add-ons



**OWASP**  
THE OPEN WEB APPLICATION SECURITY PROJECT

## Fortify

- A static code analysis tool
- Reduce business risk by identifying vulnerabilities that pose the biggest threat
- Identify and remove exploitable vulnerabilities quickly with a repeatable process
- Reduce development cost by identifying vulnerabilities early in the SDLC
- Educate developers in secure coding practices while they work
- Bring development and security teams together to find and fix security issues

\*wallet-aggregation-service - common/src/main/java/com/betfair/site/services/wallet/application/clients/CachingWalletClient.java - Audit Workbench

**AUDIT WORKBENCH** **FORTIFY**

**Summary | Audit Guide | Scan | Reports**

**Filter Set:** Quick View **My Issues**

**High (38)**

**Group By:** Category

**overrides.properties**

```

9 cougar.log.dir=target/logs
10
11
12 ws.gamexapi.query.url=http://localhost:9030/rest/v1/account/snapshot
13 ws.gamexapi.transfer.url=http://localhost:9030/rest/api/walletTransfer
14
15 ws.au.exchangeapi.url=http://localhost:9030/auexchange/
16 ws.uk.exchangeapi.url=http://localhost:9030/ukexchange/
17 ws.games.gateway.url=http://localhost:9030/gamesgateway/
18 funds.service.url=http://localhost:9030/fundsservice/
19
20 gamesgateway.keystore=file:/etc/bf-wallet-service/certs/wallet-service-client.jks
21 gamesgateway.keystore.password=changeit
22 gamesgateway.keystore.type=jks
23
24 Funds service keystore file is not the keystore that Enrich keystore file

```

**Summary | Details | Recommendations | History | Diagram | Screenshots | Filters**

**Recommendations:**

A password should never be stored in plaintext. Instead, the password should be entered by an administrator when the system starts. If that approach is impractical, a less secure but often adequate solution is to obfuscate the password and scatter the de-obfuscation material around the system so that an attacker has to obtain and correctly combine multiple system resources to decipher the password.

Some third party products claim the ability to manage passwords in a more secure way. For example, WebSphere Application Server 4.x uses a simple XOR encryption algorithm for obfuscating values, but be skeptical about such facilities. WebSphere and other application servers offer outdated and relatively weak encryption mechanisms that are insufficient for security-sensitive environments. For a secure solution the only viable option is a proprietary one.

**Tips:**

1. HP Fortify Static Code Analyzer searches configuration files for common names used for password properties. Audit these issues by verifying that the flagged entry is used as a password and that the password entry contains plaintext.
2. If the entry in the configuration file is a default password, require that it be changed in addition to requiring that it be obfuscated in the configuration file.

**Advanced...**

# APPSEC PROGRAM - BY BSIMM

The Software Security Framework (SSF)			
Governance	Intelligence	SSDL Touchpoints	Deployment
Strategy and Metrics	Attack Models	Architecture Analysis	Penetration Testing
Compliance and Policy	Security Features and Design	Code Review	Software Environment
Training	Standards and Requirements	Security Testing	Configuration Management and Vulnerability Management

# ALIGNMENT TO BUSINESS GOALS

Domain	Practice	Business Goals
Governance	Strategy and Metrics	Transparency of expectations, Accountability for results
	Compliance and Policy	Prescriptive guidance for all stakeholders, Auditability
	Training	Knowledgeable workforce, Error correction
Intelligence	Attack Models	Customized knowledge
	Security Features and Design	Reusable designs, Prescriptive guidance for all stakeholders
	Standards and Requirements	Prescriptive guidance for all stakeholders
SSDL Touchpoints	Architecture Analysis	Quality control
	Code Review	Quality control
	Security Testing	Quality control
Deployment	Penetration Testing	Quality control
	Software Environment	Change management
	Configuration Management and Vulnerability Management	Change management

## SECURITY TESTING - ACTIVITIES

***ST Level 1:*** Enhance QA beyond functional perspective.

- Ensure QA supports edge/boundary value condition testing.
- Drive tests with security requirements and security features

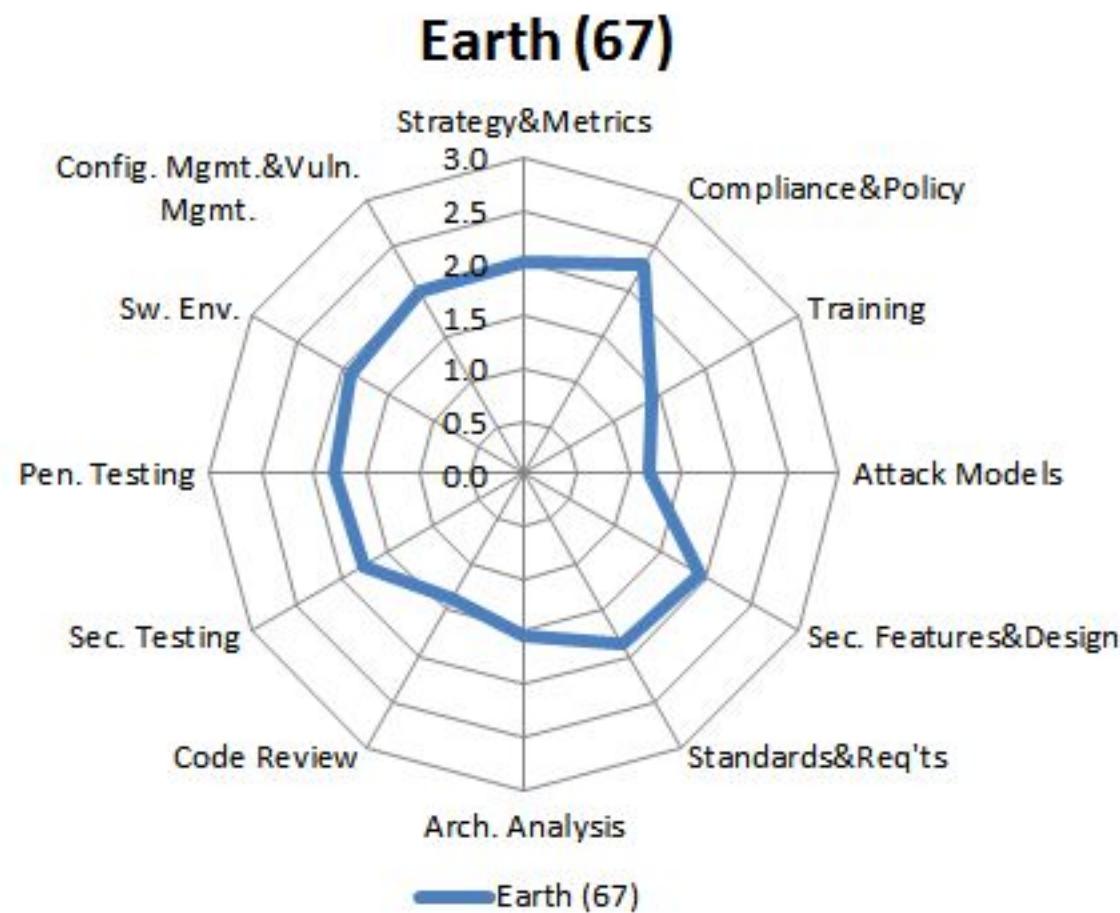
***ST Level 2:*** Integrate the attacker perspective into test plans.

- Integrate black box security tools into the QA process.
- Share security results with QA.

***ST Level 3:*** Deliver risk-based security testing.

- Include security tests in QA automation.
- Perform fuzz testing customized to application APIs.
- Drive tests with risk analysis results.
- Leverage coverage analysis.
- Begin to build and apply adversarial security tests (abuse cases).

## AVERAGE MATURITY SCORES



## References:

- [1] [https://www.owasp.org/images/7/79/OWASP-WASCAppSec2007SanJose\\_SamyWorm.ppt](https://www.owasp.org/images/7/79/OWASP-WASCAppSec2007SanJose_SamyWorm.ppt)
- [2] <http://www.w3.org/Protocols/rfc2616/rfc2616-sec5.html>
- [3] [www.bbc.co.uk/news/technology-11711478](http://www.bbc.co.uk/news/technology-11711478)
- [4] <http://blog.imperva.com/2011/06/analyzing-the-lulzsec-attacks-.html>



## Bitdefender® Awake.

### The Inner Workings of an Anti-Malware Solution

Dan Horea Lutas  
Bitdefender Cluj

#### Agenda



1. Malware characteristics
2. Infection scenarios
3. Pre launch scanning
4. Runtime-monitoring
5. Post execution detection
6. Future trends in Anti-Malware

## AV industry in 1998



## AV industry in 2008



[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 3

## Anti Virus vs Anti Malware



! ! ! ! ! ! ! ! !  
threat landscape

Implies replication via file infection

Ex : Executable file infectors (PE), Macro Viruses

Malware : a broad category of digital threats comprising

Viruses

Worms

Trojans

Rootkits

Spyware

Bots

[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 4

## Malware drivers



Financial gain

Extortion (ex Ransomware)

Pay per click

Spam delivery

Phishing

Banking

Espionage

Data about company secrets

Military intelligence

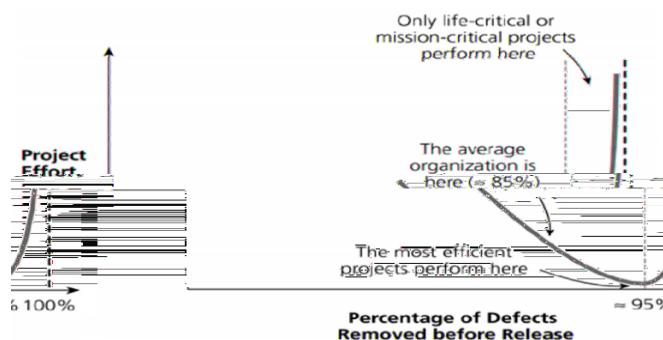
Cyber-weapons

Used instead of traditional military ways (for example instead of surgical bombing, use Stuxnet to cripple Iranian nuclear facilities)

## The problem



- network connected & functionally more complex...



- **"Today, most successful attacks simply exploit flaws that were inadvertently placed in the system during development and were not removed by industrial quality control mechanisms prior to distribution."**

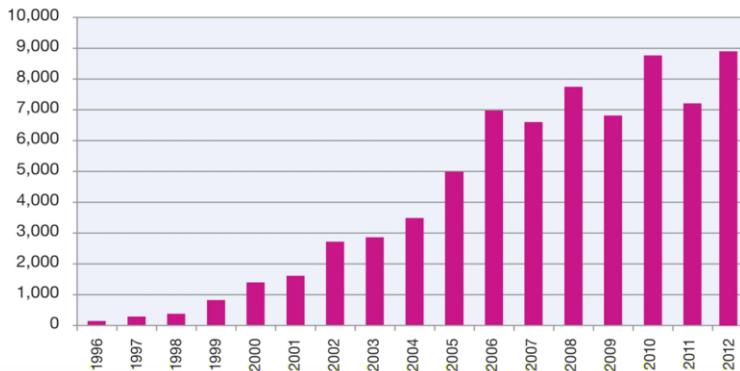
(Ladwehr, C. – Privacy and Cybersecurity: The Next 100 Years – IEEE, 2012)

## The problem



- network connected & functionally more complex...

