Countermeasures To Advanced Threats

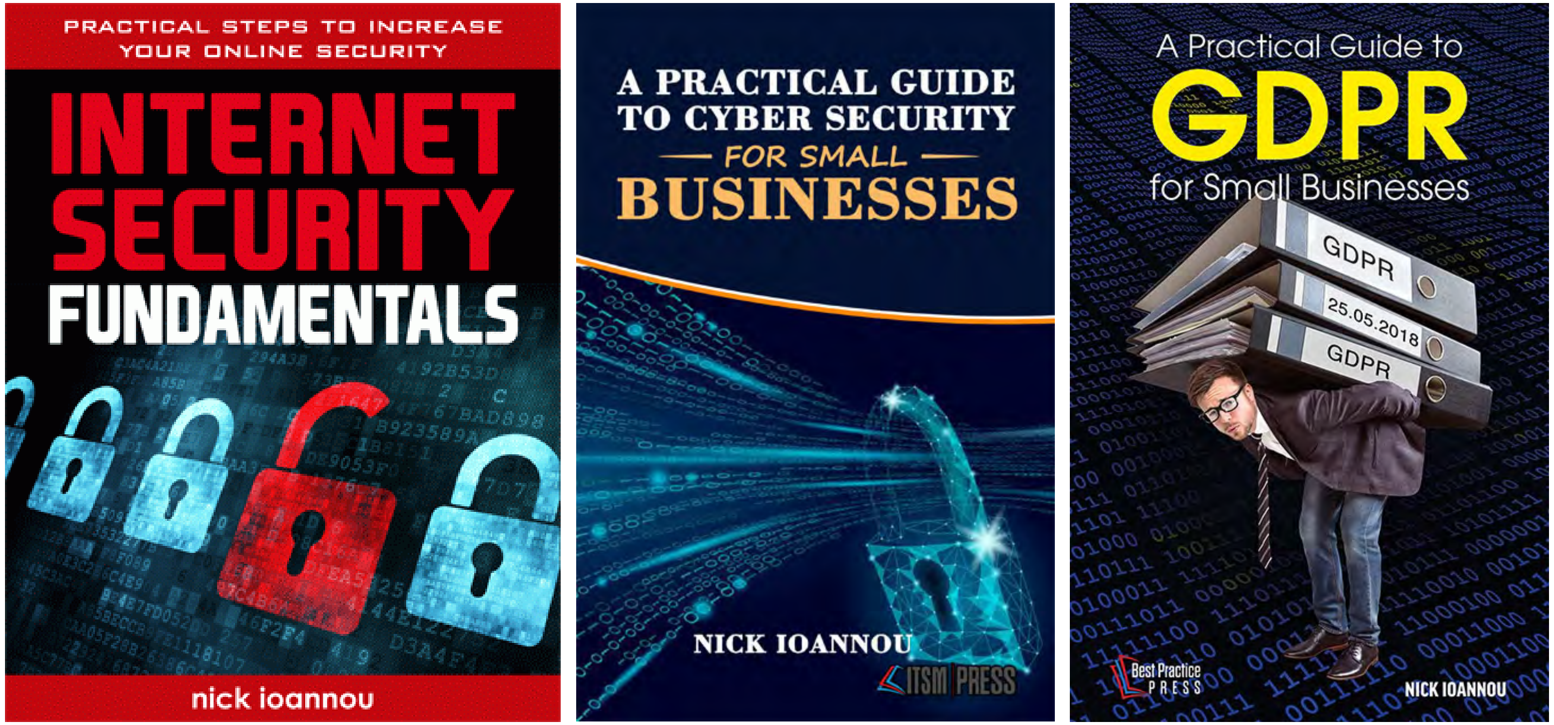
What can SMBs do to protect themselves?

BOOLEAN
LOGICAL

nick ioannou

Infosec Manager ○ Author ○ IT Blogger

My Amazon Author Page can be found at: www.amazon.com/author/nick-ioannou


PRACTICAL STEPS TO INCREASE YOUR ONLINE SECURITY
INTERNET SECURITY FUNDAMENTALS
nick ioannou
A PRACTICAL GUIDE TO CYBER SECURITY FOR SMALL BUSINESSES
NICK IOANNOU
ITSM PRESS
A Practical Guide to GDPR for Small Businesses
GDPR
25.05.2018
GDPR
Best Practice PRESS
NICK IOANNOU

- Author -

MANAGING CYBERSECURITY RISK
How Directors and Corporate Officers
MANAGING CYBERSECURITY RISK CASE STUDIES AND SOLUTIONS
THE ULTIMATE CYBERSECURITY GUIDE
CONQUER THE WEB
EDITED BY Jonathon Reuvid
MANAGING CYBERSECURITY RISK
Book 3
EDITED BY
JONATHAN REUVID
AXELOS
Beecher Madden

- Contributing Author -

BOOLEAN LOGICAL

RGP architects

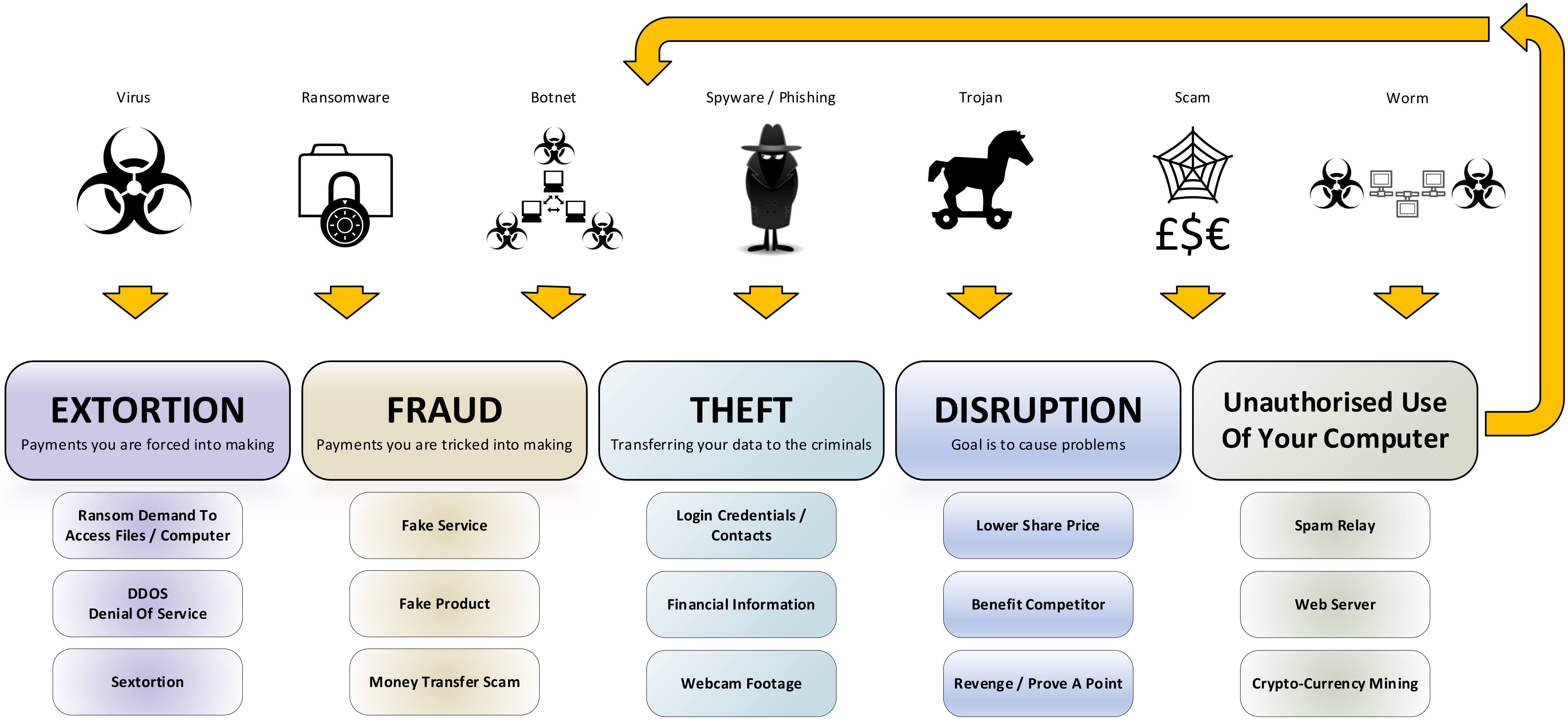
dlg architects

uio

BBC Worldwide

magmed

Who is nick ioannou?