Vulnerability Disclosures Growth by Year  
1996-2012 (projected)



cf. IBM X-Force 2012 Mid-Year Trend and Risk Report, <http://www-935.ibm.com/services/us/iss/xforce/trendreports/>

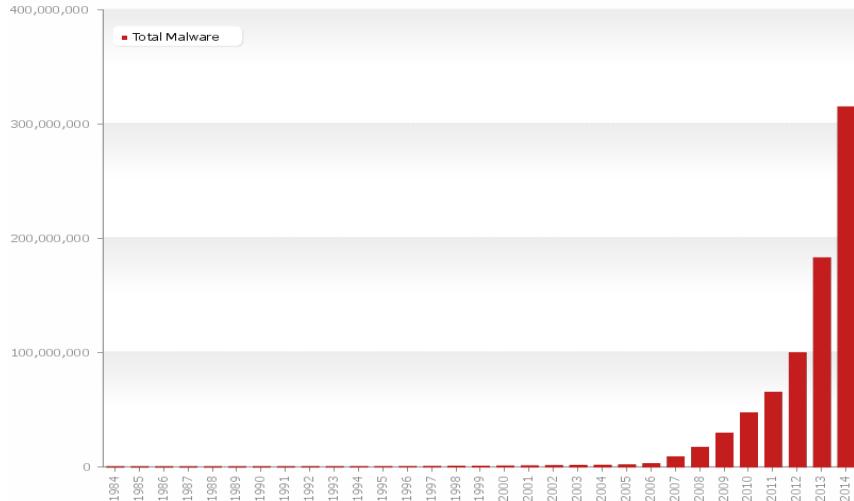
[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 7

## Malware samples growth



■ Total Malware



Last update: 12-03-2014 13:24

Copyright © AV-TEST GmbH, [www.av-test.org](http://www.av-test.org)

[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 8

## Main malware goals



Maintain persistence as long as possible

Keep a low profile

Do not display scary pop-ups, do not infect all executables (can lead to easy exposure)

Remain stealth

Use rootkit functionalities to hide files, processes, registry keys

Survive reboot

Infect boot drivers, modify registry keys,

Avoid AV detection

## Anti-Malware solutions



Paradigm shift from detection after infection (reactive detection) to preventing the infection in the first place (proactive detection)

M ! ! ! -in-

Pre-launch scanning / runtime monitoring / post execution  
deep scanning + cleaning

Defense in depth layering

Application Level (Web Browser) protection

Firewall

File Scanning (at write time) : signature based +  
emulation in virtual environment

Runtime monitoring

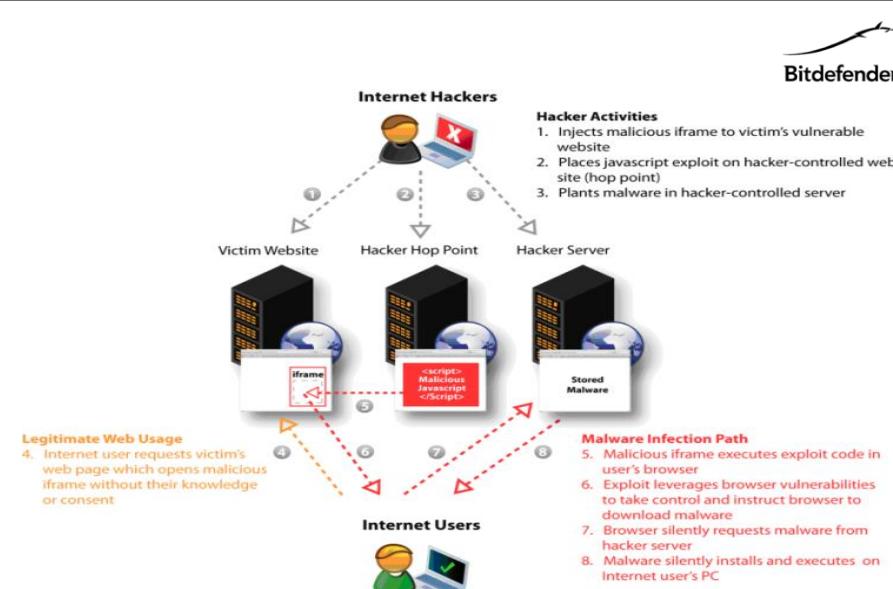
Deep scanning (reactive detection) + cleaning : used for  
detecting and removing artifacts hidden by rootkit activity

## Infection scenario 1



1. Victim visits rough web site with an unpatched web browser
2. Web site checks for browser version / OS version, chooses a vulnerability to exploit, usually encodes the payload to be unique each time (server-side generated)
3. Exploit triggers in the web browser and usually drops and launches the payload
4. Payload may download additional files and execute them
5. Malware chooses a strategy to survive reboot (registry key alterations, file infection)
6. Usually loads a kernel mode driver to hide its presence (rootkit functionality)

Rootkit hides registry keys, processes, files



Picture taken from [http://www.malware-info.com/mal\\_faq\\_inject.html](http://www.malware-info.com/mal_faq_inject.html) (Figure 8)

## Infection scenario 2



1. Victim receives a spoofed email containing an exploit embedded in a doc / pdf / etc file (Spear phishing, used mostly in APT cases)
2. Victim opens the document and the vulnerable application (eg Excel / Word / Acrobat Reader) is automatically launched.
3. Exploit executes (successfully bypassing DEP/ASLR) and drops the payload
4. Payload may download additional files and execute them
5. Malware chooses a strategy to survive reboot (registry key alterations, file infection)
6. Usually loads a kernel mode driver to hide its presence (rootkit functionality)

Rootkit hides registry keys, processes, files

## First defense : The web browser



### Bitdefender Traffic Light

In browser plugin support for IE, FireFox, Chrome, Safari

Intercepts and scans web traffic before it reaches the browser

Real time : scans the visited pages for malware and phishing attempts each and every time

Link reputation how safe if the link to be accessed

Anti-phishing

Signatures kept in the cloud, providing instant detection once a signature has been added



## The File System Filtering Driver



On Access scanning : intercept critical file operations (ex : Create, Write) on all volumes and call AV engines to perform scanning.

Interception is performed at File System level in the storage stack  
Implemented as a FltMgr minifilter driver, runs in Kernel Mode

D ! ! ! ! -mode rootkits (that perform file  
hiding by hooking in user-mode processes)

! ! ! ! ! ! ! ! ! ! ! !  
the file system, this critical driver intercepts the operation and  
dispatches the file for scanning to the AV engines.

P ! ! ! D ! ! ! ! ! ! ! ! ! ! ! !  
returned to the application

## The File System Filtering Driver (continued)



Intercepts creation of new processes, using process  
callbacks notifications from the kernel

Dispatches a Scan request to AV engines to scan the  
executable image from which the process is being  
launched

Has support for Registry filtering

Uses Registry Callbacks notifications from the kernel to  
filter operations such as

Adding a new Value to the registry

Modifying existing registry values

Filtered requests are send to the AV engines

D ! ! ! ! ! !

## Pre-execution scanning



After is written to the File System, before is allowed to run, each executable is scanned by AV engines

Main components of AV engines

Signatures : specific patterns extracted from previously analyzed malware and used by the Engines to provide detection

Engines specific to file types

Java Script

Office : Word, Excel (macro viruses, exploit detection)

BMP / JPG / Flash (exploit detection)

Routines specific to different malware families (ex : routine for detection and cleaning of files infected with a specific File Infector)

Unpacking engines

Emulator + in-Virtual Environment Behavior Analysis : B-HAVE

## Packers / protectors



Packing / protecting a file is a mean to make analysis / detection harder

Classical model :

Wrapper around a single executable

At creation time the protector compresses / encrypts the content of  
! ! !

Add another section responsible for de-compression / decryption of the sections when executed and also contain anti-debugging / anti-emulation tricks

F ! ! ! ! ! ! !

The protected program will run identically to the unprotected version

A previously seen malware, from which signatures were extracted, can be made undetectable again by packing / protecting it

Examples : UPX, Armadillo, ASPack, ASProtect etc

Unpacking engines identify the type of protector applied and perform the reverse operation

This way, existing signatures become effective again, this time applied to the unpacked executable

## Unpacked vs Packed file



The screenshot shows two memory dump windows side-by-side. The left window displays the memory dump of an unpacked file, showing various sections of assembly code and comments. The right window displays the memory dump of a packed file, where the original code has been replaced by packed data. The Bitdefender logo is visible in the top right corner of the interface.

## Unpacking limitations



Advanced protectors deploy techniques that make unpacking hard

Unpack the executable in a new process

Operate in a dual process mode : the original executable debugs a modified version of itself

Translate code into an intermediary language and interpret it during run-time : this way the original executable code is never revealed. Examples : Themida, VMProtect

Existing signatures become ineffective if same malware is protected with such advanced protectors

## Dynamic detection in virtual environment (B-HAVE)



Static signatures (reactive detection) suffer from limitations , for example

Use of packers / protectors

Polymorphic code

Sheer number of malware : aprox 100.000 unique samples **each day**  
received by Bitdefender

Solution : Heuristic Detection

Heuristics principle : if a program exhibits malware-like  
characteristics, then probably is malware

Static scanners

F ! ! ! ! ! ! ! !  
determine the actions that are likely to be performed

Dynamic scanners

Execute the program in a virtual (emulated) environment

F ! ! ! ! ! ! ! !

Check if any of those actions match malware behavior

!0 ! ! ! ! !

[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 21

## Limitations of emulation in virtual environment



Modern malware usually contains anti-debugging and anti-emulation features

It is very difficult for an emulator to properly emulate :

- a. The whole IA32/64 instruction set (such as FPU / MMX / SSE / SSE2 / AVX etc registers and instructions operating on them)
- b. A whole virtual environment consisting of all the APIs that are present in a real system (ex : kernel32.dll exports 1390 APIs on Windows 7 SP1)

Malware can make use of exotic instructions, call obscure API functions that are less likely to be implemented, causing the emulation to fail => avoids detection

Because of these limitations, a new approach is needed :  
runtime monitoring

[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 22

## Run-time monitoring – Active Virus Control



Active Virus Control is a proactive, dynamic detection technology, based on monitoring processes behavior, and tagging suspect activities

Its main components are:

User mode and kernel mode **API/system call filtering**

**Heuristic system** that identifies malware actions and evaluates their impact

It is extensible by developing new heuristics they can be updated on the fly

It is designed to facilitate **cleanup**

No user interaction needed, all decisions automatically taken



## AVC Components



Mini-filter driver

Implements a file system mini-filter, registry filtering, process filtering and heuristics evaluation logic

Function driver

Commands the hypervisor (start, stop, deliver options)

Hypervisor (on x64 platforms)

Runs in ring -1

Kernel mode heuristics mini-filter driver

Implements heuristics based on kernel filtering (file system, registry and system call filtering)

User mode filtering/heuristics library

Implements heuristics based on user mode API hooking

Injected in each monitored process, when the process starts (de-injection is not possible)

Multiple instances (even with different versions) can run at the same time

Communication library

## AVC incompatibilities / limitations



1. Like any other malware detection technologies, there is a chance that AVC can issue false positives
2. There can be incompatibilities or conflicts with:
  - Executable packers/protectors
  - Software that performs user mode/kernel mode hooking
  - Applications that expect the presence of specific data/code at fixed virtual addresses in process address space, if those virtual addresses overlap with AVC modules, or with memory allocated for/by AVC

## Post Execution - Deep scanning



Context : after the system became infected (malware executed, dropped rootkit to hide components, trying maintain persistence, survive reboot)

O ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !

Files

Processes

Registry keys

Once these artifacts are detected, they are dispatched to AV

! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !

repeated

P ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! !

(files deleted, registry keys / values removed, processes terminated)

## **Hidden Files : brief description**



Hidden files are files not seen by the generic windows API and therefore might contain (and usually do) rootkits which will evade virus scans

How is it possible ? Listing the files in a directory by using the windows API undergoes a sequence of steps (request packages getting passed to the entire storage stack) and thus a file can easily be hidden by a filter driver positioned at any of these steps

Some files may have hidden content, filtered by certain rootkits which will  
dangerous rootkit inside

How do we find them ? By issuing read requests to the lowest level driver in the storage stack (port-miniport level)

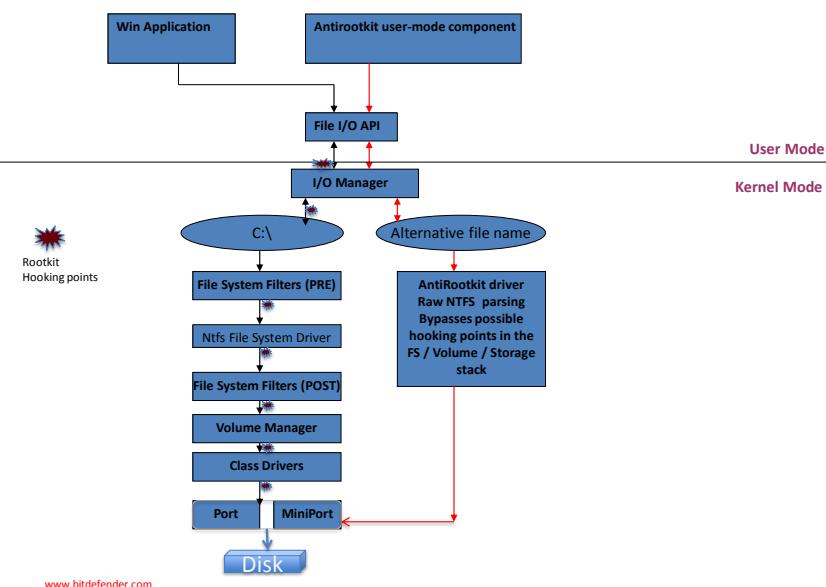
The drawback is that we have to use our own NTFS parsing algorithms, since we bypass the whole File System stack

Cross-view based detection : Read through WinAPI, then read directly from disc and check for differences

[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 27

## Windows FS / Volume / Storage stacks



[www.bitdefender.com](http://www.bitdefender.com)

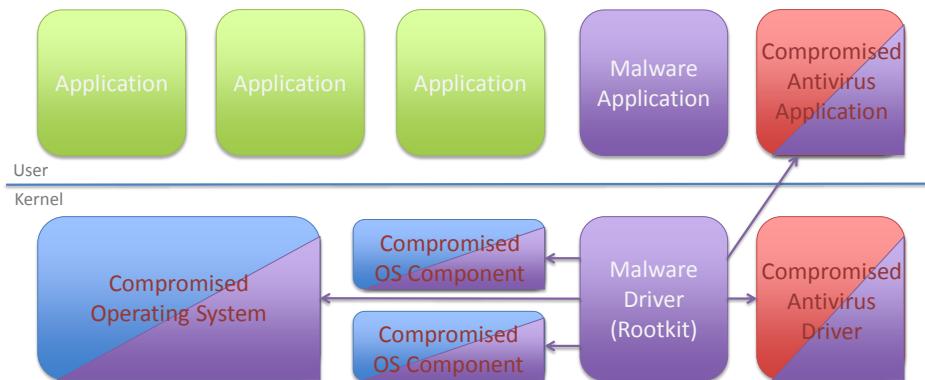
1/5/2015 • 28

## Hidden Registry / Hidden Processes



Registry keys / values hiding : same concept / mechanisms as for file hiding  
In kernel in0.36 r(cetm)-4(i)6con (y)27(st)-5eam ervic(e)5(( )8)-5(or )1(R)6(eg)4(i)

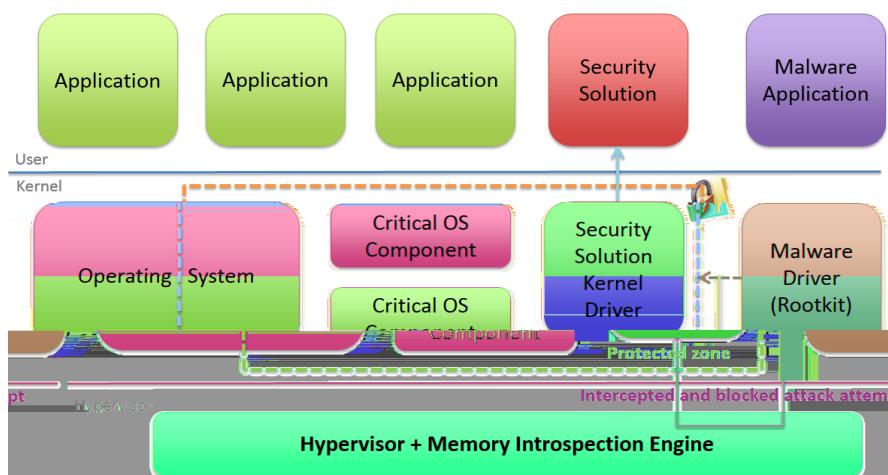
## Typical Antivirus Solutions



[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 31

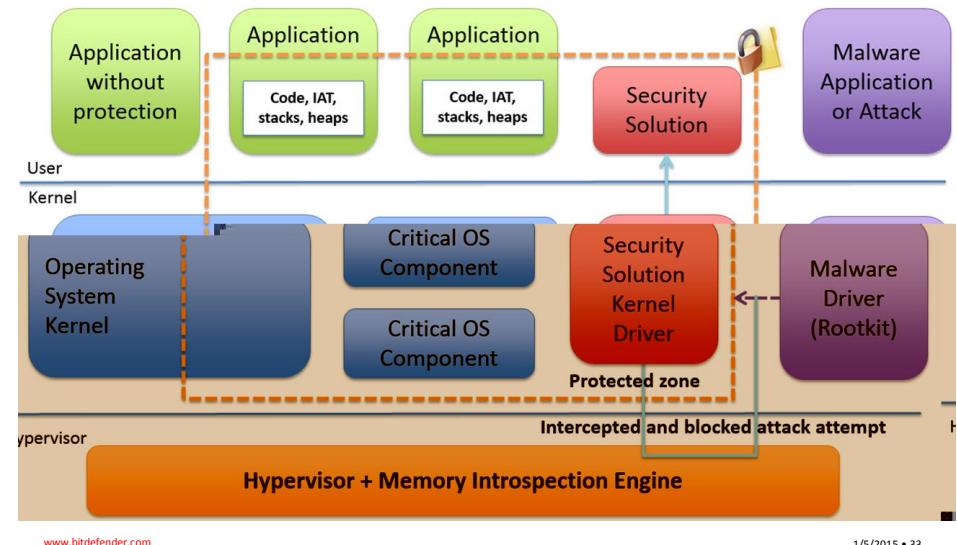
## Hypervisor protects critical kernel OS and AM security components



[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 32

## Hypervisor protects critical kernel and user-mode OS and AM security components



[www.bitdefender.com](http://www.bitdefender.com)

1/5/2015 • 33

Bitdefender®

# **SECURITATEA IN SISTEMELE IT**

---

## **RISK MANAGEMENT**

Adrian Chioreanu, PhD Eng



**UNIVERSITATEA TEHNICĂ**  
DIN CLUJ-NAPOCA

- Why Risk Management
  - What is Risk Management
  - Information Security Risk
  - How we Assess Risk
  - Risk Assessment – LAB
  - Risk Owner & Treatment
- 

# AGENDA/CUPRINS

*There is a story about a monastery in Europe perched high on a cliff several hundred feet in the air.*

*The only way to reach the monastery was to be suspended in a basket which was pulled to the top by several monks who pulled and tugged with all their strength.*

*Obviously the ride up the steep cliff in that basket was terrifying. One tourist got exceedingly nervous about half-way up as he noticed that the rope by which he was suspended was old and frayed.*

*With a trembling voice he asked the monk who was riding with him in the basket how often they changed the rope. The monk thought for a moment and answered brusquely, "Whenever it breaks."*

### **Moral:**

***Know what your appetite for risk is and make sure you put measures in place so you don't exceed this!***



**The monastery of Holy Trinity was a filming location in the 1981 James Bond movie *For Your Eyes Only***

# WHY RISK MANAGEMENT

---

# Why Risk Management

- Minimise uncertainty
- Reduce incident impacts and occurrences
- Better service for our customers
- Make informed decisions



# Risk vs. reward



# WHAT IS RISK MANAGEMENT



# What is Risk Management

## Risk – A definition

"An event that **could occur**, with the effect of bringing **uncertainty**, either **positive** or **negative**"

## Risk Management – A definition

"The means by which IT risks are **identified, assessed, mitigated, monitored** and **reported** to **manage uncertainty**"

## An Incident – A definition

"An event that **has occurred**, which is **not part of the standard operation** of a service and which causes or may cause an **interruption** to, or a **reduction** in, the **quality** of that service"

*"Understanding risk and managing it is key for **maximising benefit** and **minimising uncertainty** – risk management however should be **tailorable, dynamic** and **responsive to change**"*

# What is Risk Management

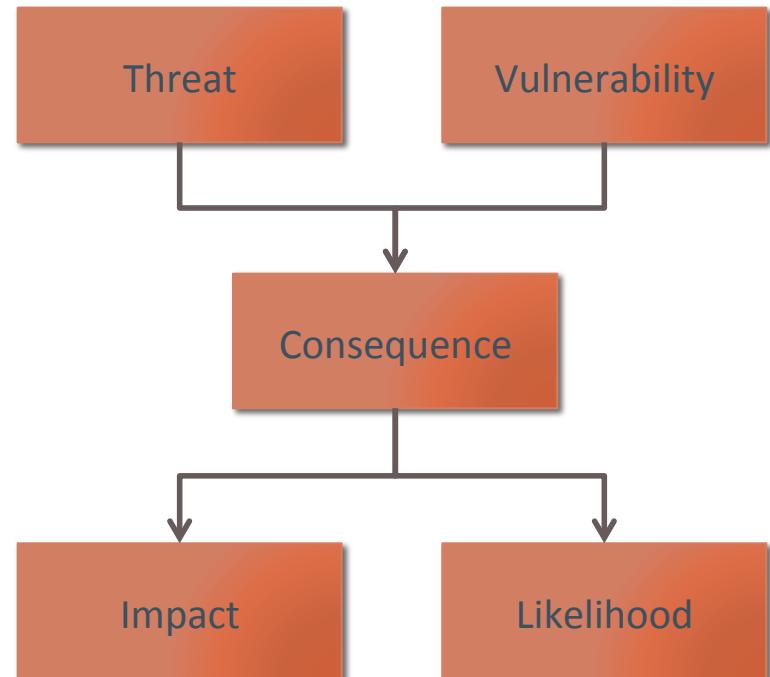
- So there's something we want to avoid - Getting wet
  - Consequence
- And a thing that might cause that - Rain
  - Threat
- A way for it to happen - Going outdoors
  - Vulnerability
- Why we care - Going to an important meeting
  - Impact
- Will it rain? - Weather forecast, look out the window
  - Likelihood
- Manage that risk - Stay inside, buy an umbrella, hire a Taxi, move in the desert?
  - Mitigation



*What we've done is make a risk based decision, so that when we walk out of the front door carrying an umbrella, it's because we feel it will rain, and if it does rain... we're covered!*

# What is Risk Management

- **Risk** – An event that could occur, with the effect of bringing uncertainty
- **Threat** – An event that could harm business assets or services
- **Vulnerability** – A weakness that could be exploited by threats
- **Consequence** – A description of the result if a threat occurs
- **Impact** – The rating we give a consequence
- **Likelihood** – The chance that a vulnerability will be exploited by a threat



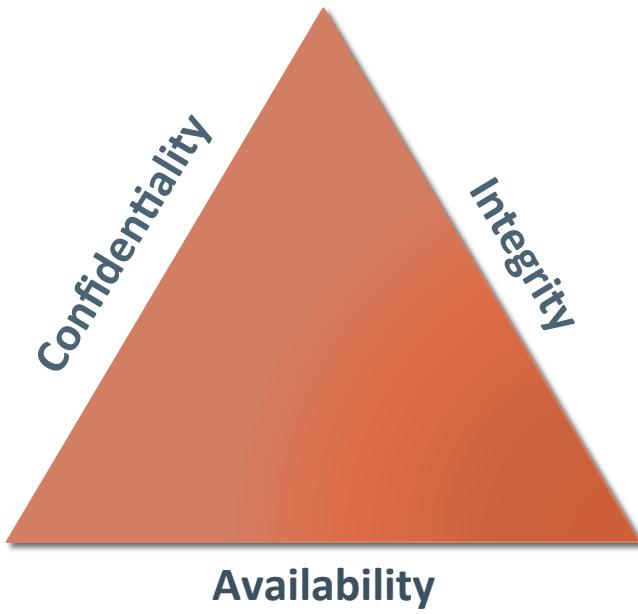
# What is Risk Management

- **Risk Identification** – ID, Analyse, Evaluate
- **Risk Treatment** – Reduce, Accept, Transfer, Avoid
- **Action Plan** - activity to reduce risk to an acceptable level



# Information Security Risk

**Information Security Risk** – Any risk to the confidentiality, integrity or availability of information.



**Confidentiality** – information is not made available or disclosed to unauthorised individuals.

**Integrity** – information is accurate and complete, so can be relied upon by authorised individuals.

**Availability** – information is accessible and usable when needed by an authorised individual.

# RISK ASSESSMENT



# How we assess risk

Threat - potential cause of the event, which may result in harm to the company



Vulnerability - weakness of an asset or control that can be exploited by the threat(s)

Consequence - a description of the result to the organisation should a risk be realised, i.e. vulnerability exploited by threat