Virus

Ransomware

Botnet

Spyware / Phishing

Trojan

Scam

Worm

EXTORTION
Payments you are forced into making

- Ransom Demand To Access Files / Computer
- DDOS Denial Of Service
- Sextortion

FRAUD
Payments you are tricked into making

- Fake Service
- Fake Product
- Money Transfer Scam

THEFT
Transferring your data to the criminals

- Login Credentials / Contacts
- Financial Information
- Webcam Footage

DISRUPTION
Goal is to cause problems

- Lower Share Price
- Benefit Competitor
- Revenge / Prove A Point

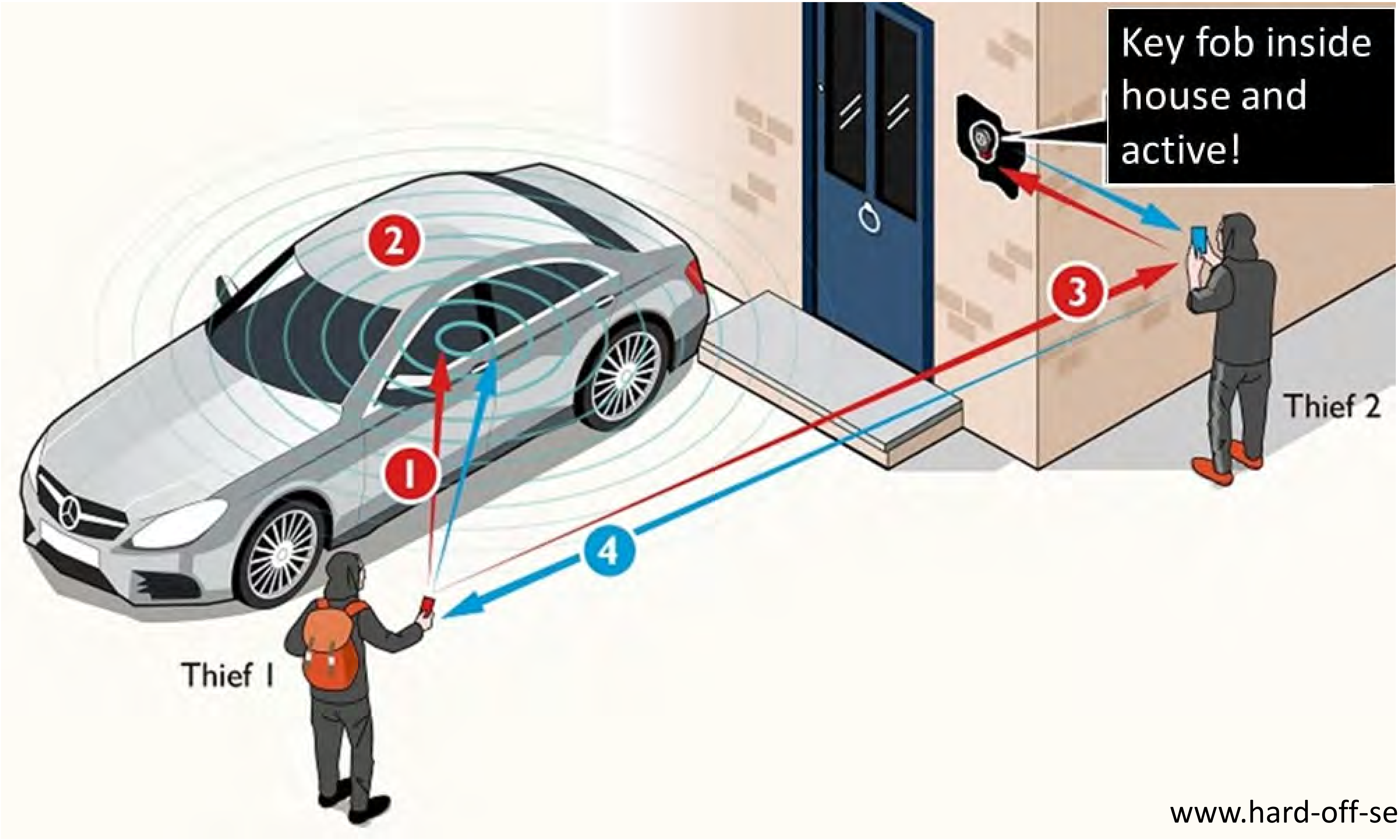
Unauthorised Use Of Your Computer

- Spam Relay
- Web Server
- Crypto-Currency Mining

Why Would Cyber Criminals Target an Organisation?

Advanced Cyber Threats

A quick explanation

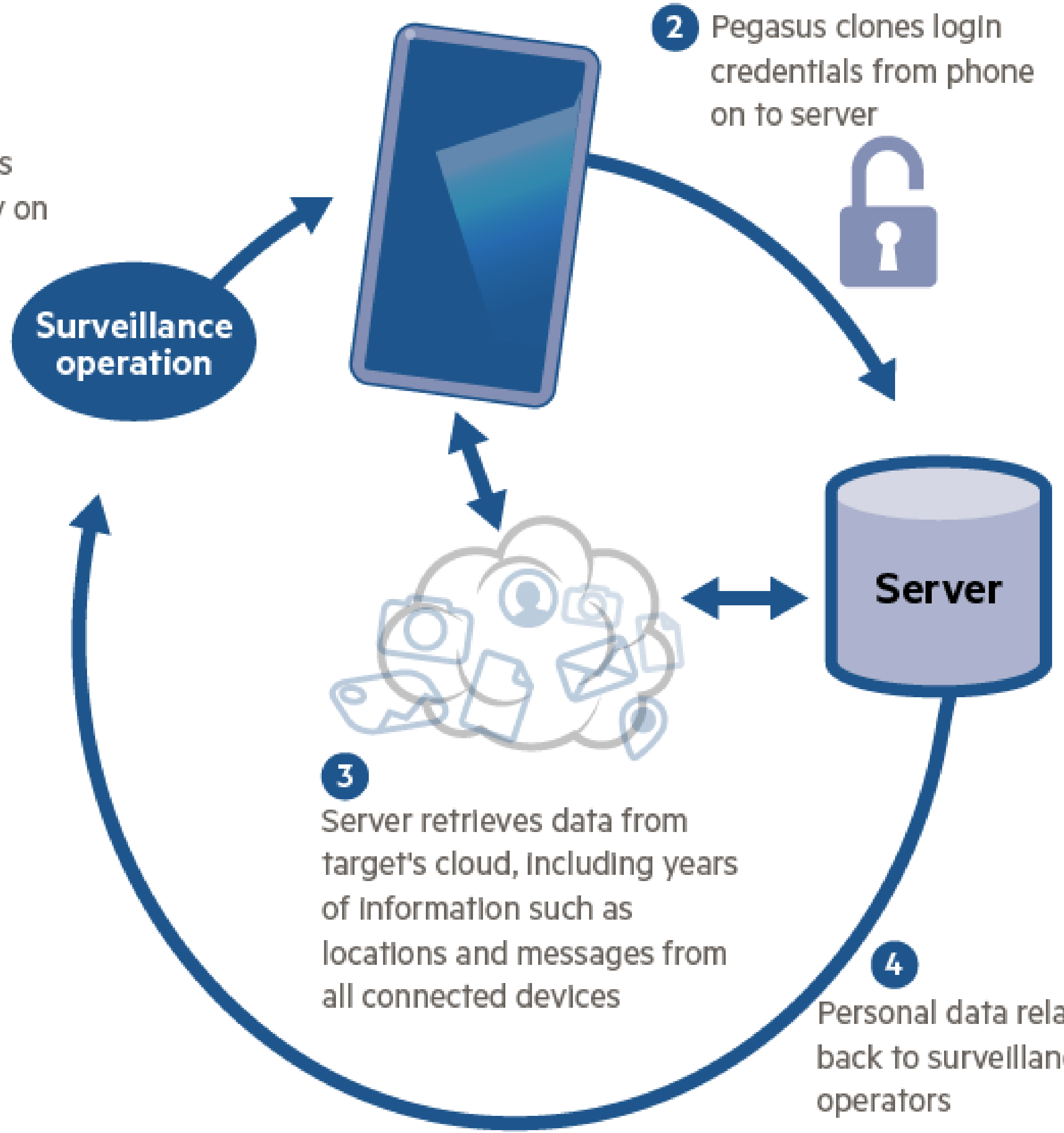


www.hard-off-security.com

What is an advanced threat?

What is an advanced cyber threat?

How NSO’s new capability is said to work



1 Installs Pegasus malware illicitly on target’s phone

2 Pegasus clones login credentials from phone on to server

3 Server retrieves data from target's cloud, including years of information such as locations and messages from all connected devices

4 Personal data relayed back to surveillance operators

Source: FT research

© *FT*

What is an advanced cyber threat?

40%

infection rate if clicked

NIST

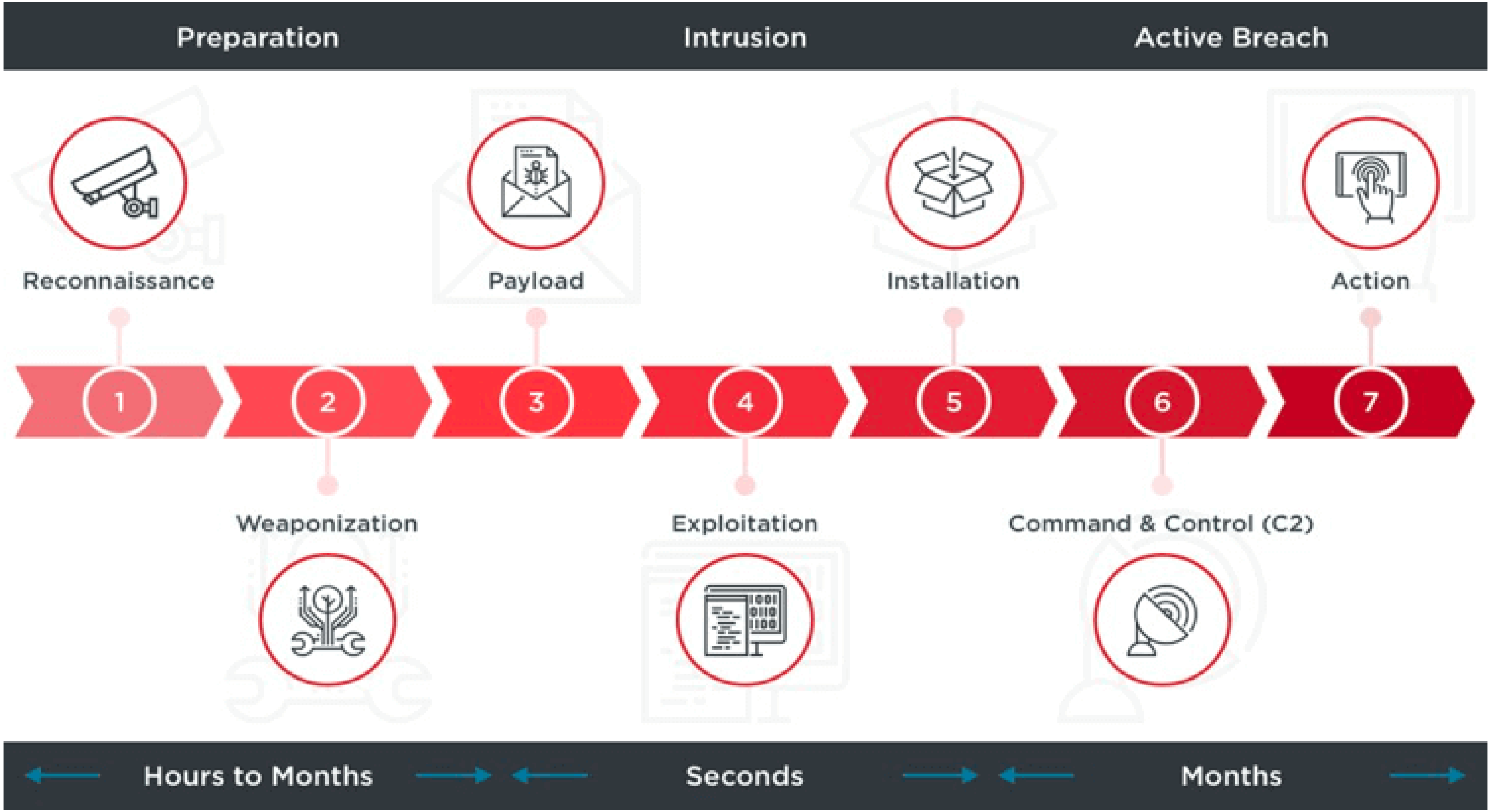
National Vulnerability Database – October 2021

110 known vulnerabilities - last 3 months

1637 known vulnerabilities - all time

AUTOMATED EXPLOIT KITS ARE SOLD AS A WEB SERVICE BY CRIMINALS TO OTHER CRIMINALS

184	16	1	9	67
Big Sur	Java™	Windows 10		
344	835	1,110	640	1,870



Any single part of the cyber kill chain can be advanced?

?

The What

Understanding the attack surface of your organisation

Understanding your attack surface

Understanding your all your attack surface

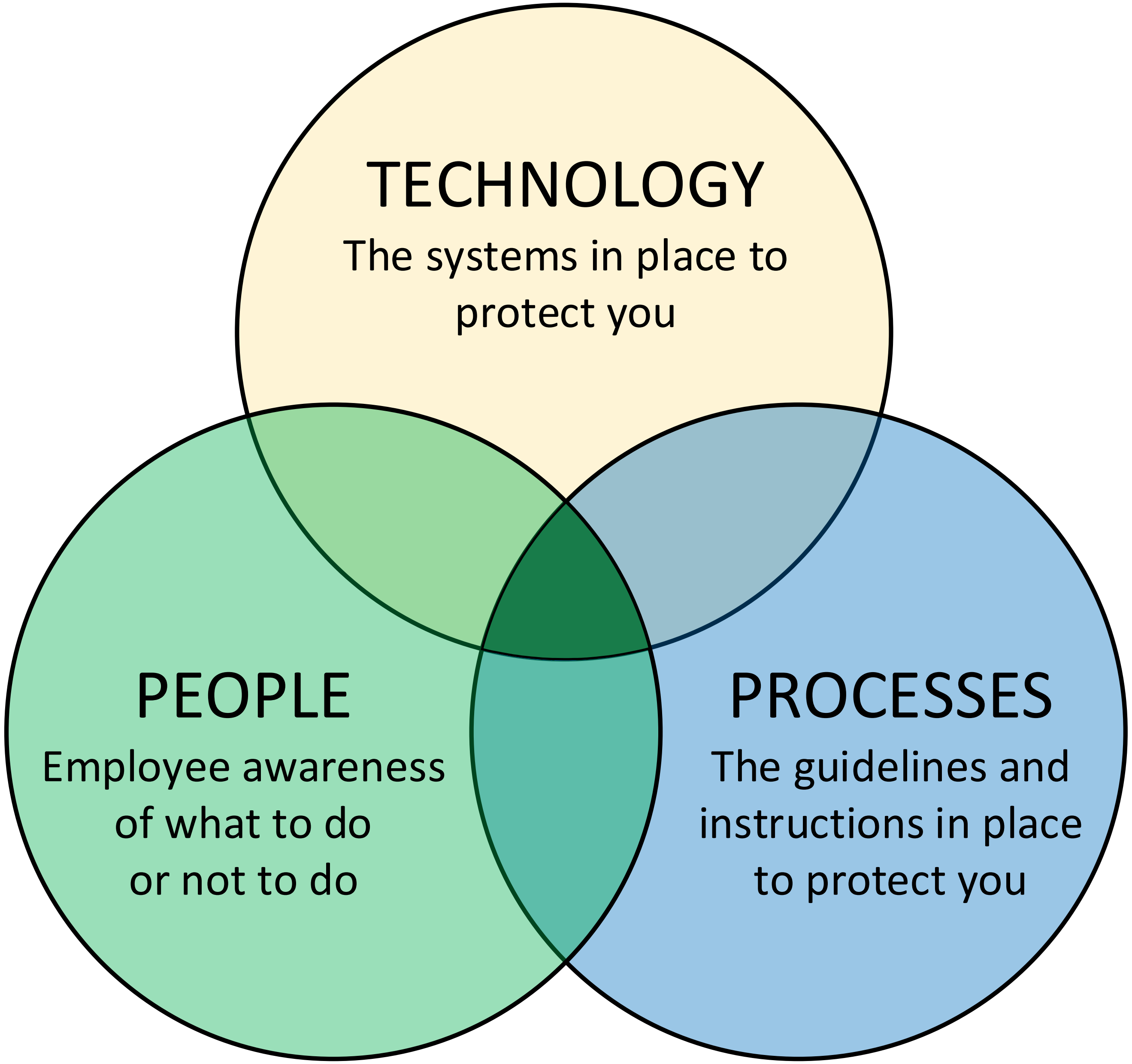
REALVNC
aws
Google Cloud Platform
Office 365
salesforce
Java™
CRASHPLAN For Small Business
vmware®
zoom
Windows
iCloud
Adobe
Google Workspace
Dropbox
EVERNOTE
Azure
box

Your software is also part of your attack surface

July 2009

October 2021

Legacy technology creep vs emerging technology



TECHNOLOGY
The systems in place to protect you

PEOPLE
Employee awareness of what to do or not to do

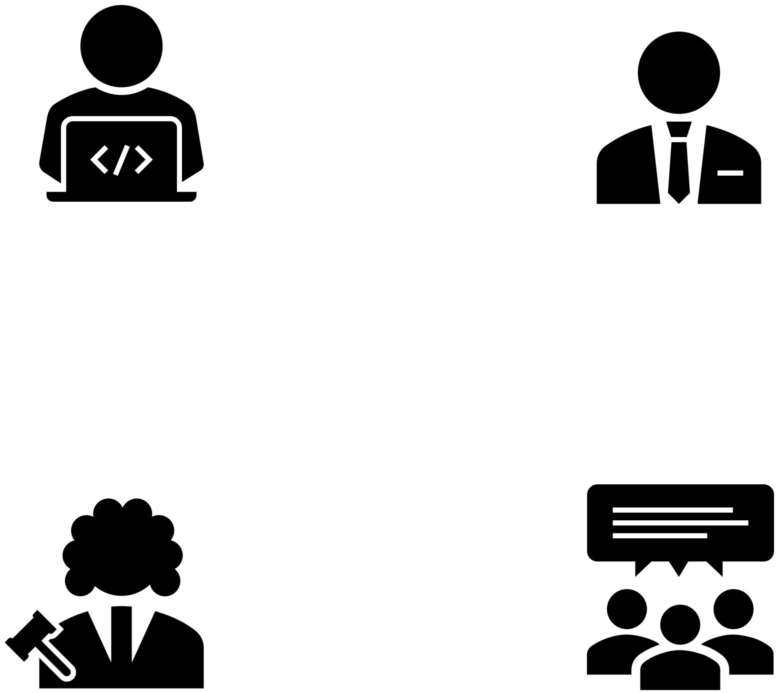
PROCESSES
The guidelines and instructions in place to protect you

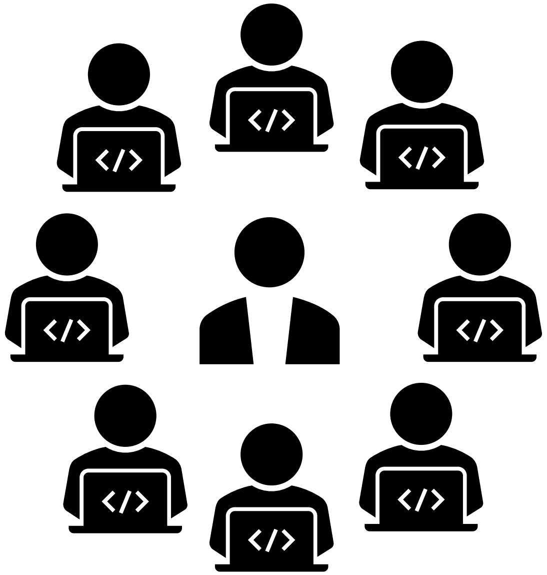
Let’s not forget the human element

The Where, Who & Why

Expanding the asset list information

Where assets are physically or virtually





Who is the accountable person or team responsible?

Training

Risk Management

Productivity Tool

Marketing

Business Analytics

Legal / Regulatory

Forensics

Communications

Management

Why is this asset in the organisation?

Reducing The Attack Surface

Removing may equal reducing, but reducing does not always equal removing

iPadOS

Windows 11

chromebook

chrome enterprise

Adobe Illustrator

Consider upgrades or alternative operating systems

GRANT ME the SERENITY to ACCEPT THAT MY PASSWORD WILL BE HACKED, THE COURAGE to FREQUENTLY CHANGE IT, AND the WISDOM to COME UP WITH A BETTER ONE.
12 - STEP VERIFICATION
klossner
copyright 2014 john klossner www.jklossner.com

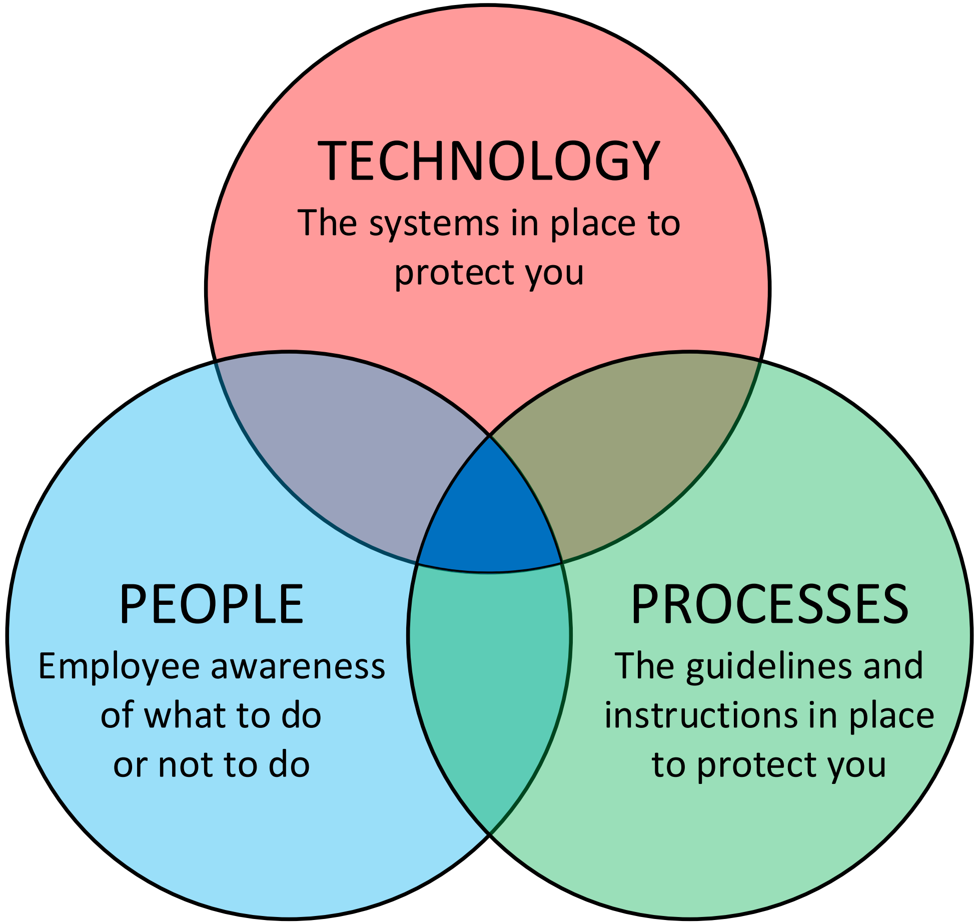
People need engaging cyber security awareness training

One of the first questions the ICO ask when a breach is reported is whether the staff member was trained in data protection