Impact - a rating of the described consequence

Likelihood – a rating of probability of the described consequence occurring

# How we assess risk

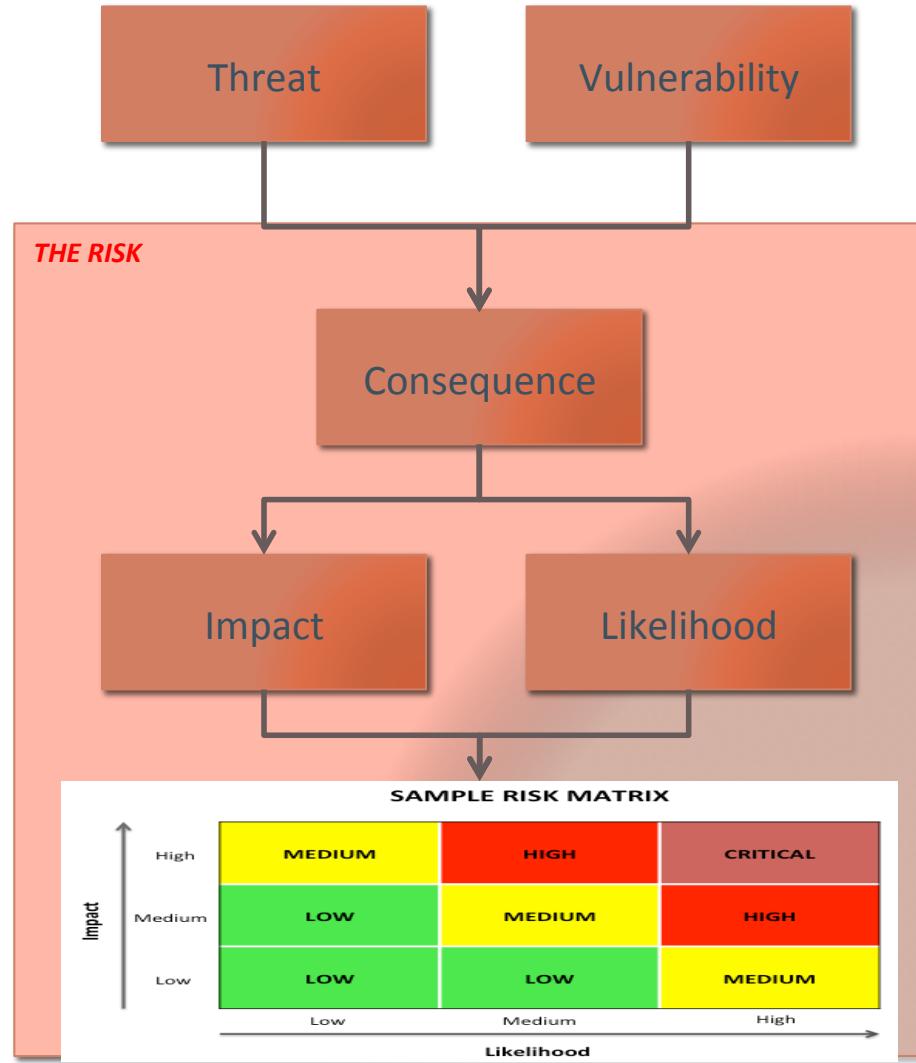
A potential event or **sequence of events** that has the **potential to harm** assets such as information, processes and systems and therefore. Threats may be of **natural** or **human** origin, and could be **accidental** or **deliberate**

e.g – A hacking group release malware that infects an employees machine via a download

The rating of the **impact** of the **consequence** occurring

Weaknesses that can be **exploited** by **threats** to cause harm to assets or to company

e.g – Virus protection software is not updated automatically on all employees machines



A description of the result to the company should a **risk be realised**, i.e. a vulnerability be exploited by a threat

e.g – Loss or damage of company information assets

The rating of the **probability** of the **consequence** occurring

# Likelihood

Score	Rating	Likelihood
1	Rare	May occur only in exceptional circumstances. Occurs once in 100 years or more.
2	Unlikely	Could occur at some time but would require remotely possible coincidences. Occurs once in 50 years.
3	Possible	Might occur at some time. Possible sequence of coincidence is unusual. Occurs once in 10 years.
4	Likely	Will probably occur in most circumstances. Not unusual. Occurs once in every 2 to 5 years.
5	Almost Certain	Is expected to occur in most circumstances. Occurs more often than once in two years or is almost constant.

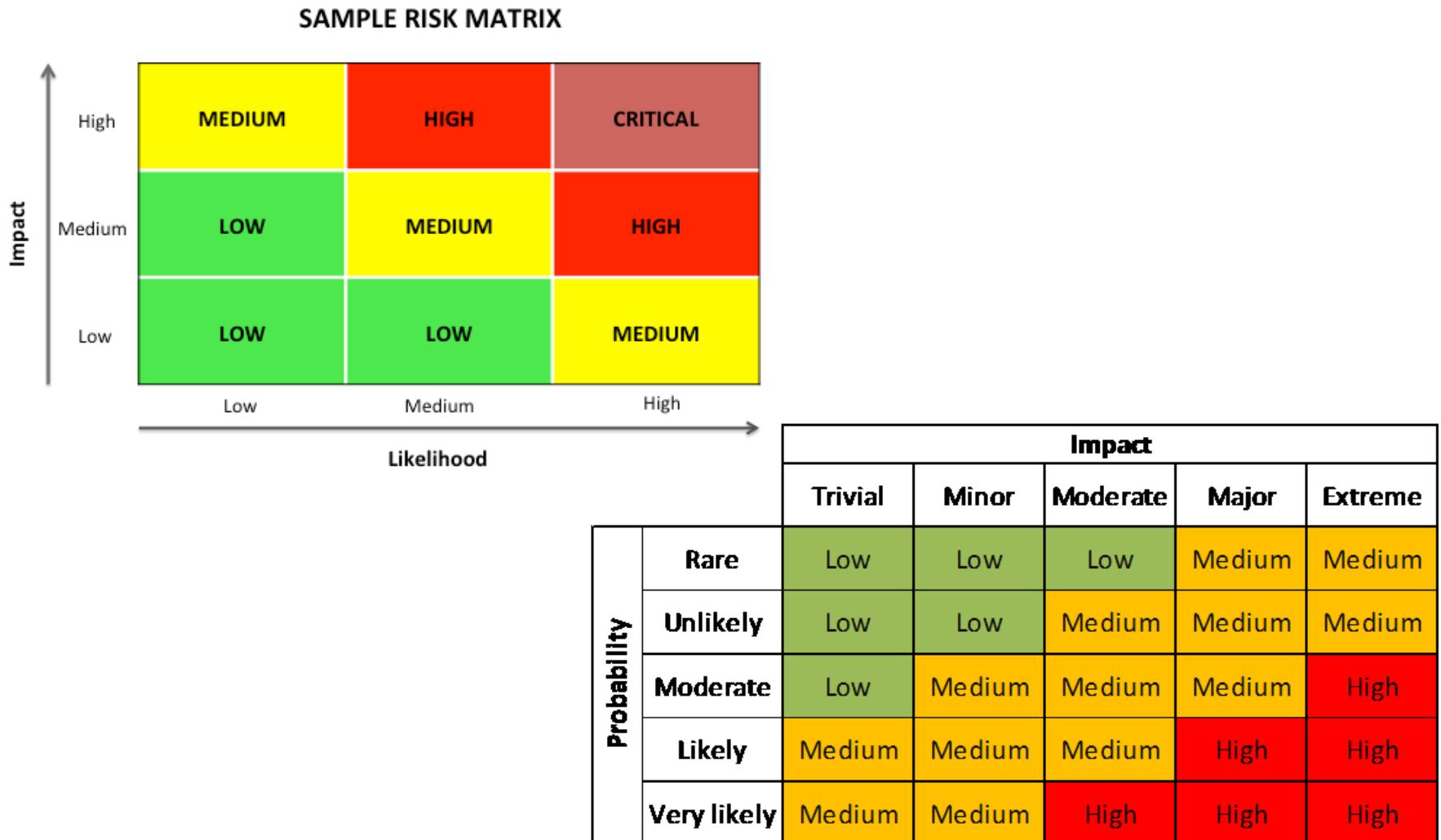
Image from: [http://  
www.marchmenthill.com](http://www.marchmenthill.com)

# Impact

Score	Rating	Health and Safety Consequence	Environmental Consequence	Financial Consequence
1	<b>Minor</b>	Minor first aid or no injury.	Minor harm to the environment (e.g. noise complaint).	< \$100k Loss
2	<b>Important</b>	Disabling injury (less than 5 days off work).	Temporary harm to the environment (e.g. small area of contamination).	\$100k - \$1m Loss
3	<b>Serious</b>	Serious injury (amputation, permanent disability).	Harm to the outside environment.	\$1m - \$10m Loss
4	<b>Major</b>	One fatality.	Extensive damage to the environment (e.g. large area of contamination).	\$10m – \$100m Loss
5	<b>Catastrophic</b>	More than one fatality.	Massive, irreversible damage to the environment.	> \$100m Loss

Image from: <http://www.marchmenthill.com>

# Likelihood & Impact



# RISK ASSESSMENT - LAB

---

# RISK OF CRICKET STUMPS BEING STOLEN

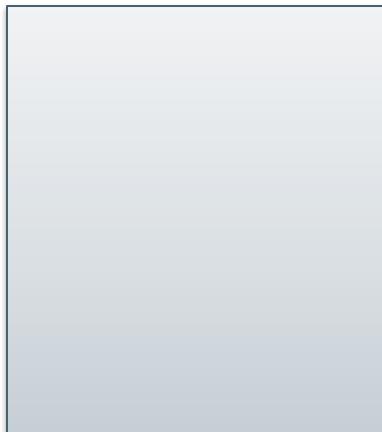
Threat



Consequence



Vulnerability

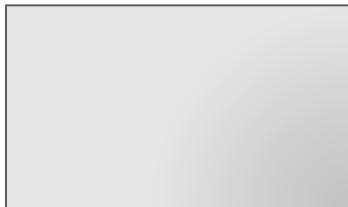


Likelihood Factors

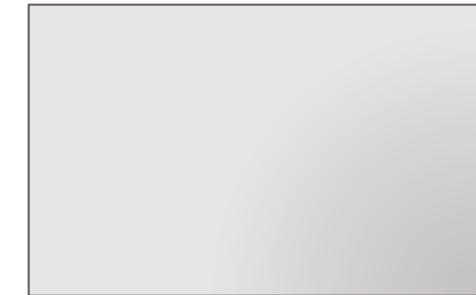


# Risk of a rugby post breaking

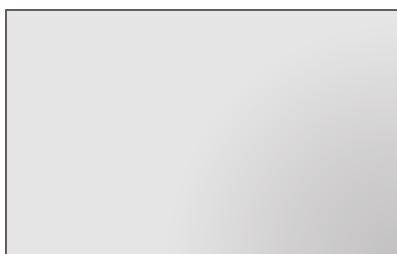
Threat



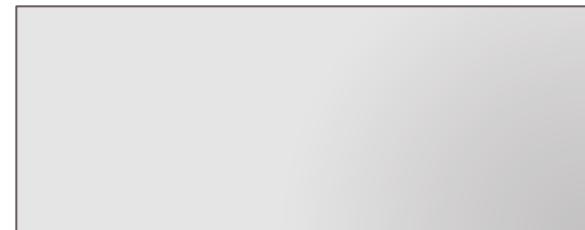
Consequence  
(Impact)



Vulnerability



Likelihood



# RISK OF CRICKET STUMPS BEING STOLEN

## Threat

- Drunk Spectator
- Protestor
- Hungry Seagull



## Consequence

- Interruption of the game
- Game abandoned
- Spectators refunded
- Reputation damage to "The Game of Cricket"

## Vulnerability

- Open access to the pitch
- Stumps are light, and small
- No vetting of fans
- Proximity to the coast...

## Likelihood Factors

- Alcoholic drinks available in the ground
- Police intelligence - activism/protests
- RSPB advisory!

# Risk of customer data being lost

Threat

- Disgruntled employee joins rival company
- Customer data used during development
- Crime Syndicate targeting sites

Vulnerability

- No removable media controls
- Lack of security testing for new Products
- Default name for accounts

Consequence

- Reputational damage
- Customer complaints
- Regulator penalties
- Loss of revenue

Likelihood Factors

- Intell (increased gambling sector hacker activity)
- Busy Project pipeline



# Risk of a rugby post breaking

Threat

- Ball hitting the upright
- Strong winds
- Termites

Consequence (Impact)

- Death (VH)
- Injury (H)
- Delayed Game (L)
- Abandoned Game (M)
- Refunds (M)

Vulnerability

- Low quality materials
- Dodgy supplier
- Lack of weather proofing
- No inspections

Likelihood



- Experienced Player
- Average attempts per game
- Number of games per day
- Number of uprights
- Weather reports

# Risk of an IT system failing



Threat

- It's a hot day
- Software Upgrade

Consequence (Impact)

- Loss of service (H)
- Loss of revenue (H)
- Customer complaints (M)
- Bad press (M)
- Regulator penalty (VH)

Vulnerability

- Hardware is EoL
- Support contract has expired
- Software is 'buggy'
- Environment is poor
- Lack of experienced staff

Likelihood

- History of low-level service issues in Company
- Industry articles on recent major failures