Explain the risks according to department

Demonstrate through real-world examples

Create a no-blame culture



TECHNOLOGY
The systems in place to protect you

PEOPLE
Employee awareness of what to do or not to do

PROCESSES
The guidelines and instructions in place to protect you

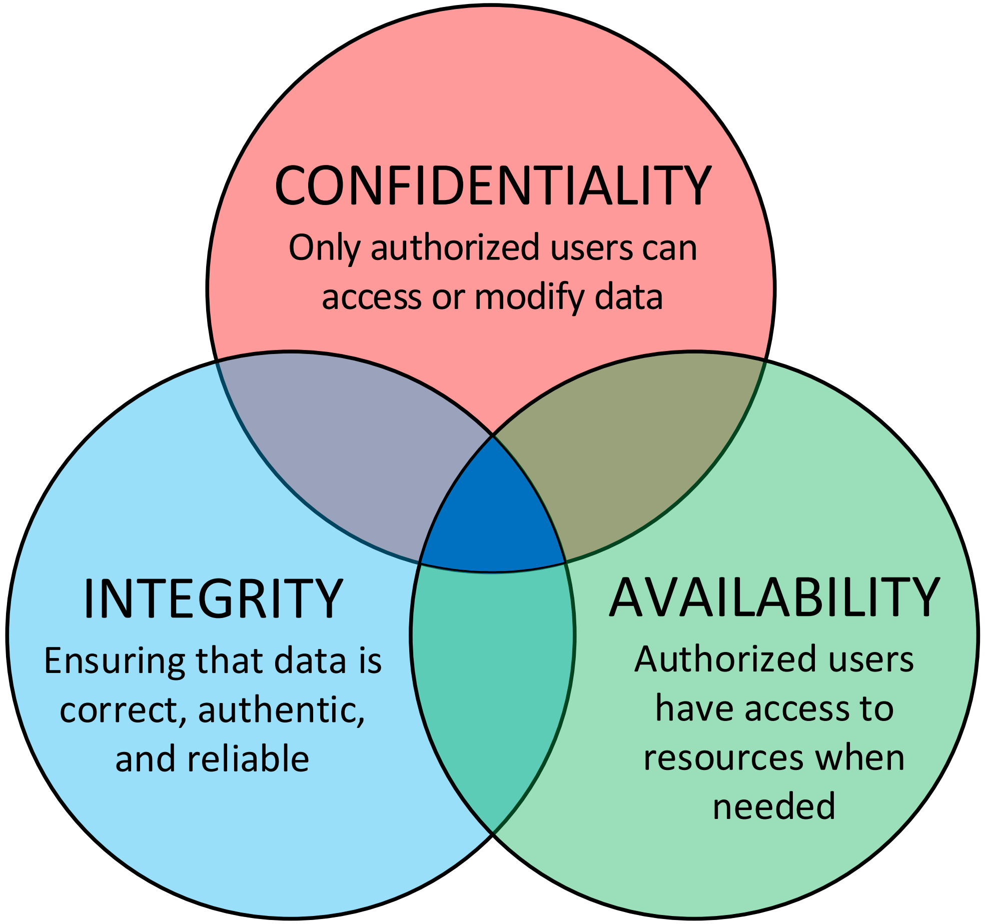
Raise awareness of social engineering attacks

A one size fits all approach does not work for security awareness training

Marketing
Data privacy risks

Engineering
Supply chain compromise, extortion & theft

Finance
Fraud



CONFIDENTIALITY
Only authorized users can access or modify data

INTEGRITY
Ensuring that data is correct, authentic, and reliable

AVAILABILITY
Authorized users have access to resources when needed

Explain the major risks by department

To PHISH or not to PHISH your own staff; that is the question?