# RISK OWNER & TREATMENT

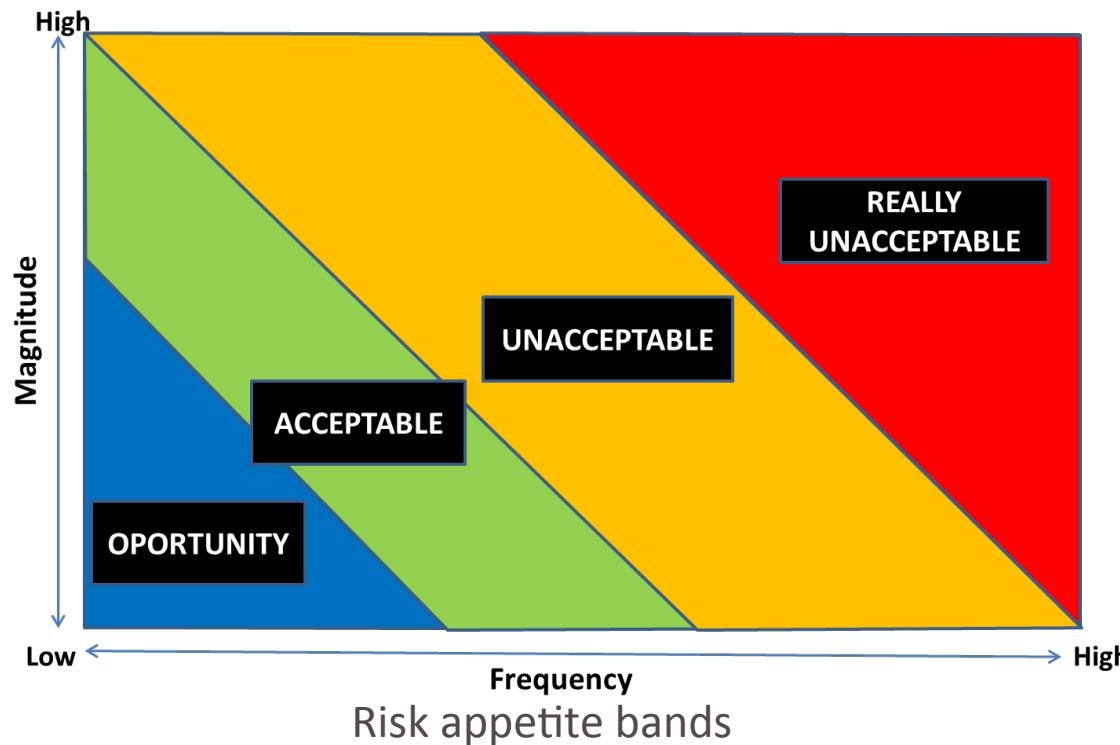
---

# Risk Owner & Treatment

- Risk Owner – the individual at the appropriate level (according to the risk rating and risk acceptance criteria) leading the team most impacted by the consequence of the risk. Where the risk owner is unclear it should be the system/process owner (at the appropriate level) acting as the custodian for the data
- Risk Treatment – the process of selecting and implementing measures to manage the risk.
- 4 risk treatment options:
  - Reduce - action is taken to reduce the likelihood and/or impact of the risk
  - Accept - no action is taken relative to the risk, and loss is accepted when/if it occurs. Note: this is different from being ignorant of risk; i.e. an informed, cost-benefit decision has been made by management
  - Transfer - reducing risk likelihood or impact by sharing a portion of the risk (e.g. insurance or outsourcing)
  - Avoid - exit the activities that give rise to the risk

# Risk Appetite & Tolerance

- Risk appetite—The broad-based amount of risk Company is willing to accept in pursuit of its mission (or vision)
- Risk tolerance—The acceptable variation relative to the achievement of an objective



# Risk vs. Reward

- Risk doesn't stop us doing things
- Taking risk is an important aspect of what we do as a business
- However, we need to take the right risks...
- It helps us to do the things we want to do, whilst knowing what *could* happen, and allowing us to prepare for that.

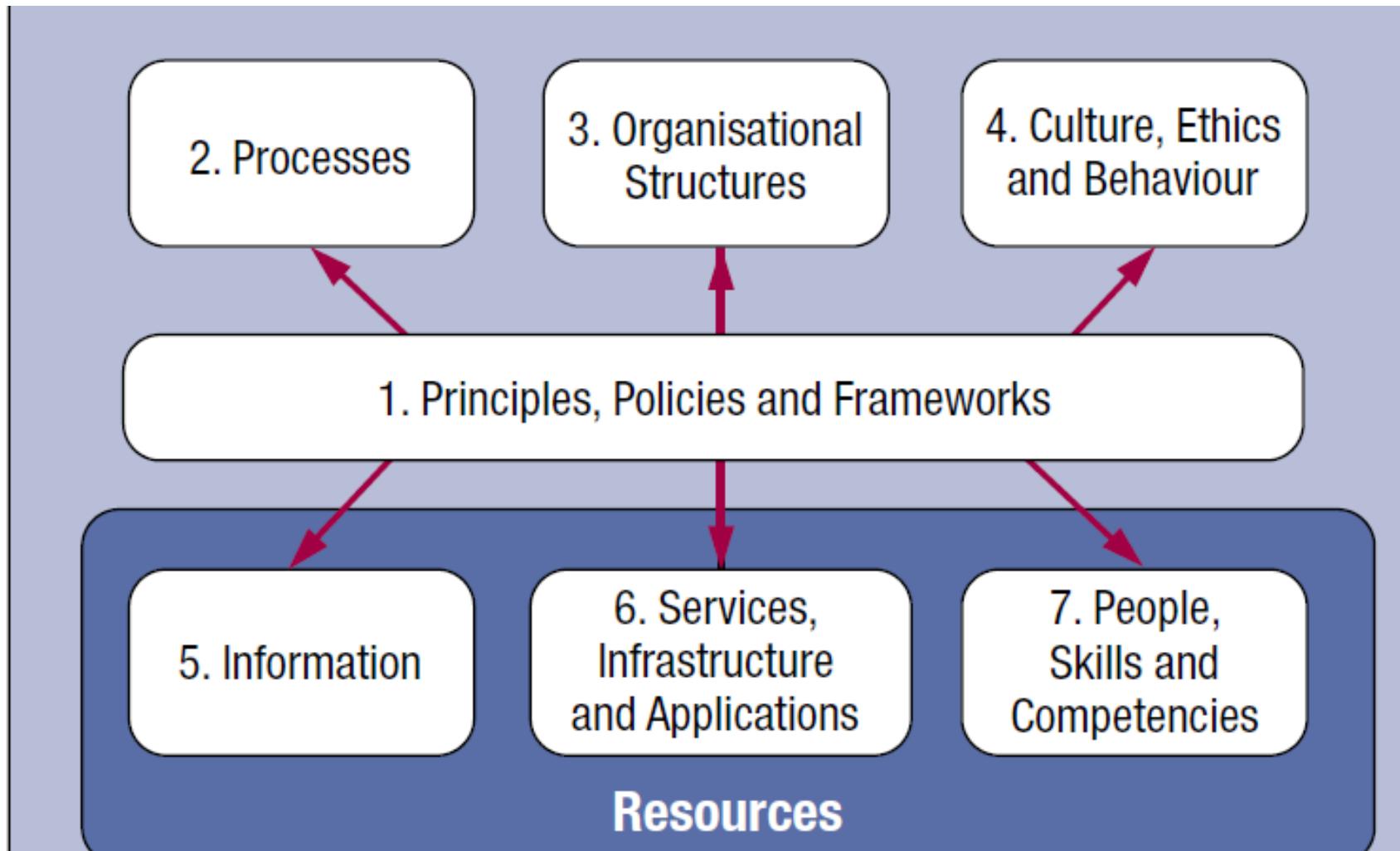


# Q&A

---



# Enablers



# INFORMATION SECURITY

AWARENESS



Nov 17, Vasile Dorca

# summary

**Global Cyber Crime**

**Exercise**

**Video – Social Networking**

**Why we do awareness?**

**How we do awareness?**

**Topics to cover**

**Next steps**

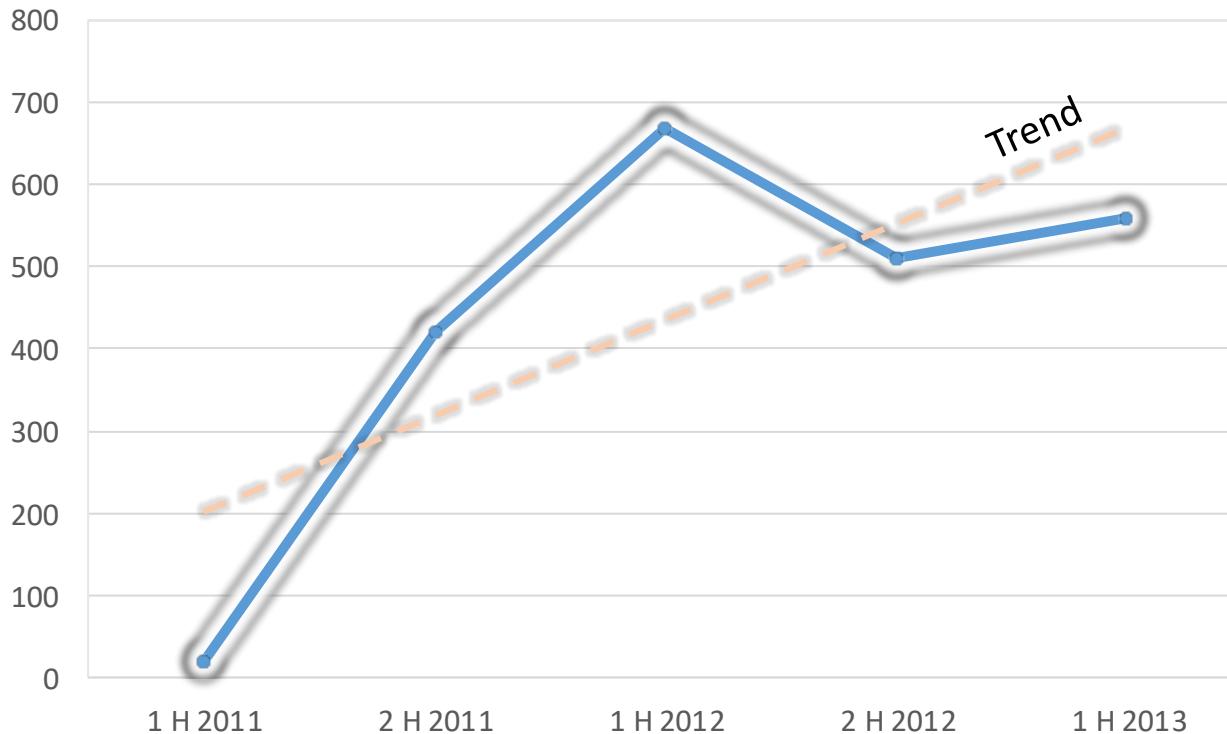


If you could be any animal, what would you be and why?



# Cybercrime – the “best” investment on the planet

## International Serious Cyber Attacks



**254% growth** in attacks against Companies and Government in 2012

# Cybercrime – the “best” investment on the planet

copyright @ Ralf Christian Kunkel



Today's ICT is like **my first 1990 Oltcit** in terms of built-in security.

As a consequence, **in 2012 this inherent cyber insecurity** had a global (direct and indirect) estimated cost of **USD 388 billion (that is Denmark's GBP)**

## Economical aspects for criminal organisations

### **COST:**

Development of the malware on basis of the existing Zeus toolkit	\$500
Use of spam botnet	\$50
Hosting a command and control centre	\$2,000
Use of the PC botnet for setting up sessions to Internet Banking	\$500
Translators for bank error pages	\$500
Cost of money mules in the Netherland and Ukraine/Russia	\$10,000

### **BENEFITS:**

23 transactions \$116,000

**Return of investment:** **750%**

# Cybercrime – the “best” investment on the planet

## Threats are growing especially on Social Media

Threats to Online Services, including Social Media and Cloud Services: 900% Y/Y

Victims per typology	2011	2012	Variations
Gov – intelligence	153	374	244%
Others	97	194	200%
Entertainment/News	76	175	230%
Online Services/Cloud	15	136	907%
Research – Education	26	104	400%
Banking/Finance	17	59	347%
SW/HW Vendor	27	59	219%
Telco	11	19	173%
Gov Contractors	18	15	-17%
Security	17	14	-18%
Religion	0	14	140%
Health	10	11	110%
Chemical/Medical	2	9	450%
Critical Infrastructures	-	-	
Automotive	-	-	
Org/ONG	-	-	

# Real world examples

The collage includes the following snippets:

- Open Letter to Information Security Officer Resigns**  
U.S. Department of Veterans Affairs' (VA) chief information officer resigns effective July 13.
- The Attack On G...**  
Posted January 15, 2010
- Mail Online**  
Home News U.S. | Sport | TV&Showbiz | Femail | Health | Science | Money | Video | Coffee Break | Travel | Columnists Login
- LAST CHANCE to register for Dec 2013 exam!**  
Registration closes on 30 Oct.
- Gambling giant Betfair loses millions of customers' credit card details to cyber attack... then covers it up for 18 MONTHS**  
Hacking believed to be the work of criminals based in Cambodia
- By LUCY BUCKLAND**  
UPDATED: 14:44 GMT, 30 September 2011
- Book a Room >**
- Hilton HOTELS & RESORTS**  
From £124 per night  
Book a Room >
- Hilton Malta**  
St. Julians
- From £76 per night**  
Book a Room >
- Hilton Vilamoura**  
Vilamoura

Other visible text and snippets include:  
First, b...  
the acco...  
of the atta...  
George Ku...  
Aurora. As a...  
pulling out of...  
Second, the How...  
vectors. Microsoft...  
higher was the atta...  
used. iDefense spec...  
shown definitively to be...  
Third, the attacks were no...  
campaign that targeted the...  
Dow Chemical, Symantec,...  
Fourth, many affected parties a...  
Google, Adobe, Microsoft, McAfe...  
More than 3.1 million account names with encrypted security questions, 2.9 million usernames, and nearly 90,000 account usernames with bank account post-mortem analysis, including those with fatal errors, is often a fatal error.