PHISHME

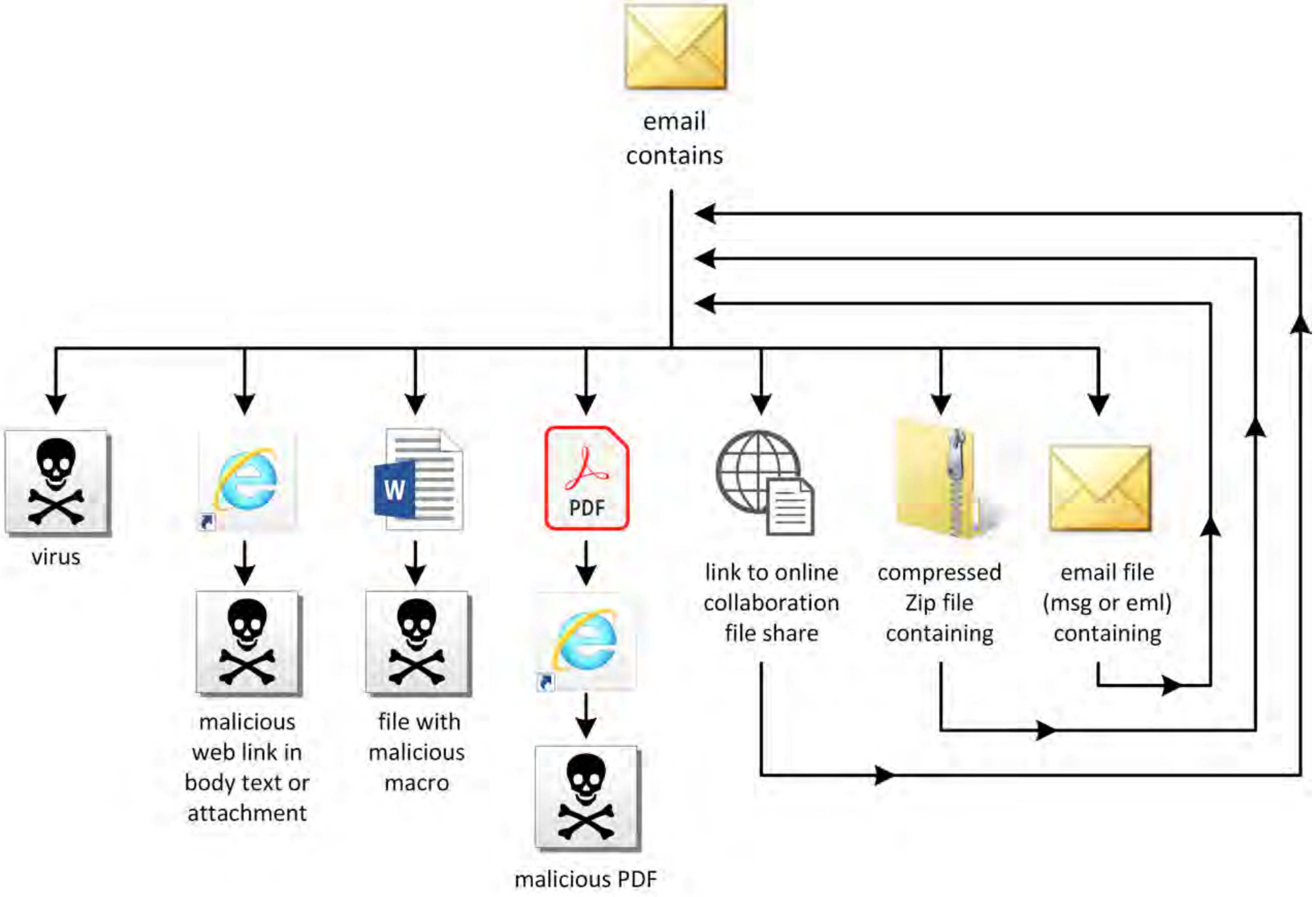
phishd

PHISHLABS

DUO

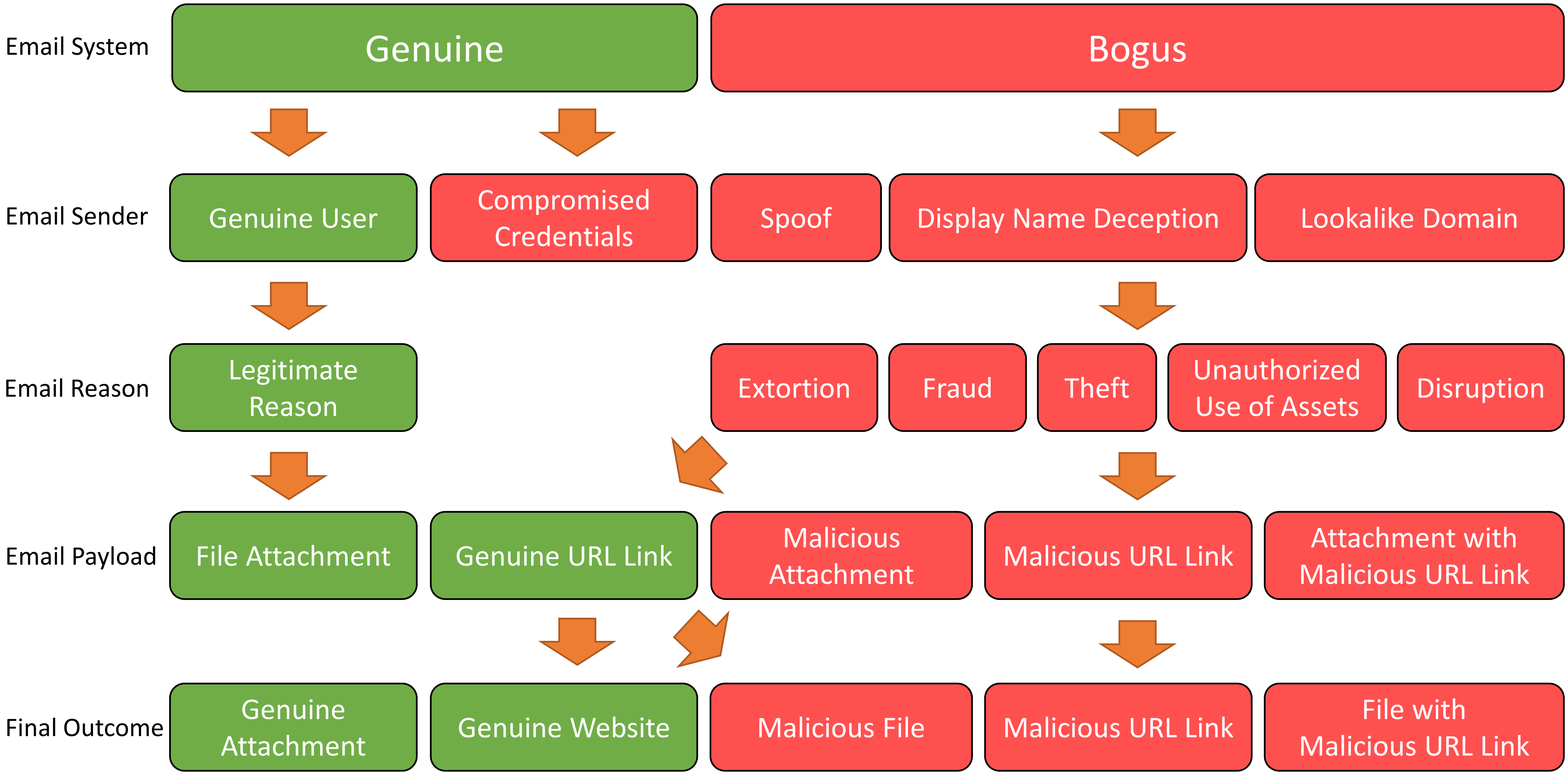
proofpoint

REDSCAN



Emails are still the main infection route

Types of email



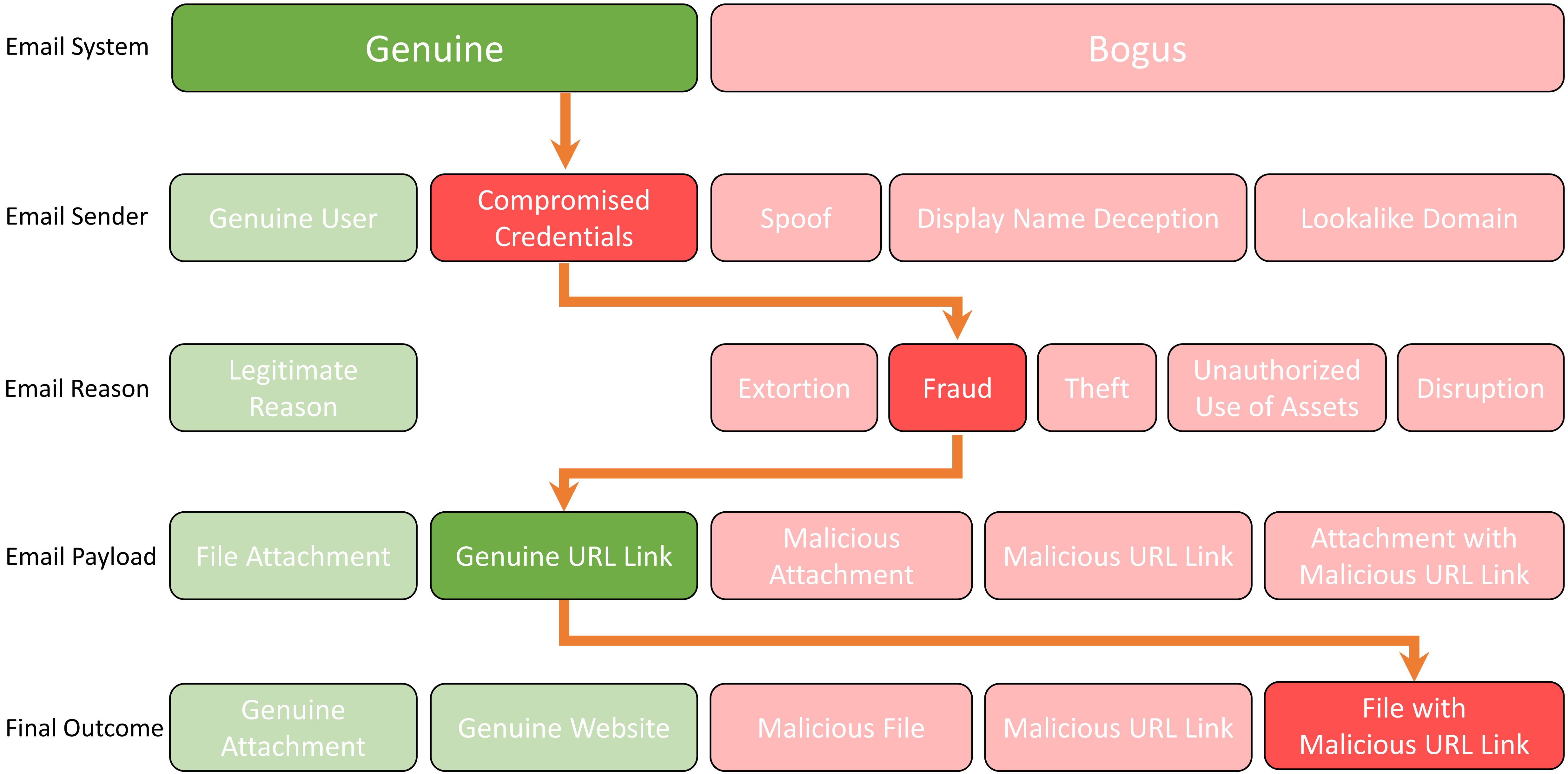
Email System: Genuine | Bogus

Email Sender: Genuine User | Compromised Credentials | Spoof | Display Name Deception | Lookalike Domain

Email Reason: Legitimate Reason | Extortion | Fraud | Theft | Unauthorized Use of Assets | Disruption

Email Payload: File Attachment | Genuine URL Link | Malicious Attachment | Malicious URL Link | Attachment with Malicious URL Link

Final Outcome: Genuine Attachment | Genuine Website | Malicious File | Malicious URL Link | File with Malicious URL Link



Email System: Genuine | Bogus

Email Sender: Genuine User | Compromised Credentials | Spoof | Display Name Deception | Lookalike Domain

Email Reason: Legitimate Reason | Extortion | Fraud | Theft | Unauthorized Use of Assets | Disruption

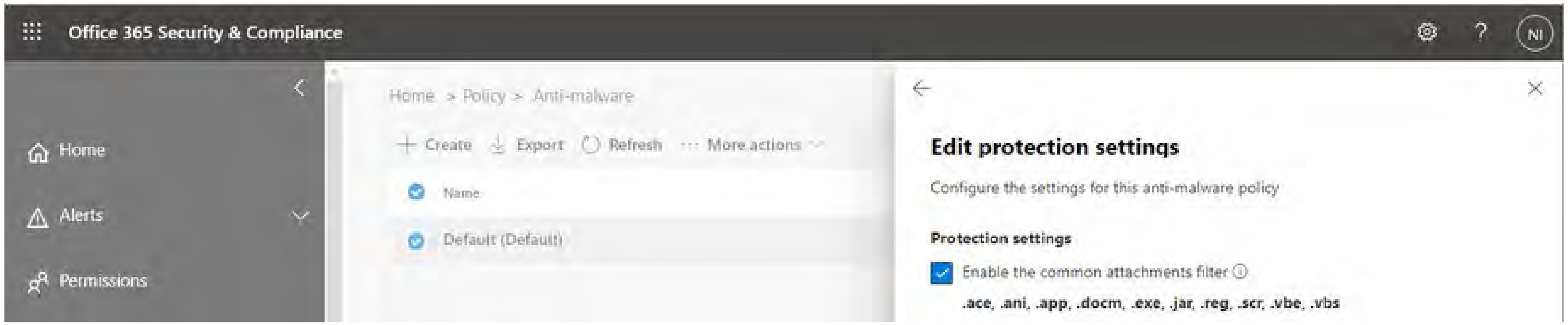
Email Payload: File Attachment | Genuine URL Link | Malicious Attachment | Malicious URL Link | Attachment with Malicious URL Link

Final Outcome: Genuine Attachment | Genuine Website | Malicious File | Malicious URL Link | File with Malicious URL Link

Types of email

Filter email & block executable file types

ace	ade	adp	ani	app	asp	bas	bat	cer	chm
cmd	com	cpl	crt	csh	der	dll	docm	dos	exe
fxp	gadget	hlp	hta	inf	ins	isp	its	jar	js
jse	ksh	lnk	mad	maf	mag	mam	maq	mar	mas
mau	mav	maw	mda	mdb	mde	mdt	mdw	mdz	msc
msh	msh1	msh1xml	msh2	msh2xml	mshxml	msi	msp	mst	obj
ops	os2	pcd	pif	plg	prf	prg	ps1	ps1xml	ps2
ps2xml	psc1	psc2	pst	rar	reg	scf	scr	sct	shb
shs	tmp	url	vb	vbe	vbs	vsmacros	vsw	vxd	w16
ws	wsc	wsf	wsh	xnk					


Office 365 Security & Compliance
NI
Home
Alerts
Permissions
Home > Policy > Anti-malware
+ Create
Export
Refresh
More actions
Name

Default (Default)

Edit protection settings

Configure the settings for this anti-malware policy

Protection settings

☑ Enable the common attachments filter

.ace, .ani, .app, .docm, .exe, .jar, .reg, .scr, .vbe, .vbs

You can find my free step-by-step instructions for Office 365 at: **www.booleanlogical.com/office-365-security** quad9

censornet.

OpenDNS

zscaler™

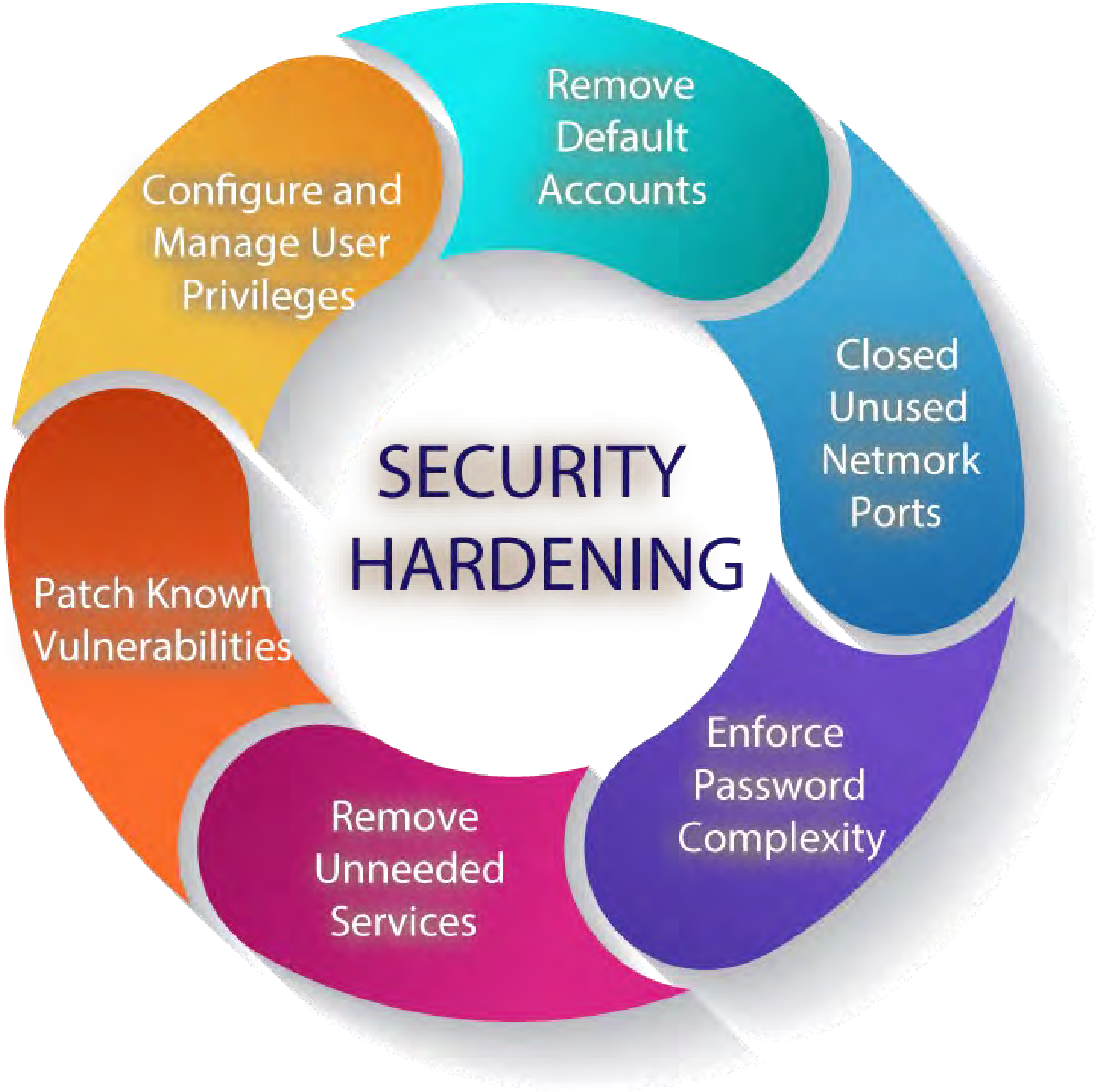
cisco Cisco Umbrella

MENLO SECURITY

Filter web traffic

Secure Configuration

Has everything been securely configured?



SECURITY HARDENING

Remove Default Accounts

Closed Unused Netmork Ports

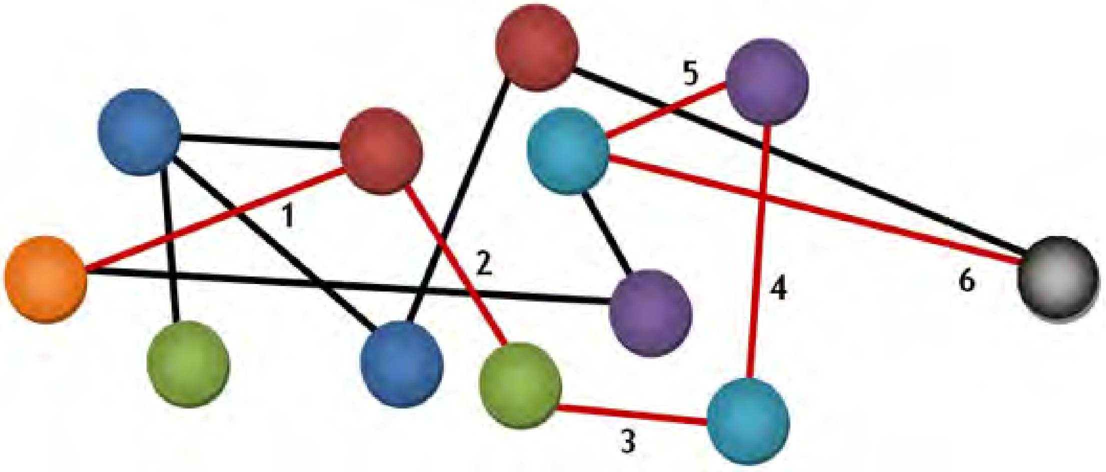
Enforce Password Complexity

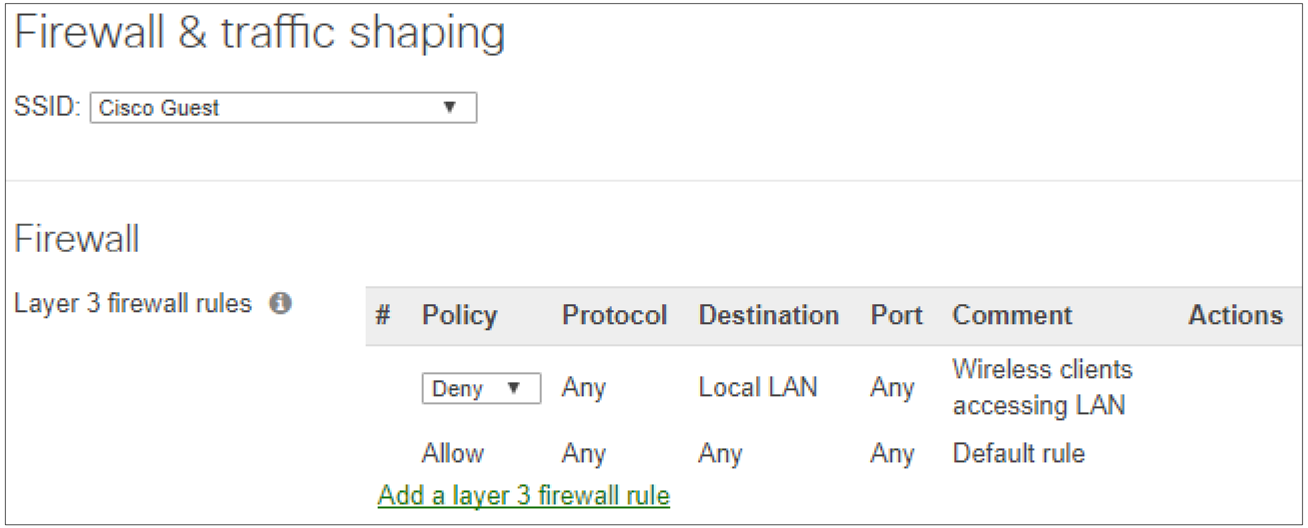
Remove Unneeded Services

Patch Known Vulnerabilities

Configure and Manage User Privileges

Is everything securely configured?





Firewall & traffic shaping

SSID: Cisco Guest ▼

Firewall

Layer 3 firewall rules ℹ

#	Policy	Protocol	Destination	Port	Comment	Actions
	Deny ▼	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

Add a layer 3 firewall rule

Does six degrees of separation apply to all your systems?

Access Control

Reducing user identity related risks

IAM / Single Sign-On & Multi-Factor Authentication

SSO
Single Sign On

2 step verification logins

Ping Identity

onelogin

dashlane

LastPass

okta

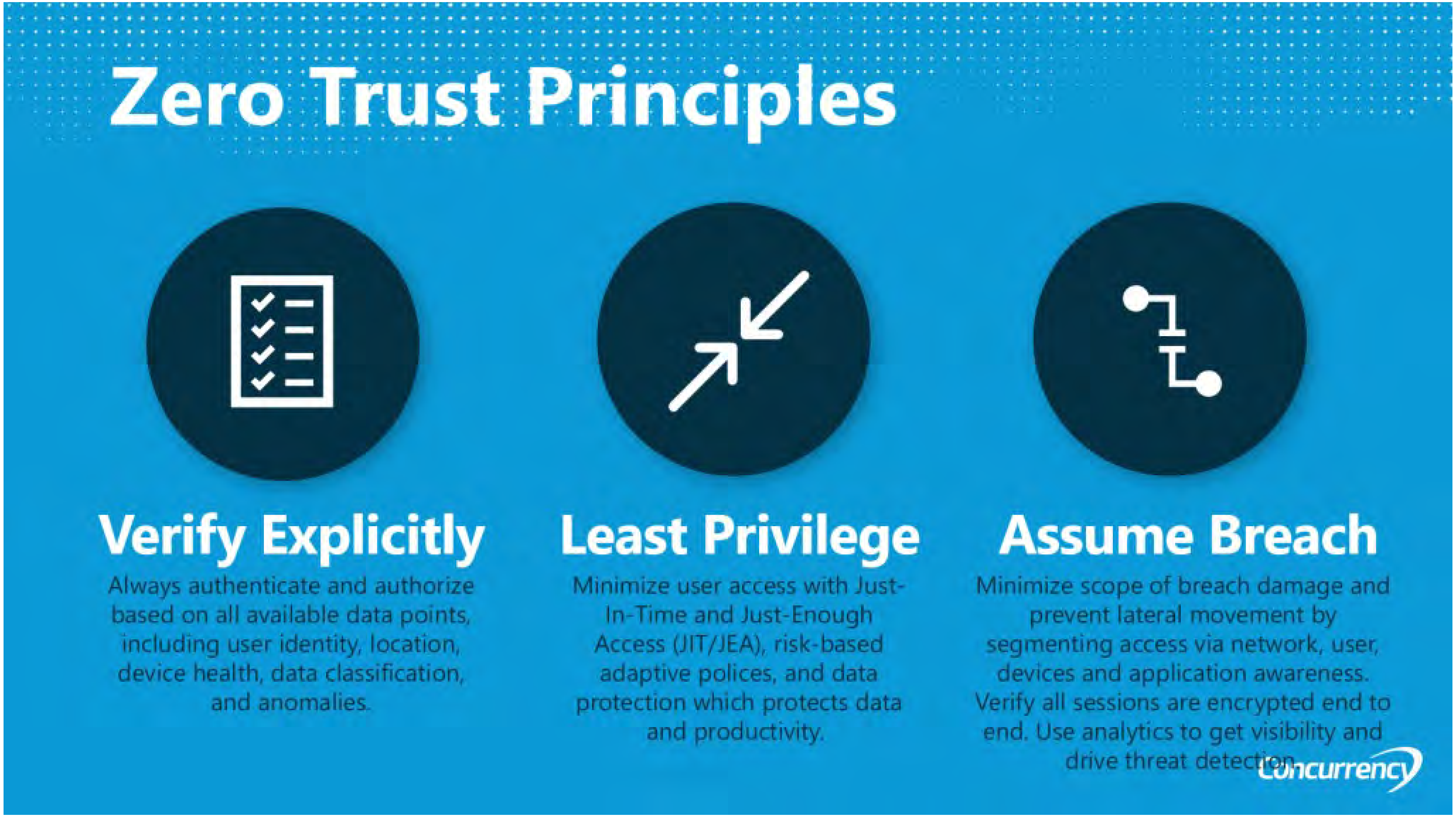
KEEPER

bitwarden

SECUREAUTH

my1login™
Connecting People, Apps and Devices

SecurEnvoy
A Shearwater Group plc Company



Zero Trust Principles

Verify Explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, data classification, and anomalies.

Least Privilege

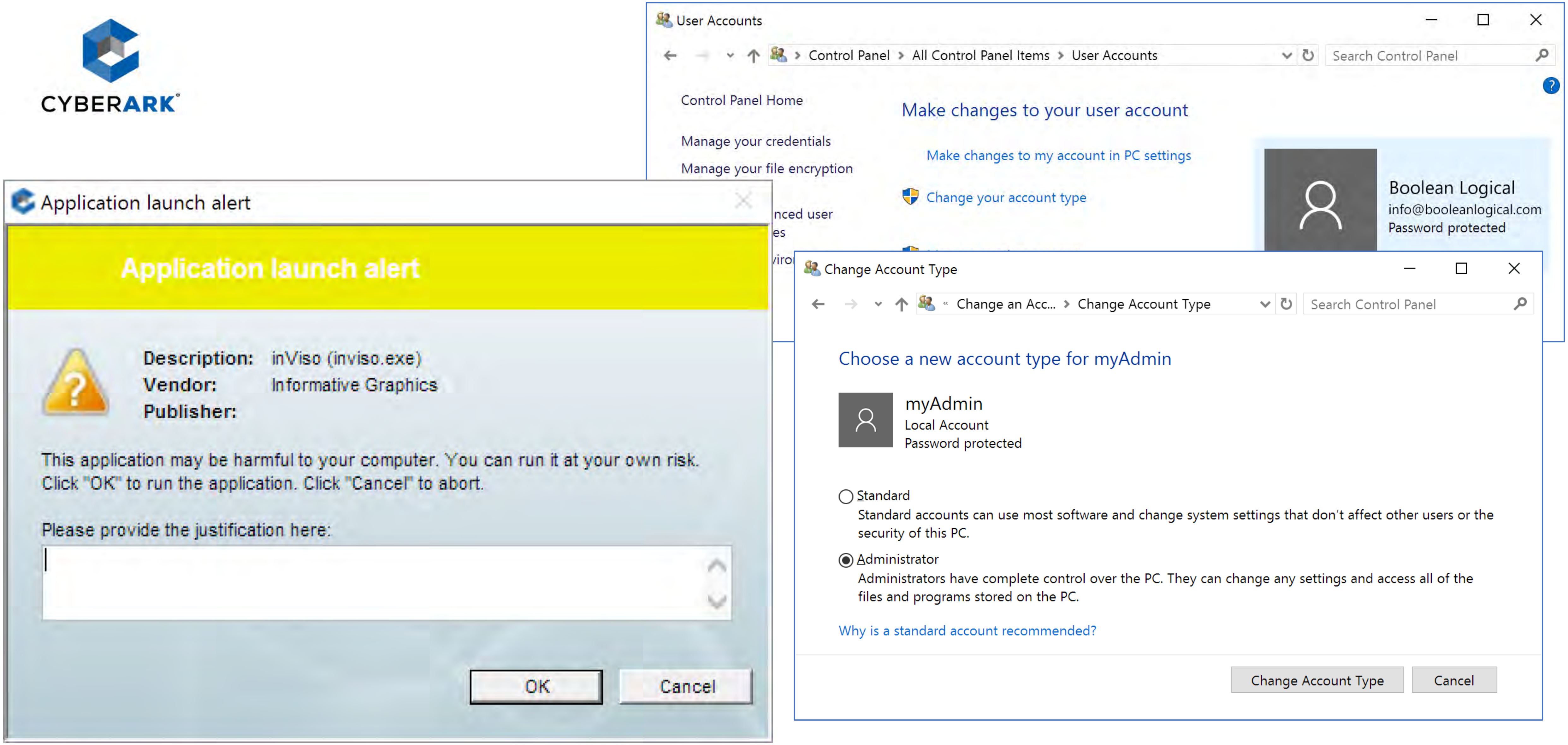
Minimize user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive polices, and data protection which protects data and productivity.