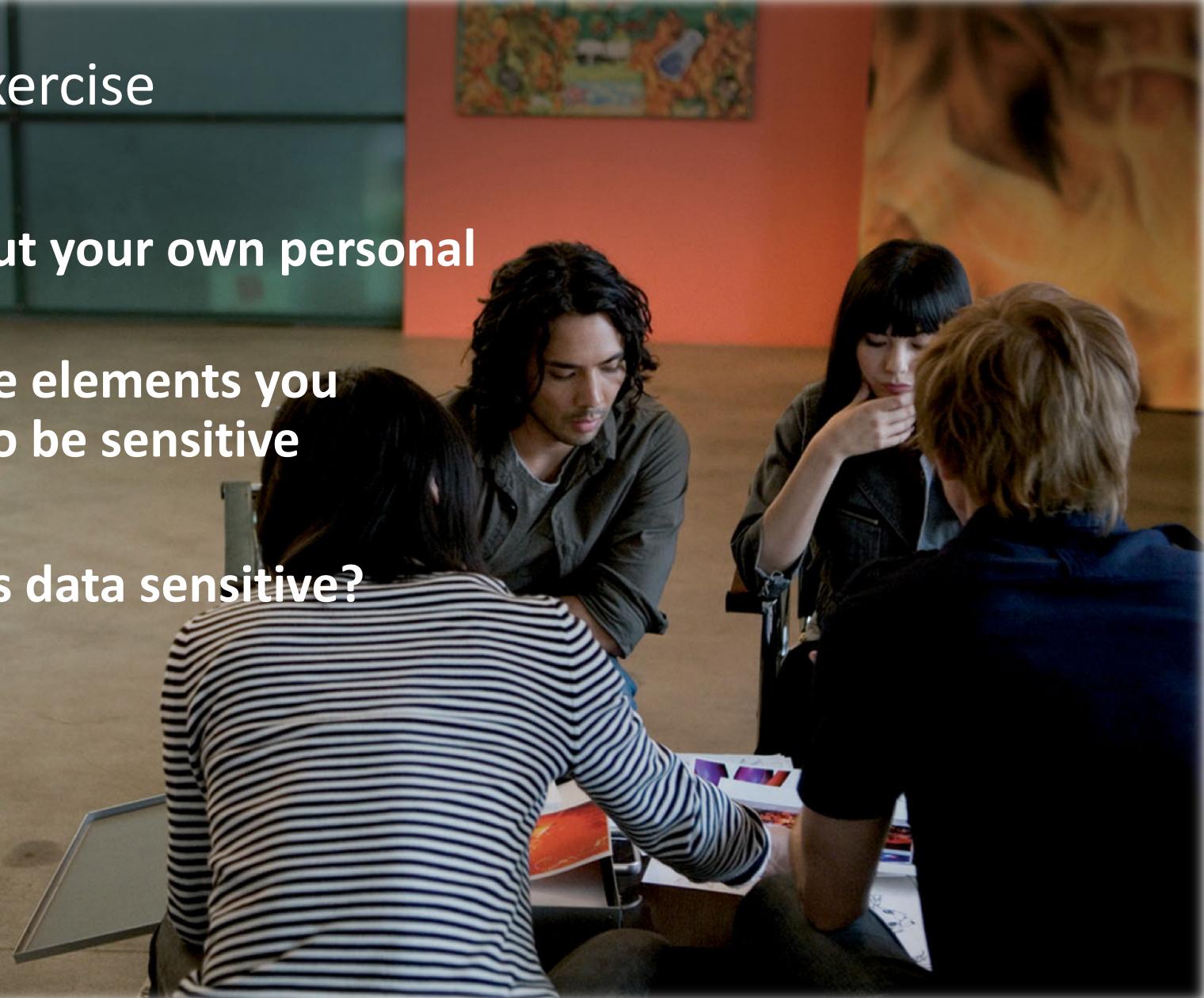
Amazing mind reader reveals his 'gift'.MP4

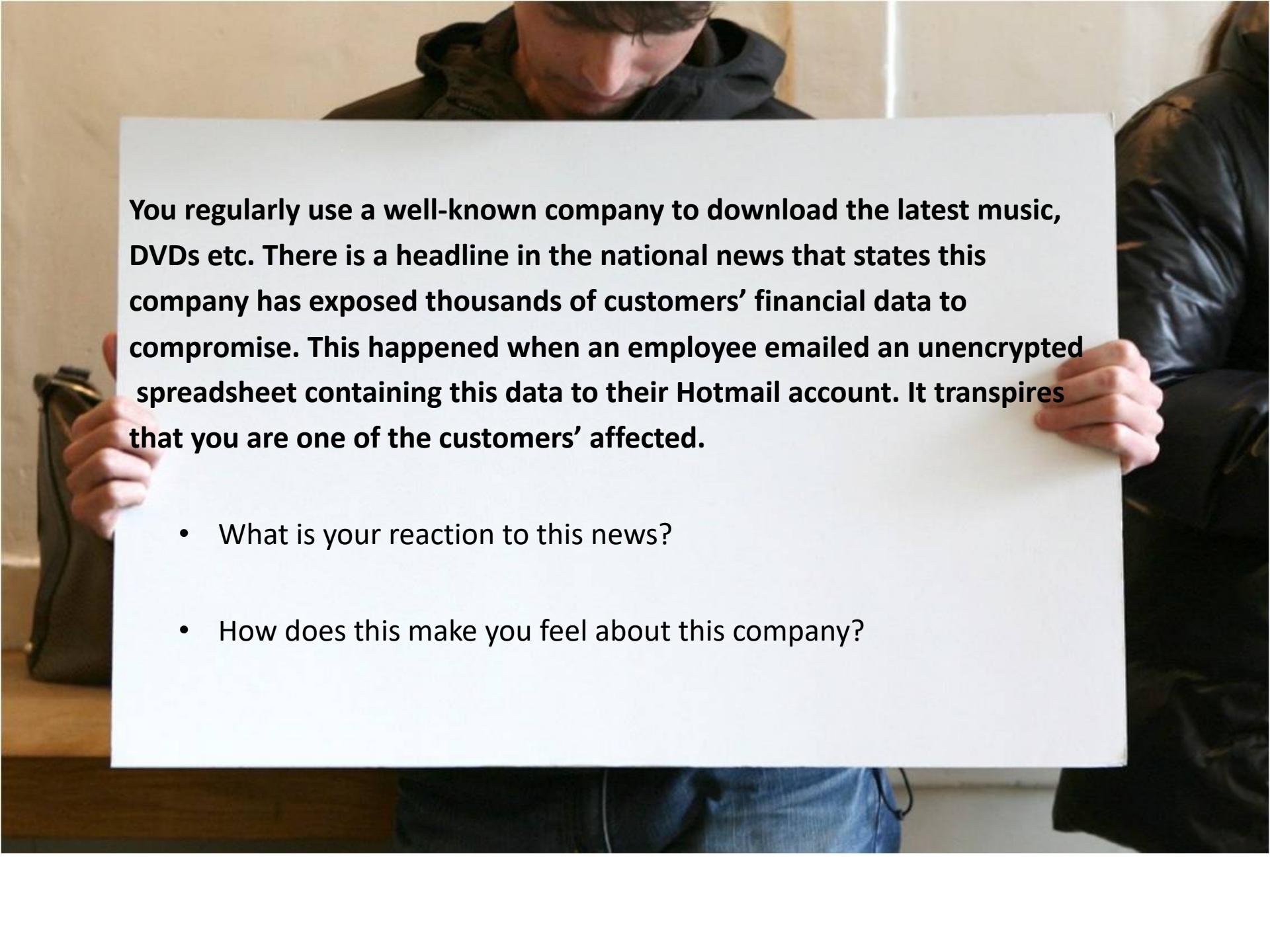
<https://www.youtube.com/watch?v=F7pYHN9iC9I>

# Group exercise

Think about your own personal data  
and list the elements you consider to be sensitive

Why is this data sensitive?





You regularly use a well-known company to download the latest music, DVDs etc. There is a headline in the national news that states this company has exposed thousands of customers' financial data to compromise. This happened when an employee emailed an unencrypted spreadsheet containing this data to their Hotmail account. It transpires that you are one of the customers' affected.

- What is your reaction to this news?
- How does this make you feel about this company?

# Group exercise

**What data do you handle as part of your role?**

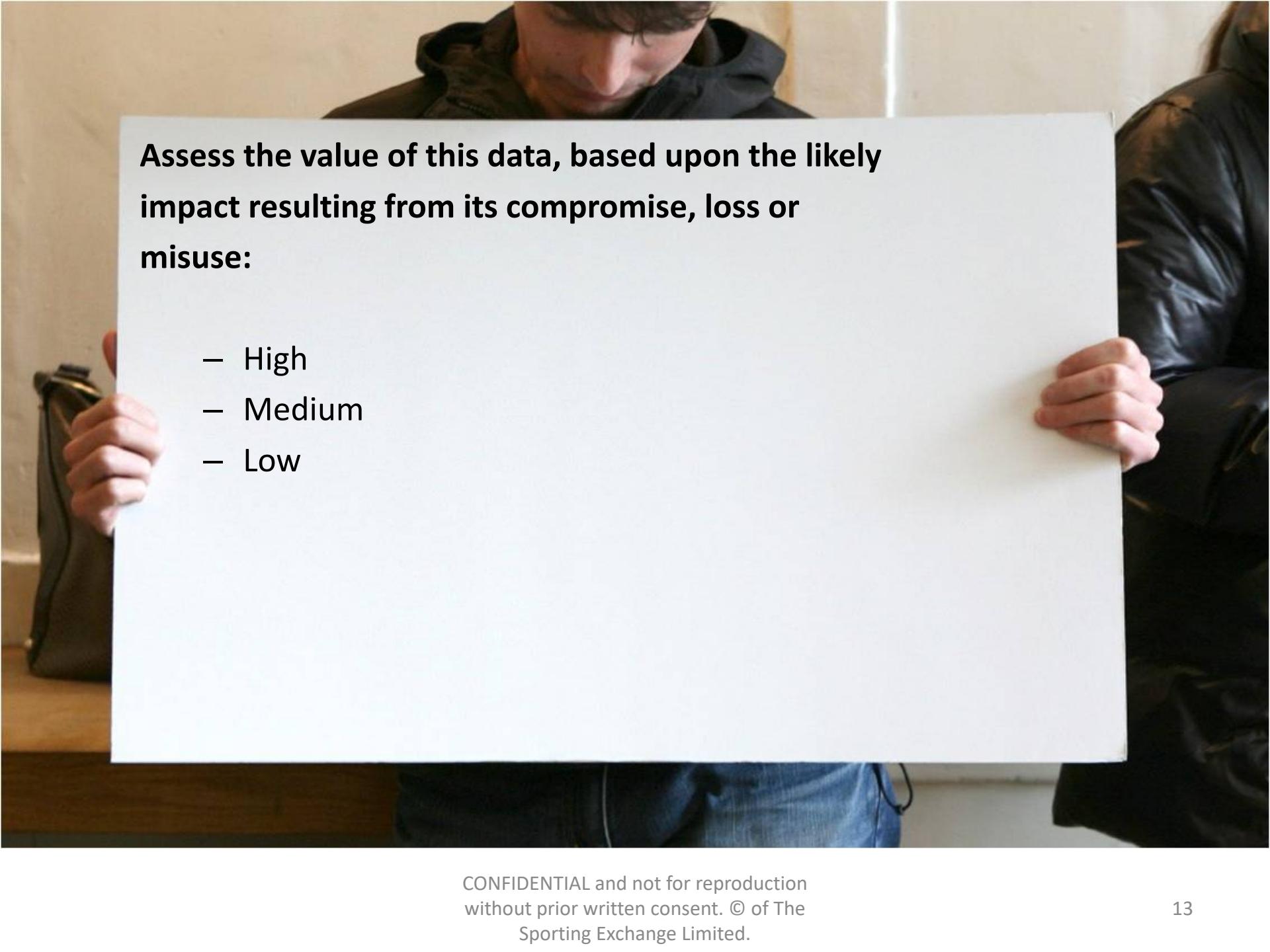
- Employee data
- Customer data
- Company data