Assume Breach

Minimize scope of breach damage and prevent lateral movement by segmenting access via network, user, devices and application awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility and drive threat detection.

Concurrency

Zero-trust security model & context-aware access



Make changes to your user account

Make changes to my account in PC settings

Change your account type

Boolean Logical
info@booleanlogical.com
Password protected

Application launch alert

Description: inViso (inviso.exe)
Vendor: Informative Graphics
Publisher:

This application may be harmful to your computer. You can run it at your own risk. Click "OK" to run the application. Click "Cancel" to abort.

Please provide the justification here:

Choose a new account type for myAdmin

myAdmin
Local Account
Password protected

○ Standard
Standard accounts can use most software and change system settings that don't affect other users or the security of this PC.

● Administrator
Administrators have complete control over the PC. They can change any settings and access all of the files and programs stored on the PC.

Why is a standard account recommended?

Admin rights equals a security risk

Visibility

Can you see network traffic and device activity?

Attivo NETWORKS®

ThreatConnect™

SECURONIX

LogRhythm™

DARKTRACE

ALERT LOGIC®
SIEMLESS THREAT MANAGEMENT

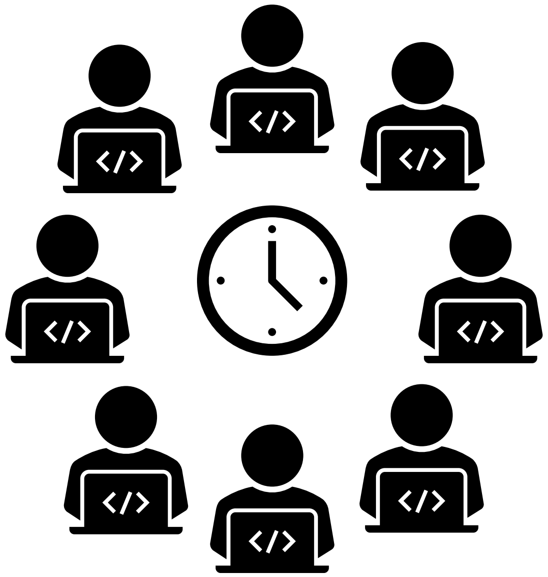
SWIMLANE

seceon

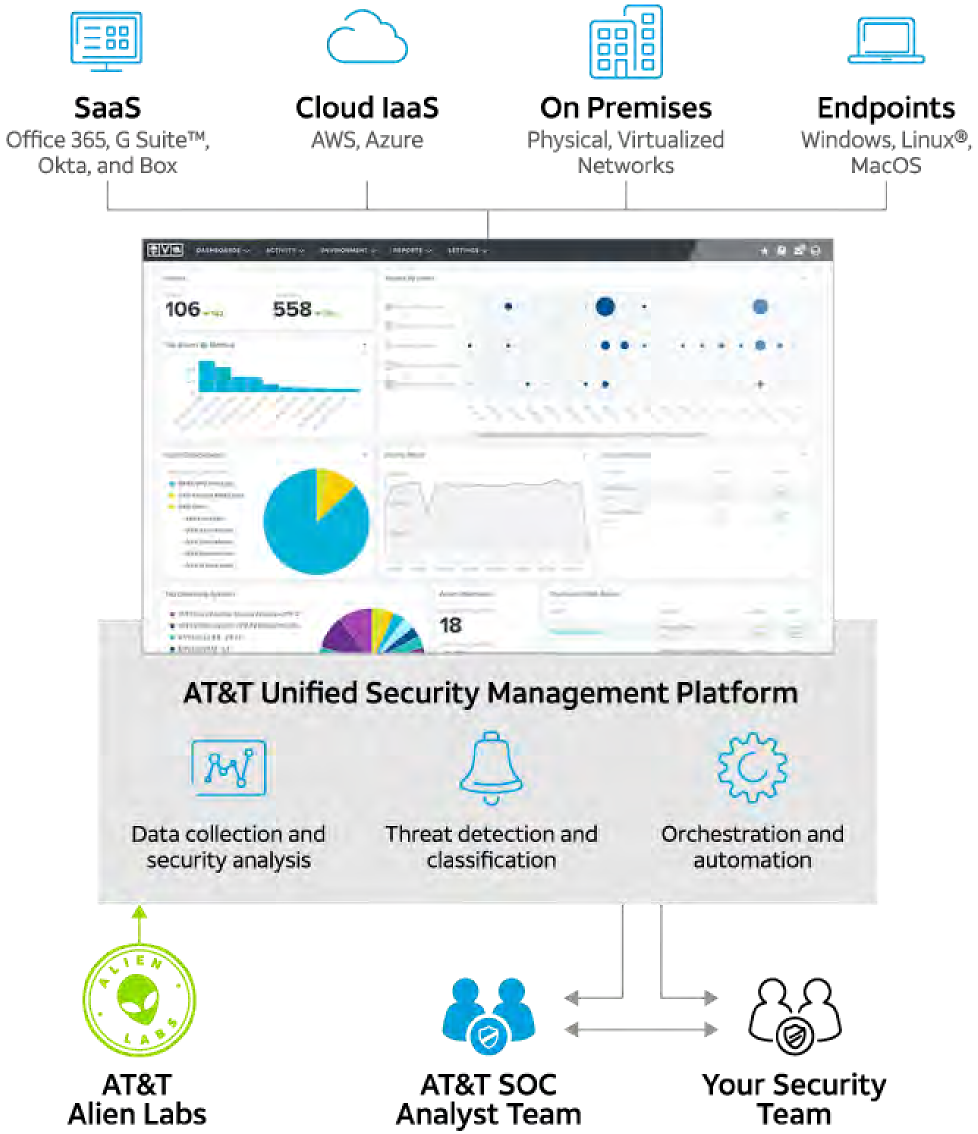
Do you need a SIEM (security info and event management)?

Do you need a SOC (security operations centre)?