**Does all of the data we hold have the same value?**

**How do we determine its value?**

**What do we need to consider?**

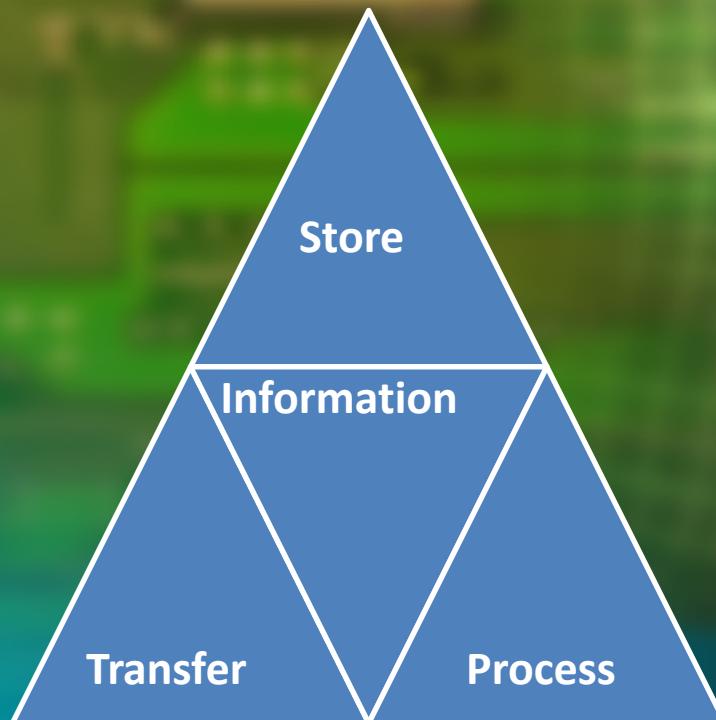
- Value of data = the impact on Betfair of the loss or compromise of the data.

A photograph of a young man with dark hair and glasses, wearing a dark hoodie and blue jeans. He is holding a large, blank white sheet of paper in front of him with both hands. The paper covers most of the lower half of the frame. He is looking down at the paper. To his left, a portion of a black smartphone is visible. The background is a plain, light-colored wall.

**Assess the value of this data, based upon the likely impact resulting from its compromise, loss or misuse:**

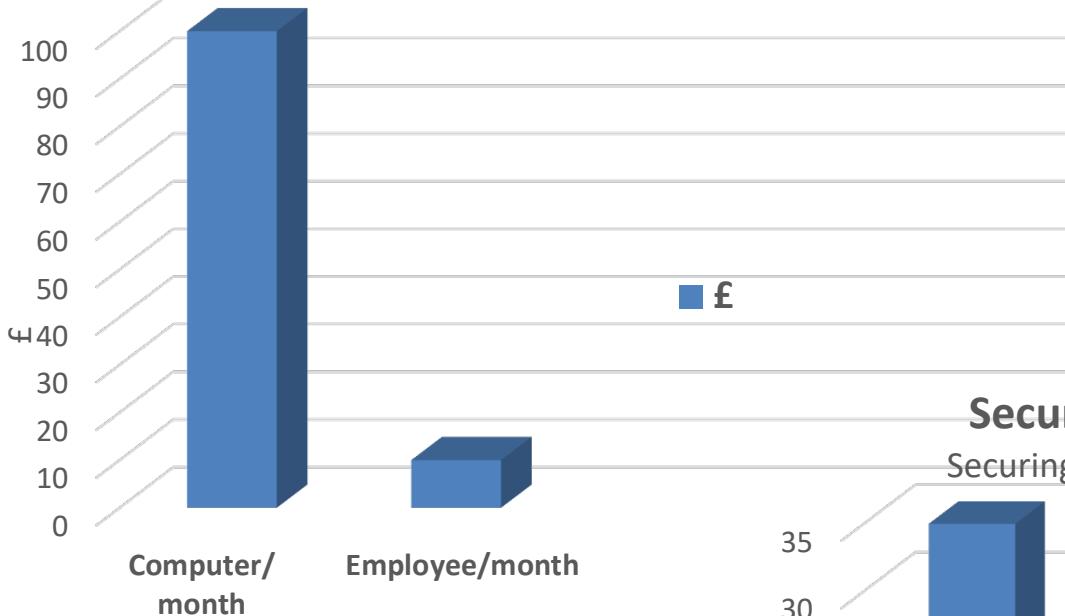
- High
- Medium
- Low

Like computers, people store, process and transfer information, in some ways they are another operation systems



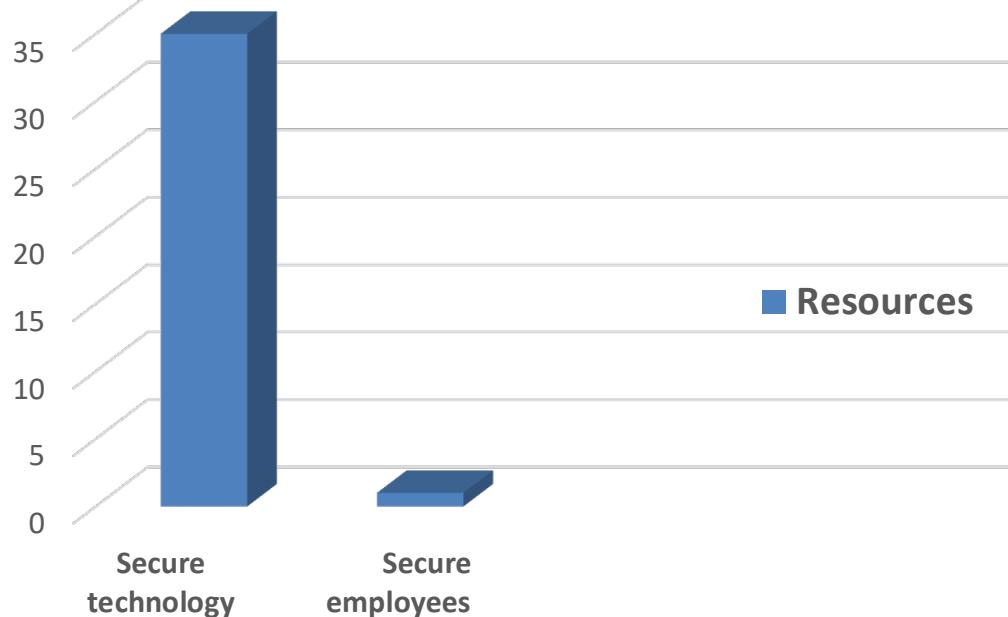
## Cost Comparison

Securing computers vs. Securing employees



## Security Resources Comparison

Securing technology vs. Securing employees

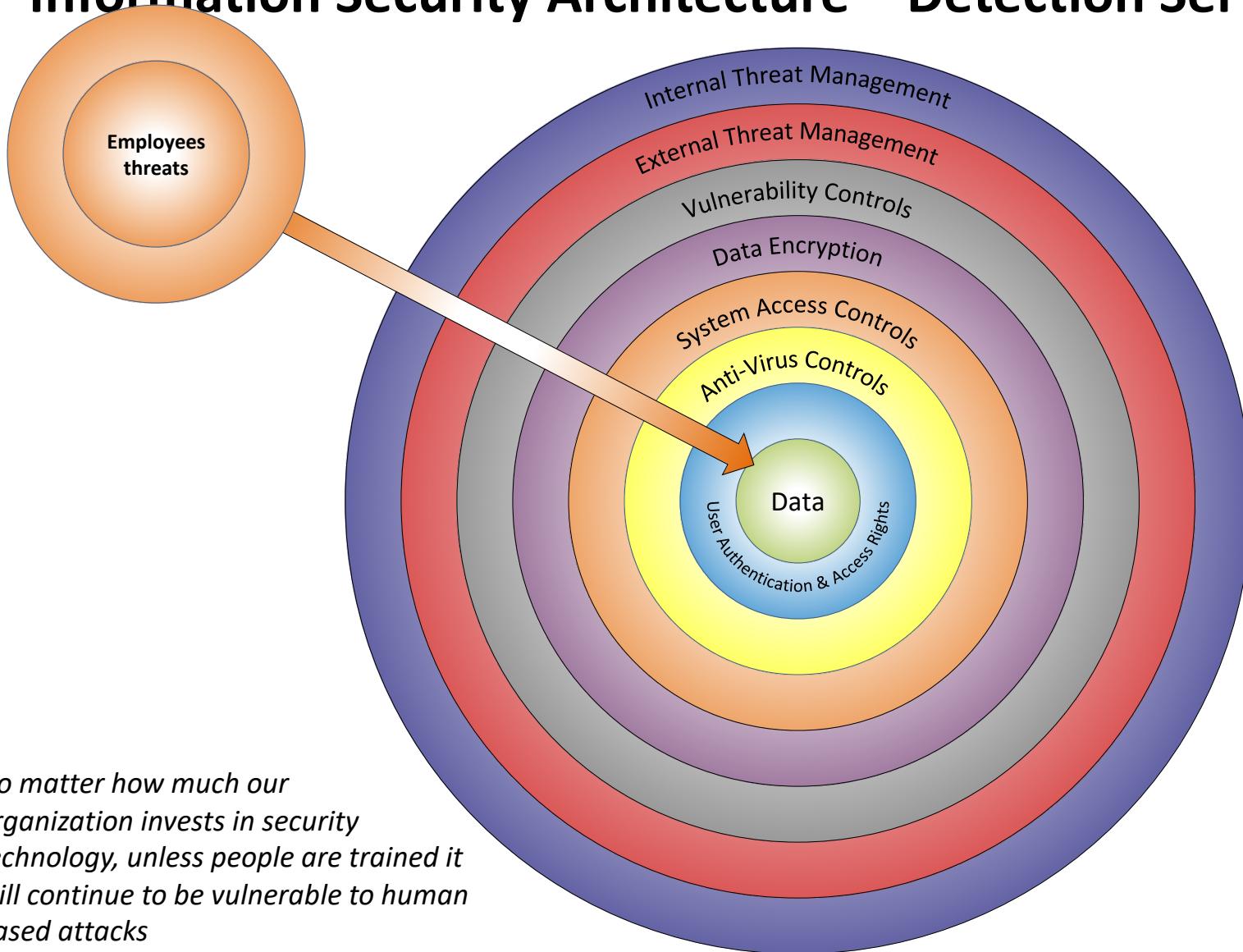


# WHY WEEDO AWARENESS?

The collage includes the following snippets:

- info security** (Europe Edition): "View UK Content", "View US Content", "No Preference", "infosecurity EUROPE". Categories: News, Blog, Virtual Conference, Webinars, Downloads/ White Papers, Events & Training, Podcasts/ Newscasts, Company Directory, Application Security, Biometrics, Business Continuity and Disaster Recovery, Cloud Computing, Compliance and Policy, Data Privacy.
- ADVANCED TARGETING**: "WE GET THEM".
- THE WALL STREET JOURNAL**: "EUROPE EDITION". Headline: "Successful bank phishing attacks target compromised infrastructure". Date: 06 March 2012. Subtext: "Nearly all of the successful phishing attacks against US banks exploit compromised infrastructure, according to data compiled by email security firm Agari." Paragraph: "Criminals use legitimate infrastructure – servers and software – owned by reputable institutions to conduct successful phishing campaigns against banks, a technique known as infrastructure hijacking, Agari said in a release." Paragraph: "Using compromised, legitimate servers allows the criminals to bypass a battalion of email security defenses and deliver phish to the inbox. In fact, of the top 300 successful phishing attacks to US banks, all used compromised servers from legitimate companies", Agari noted." Paragraph: "Surprisingly, the greatest phishing threats to US banks originate from US servers, which were responsible for distributing the majority of top phishing threats to US institutions. Of all phishing threats to US banks, 39.2% originated from the US, nearly four times higher than number two-ranked Germany."
- CNN Money**: "AD View".
- SOCIAL-ENGINEERING**: "SOCIAL-ENGINEERING AS IT'S PRACTICED BY CYBERCRIMINALS".

# Information Security Architecture – Detection Services



*No matter how much our organization invests in security technology, unless people are trained it will continue to be vulnerable to human based attacks*

# Why we do Awareness?

## 1. Reduce risk

- Phishing awareness – Measure: decrease in number of “victims”
- Infected computers – Measure: decrease in number of infections
- Awareness Test – Measure: increase in number of correct answers

## 2. Remain compliant

- ISO27001, BS25999 – Measure: Keep compliant
- PCI – Measure: keep compliant
- Regulatory compliance requirements - Measure: keep compliant

# Why we do Awareness?

## 3. Reduce costs

- freeing up security resources to focus on more advanced threats –  
Measure: decrease in time spent on malware incidents, infections

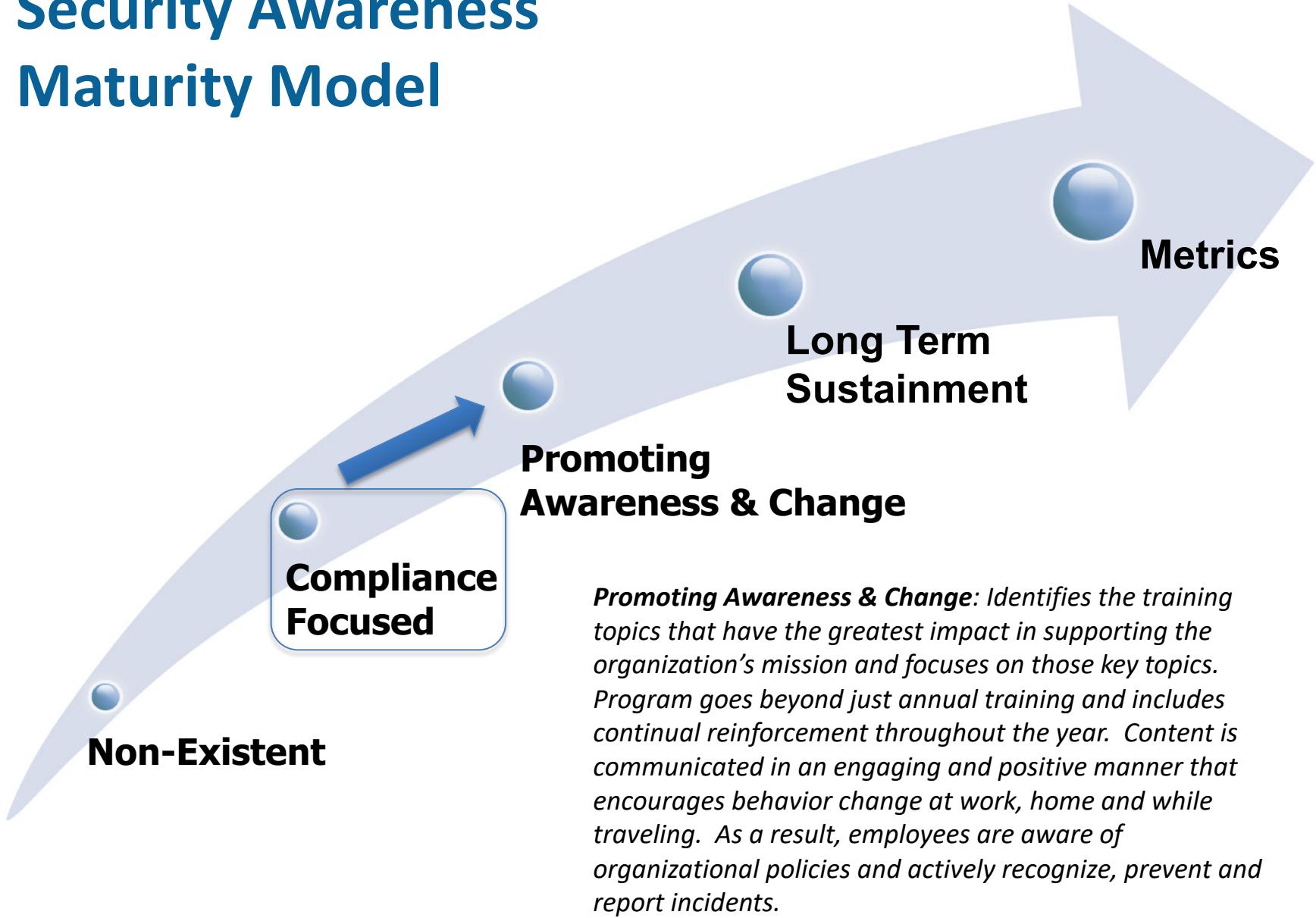
## 4. Promote a secure Betfair brand

- that is serious about protecting our customers
- keeping the customer commitment

## 5. Train employees – Measure: increase in number of training participants

- on our policies
- processes
- standards

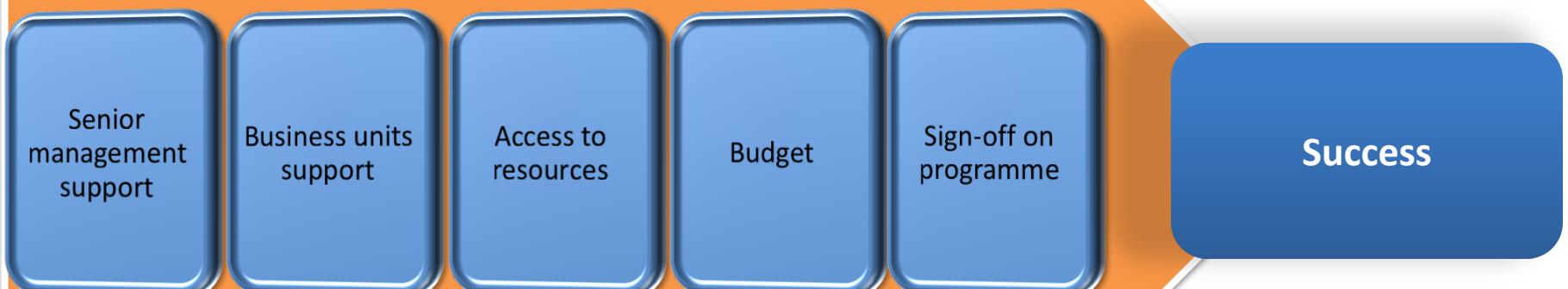
# Security Awareness Maturity Model



# Key Points on Awareness

- **Most awareness programs have had little impact because they were never designed to:** Most awareness programs were or currently are driven to check the compliance box. As such minimum resources were invested, perhaps a workshop once a year or an occasional newsletter. Of course this would have little or no impact, would we consider our systems secure if we patched them once a year? Security awareness has radically changed in the past several years in the industry, now they are designed to change behavior, to have an impact.
- **Awareness is another control:** No matter how much we train people someone will always fall victim. This is true. However security awareness is nothing more than a control to reduce risk, just like firewalls, Intrusion Detection Systems or Anti-Virus. Just like any of these other technologies security awareness cannot stop all attacks, just most.
- **Long term program – lifecycle:** Awareness is also a long-term investment. To truly change behavior and create a secure culture, security awareness training must happen year after year. We would not actively patch our computers month after month for a year, then at the end of the year say “That’s it, we are done”.
- **Not just prevention – detection and response:** Also, why limit awareness to just prevention? We need to give people the ability to identify and report hacked systems, greatly expanding our detection and response capabilities.

# What We Need



# Summary

- Humans are **another operating system** but to date very little has been done to secure them.
- We can **dramatically reduce risk** to our organization and remain compliant by implementing an active, longer term awareness program.

# SCOPE

**General end user awareness:** Provide general awareness training to employees in order to meet the objectives:

- Launch the **phishing exercise and the end user security test**
- Advertise the new **CBT online internal training portal**
- Provide **monthly awareness packs**: videos, newsletters, emails, policy messages
- Provide **periodical updates**: lessons learned, did you know articles, leadership awareness messages
- Standardize and customize the **Security Induction Training**
- Keep the **Security Intranet page updated**
- Build and maintain an **awareness metrics pack**
- Continuously provide **visual awareness materials** (posters, screensavers, etc.)
- Re-launch the same **phishing exercise and the awareness test**
- **Risk Management Awareness, 3<sup>rd</sup> Party Security Management**

# Scope

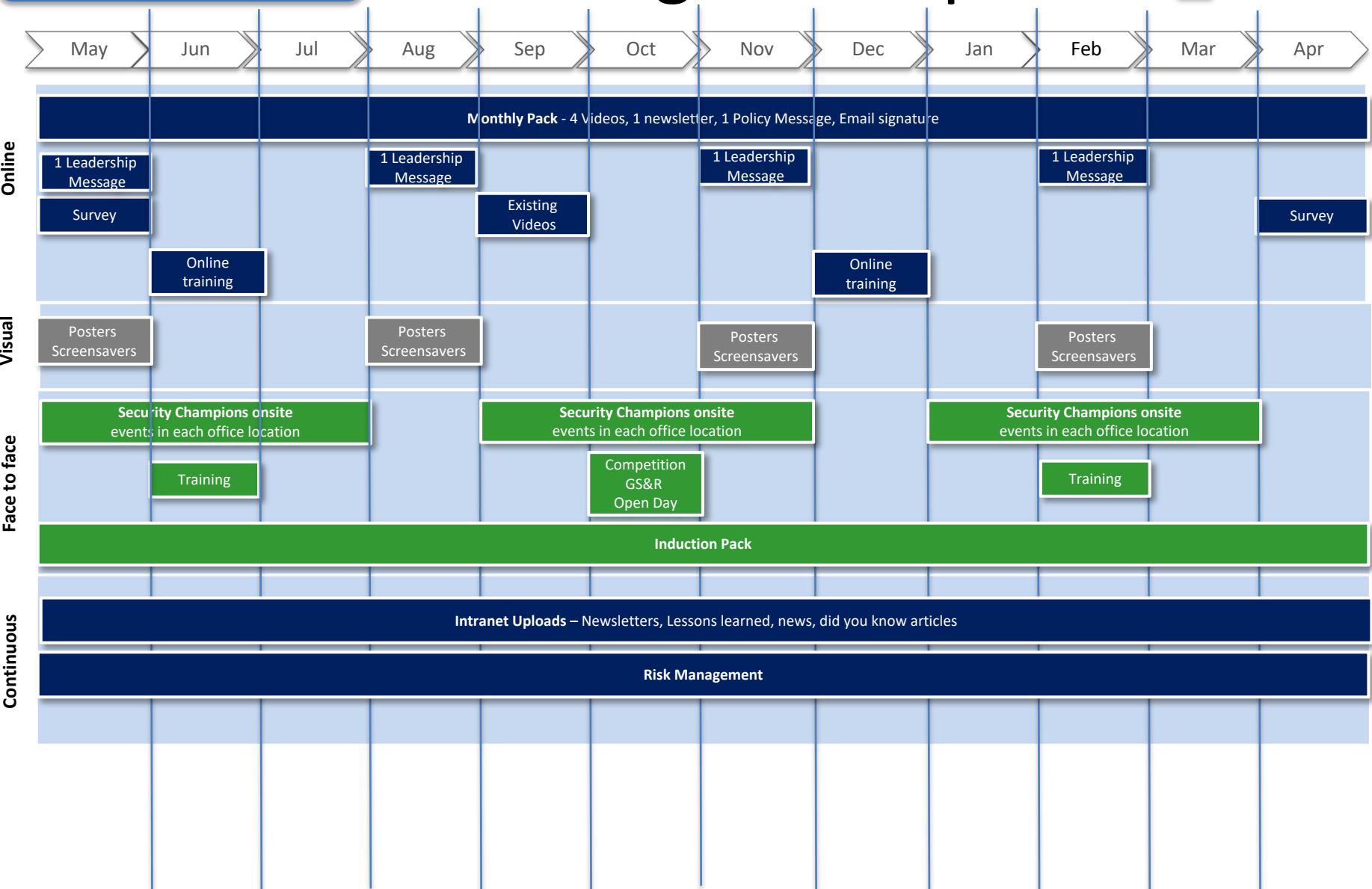
**Customized security awareness:** Provide customized awareness training to certain teams, based on risks (e.g. incidents history) and access to (deal with) customer data in order to meet the objectives:

- Continue the **Security Champions** programme – provide at least 3 training/workshop events/year/location (Romania, UK, Porto).
- Provide **periodical trainings** to Development and IS teams
- Define the “**high risk**” areas that deal with customer data and need awareness trainings – e.g. marketing
- Provide **periodical updates**: videos, newsletters, lessons learned, did you know articles, leadership awareness messages

## AWARENESS PLAN

# Programme plan

 Online  
 Face to face  
 Visual



# Awareness topics

[www.securingthehuman.org](http://www.securingthehuman.org)

- You Are the Target
- Social Engineering
- Email & Messaging
- Passwords
- Encryption
- Data Security
- Insider Threats
- Help Desk
- IT Staff
- Browsing
- Social Networks
- Mobile Device Security
- Wi-Fi Security
- Working Remotely
- Physical Security
- Protecting Your Personal Computer
- Protecting Your Home Network

**Thank You!**