24/7 monitoring is expensive



ARCTIC WOLF



SaaS
Office 365, G Suite™, Okta, and Box

Cloud IaaS
AWS, Azure

On Premises
Physical, Virtualized Networks

Endpoints
Windows, Linux®, MacOS

AT&T Unified Security Management Platform

Data collection and security analysis

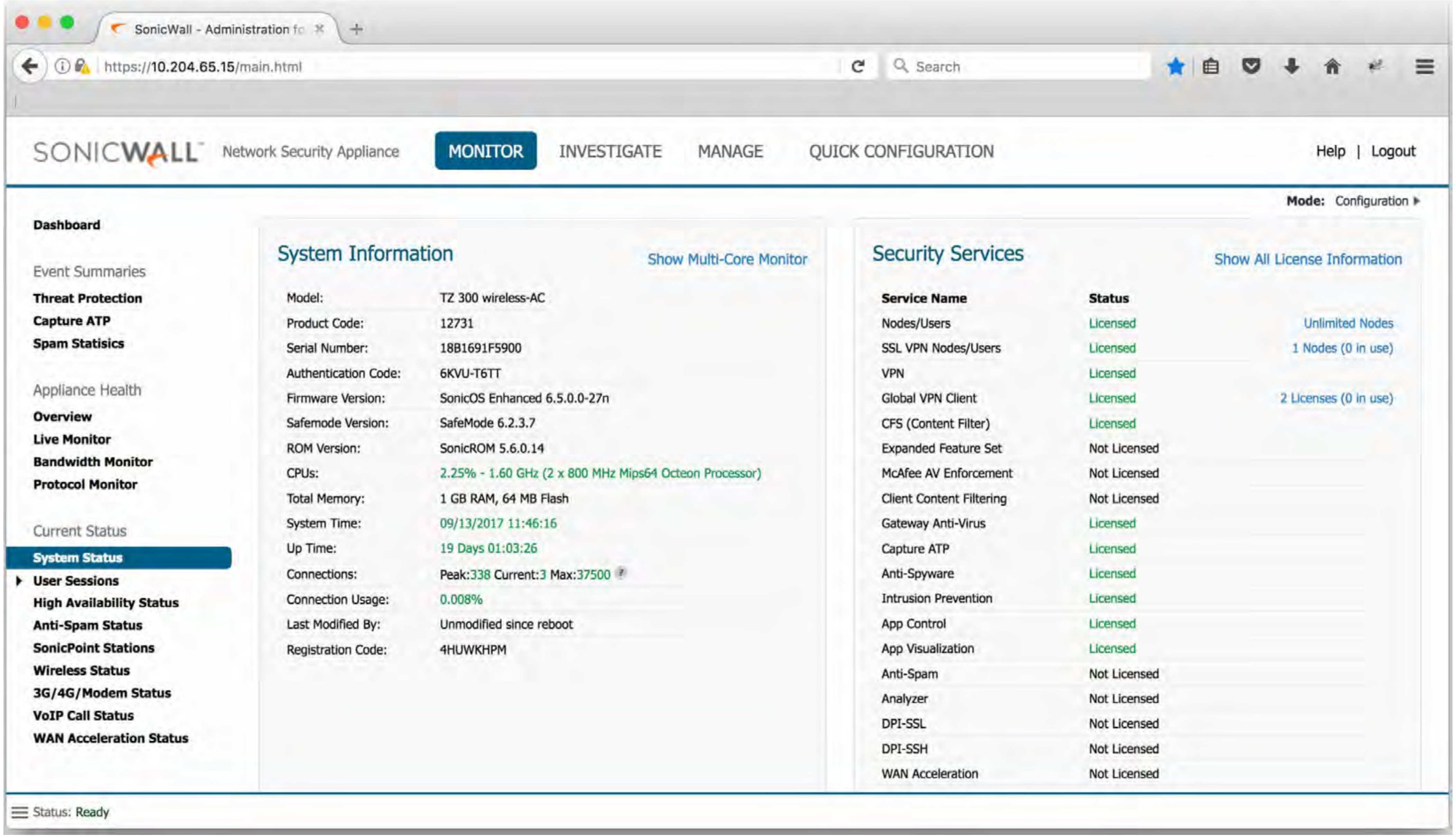
Threat detection and classification

Orchestration and automation

AT&T Alien Labs

AT&T SOC Analyst Team

Your Security Team



System Information

Show Multi-Core Monitor

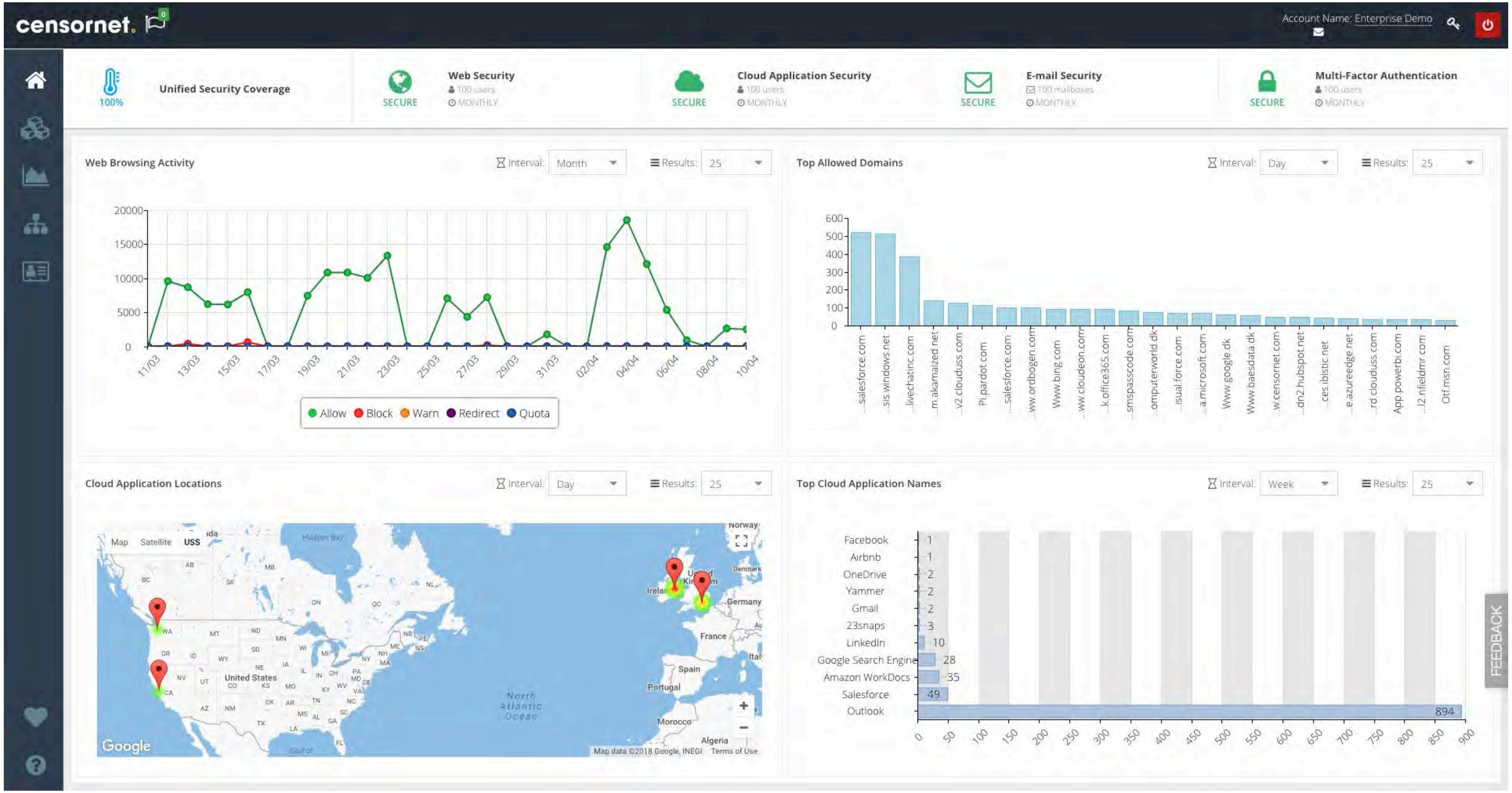
Model:	TZ 300 wireless-AC
Product Code:	12731
Serial Number:	18B1691F5900
Authentication Code:	6KVU-T6TT
Firmware Version:	SonicOS Enhanced 6.5.0.0-27n
Safemode Version:	SafeMode 6.2.3.7
ROM Version:	SonicROM 5.6.0.14
CPUs:	2.25% - 1.60 GHz (2 x 800 MHz Mips64 Octeon Processor)
Total Memory:	1 GB RAM, 64 MB Flash
System Time:	09/13/2017 11:46:16
Up Time:	19 Days 01:03:26
Connections:	Peak:338 Current:3 Max:37500
Connection Usage:	0.008%
Last Modified By:	Unmodified since reboot
Registration Code:	4HUWKHPM

Security Services

Show All License Information

Service Name	Status	
Nodes/Users	Licensed	Unlimited Nodes
SSL VPN Nodes/Users	Licensed	1 Nodes (0 in use)
VPN	Licensed	
Global VPN Client	Licensed	2 Licenses (0 in use)
CFS (Content Filter)	Licensed	
Expanded Feature Set	Not Licensed	
McAfee AV Enforcement	Not Licensed	
Client Content Filtering	Not Licensed	
Gateway Anti-Virus	Licensed	
Capture ATP	Licensed	
Anti-Spyware	Licensed	
Intrusion Prevention	Licensed	
App Control	Licensed	
App Visualization	Licensed	
Anti-Spam	Not Licensed	
Analyzer	Not Licensed	
DPI-SSL	Not Licensed	
DPI-SSH	Not Licensed	
WAN Acceleration	Not Licensed	

Unified threat management (UTM) firewalls



censornet.

Account Name: Enterprise Demo

100%	Unified Security Coverage
SECURE	Web Security 100 users MONTHLY
SECURE	Cloud Application Security 100 users MONTHLY
SECURE	E-mail Security 100 mailboxes MONTHLY
SECURE	Multi-Factor Authentication 100 users MONTHLY

Web Browsing Activity — Interval: Month — Results: 25

Top Allowed Domains — Interval: Day — Results: 25

Cloud Application Locations — Interval: Day — Results: 25

Top Cloud Application Names — Interval: Week — Results: 25

censornet. zscaler™ MENLO SECURITY cisco Cisco Umbrella

Web traffic filters also have extensive reporting

Mobile device management (MDM)

SOTI

kandji

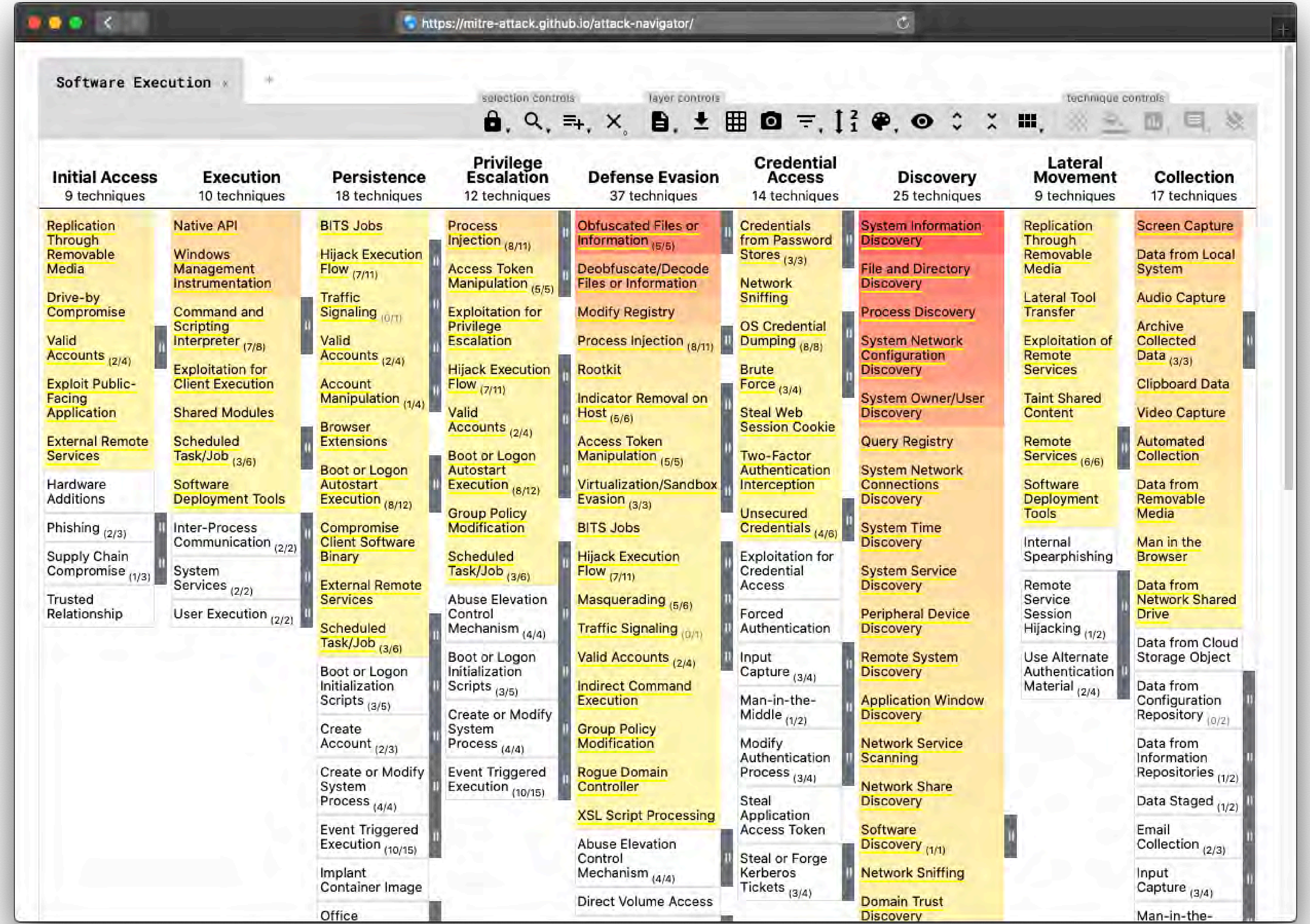
ManageEngine
Mobile Device Manager Plus

★★★
25 DEVICES
Free

Fully-functional, perfect for small businesses.

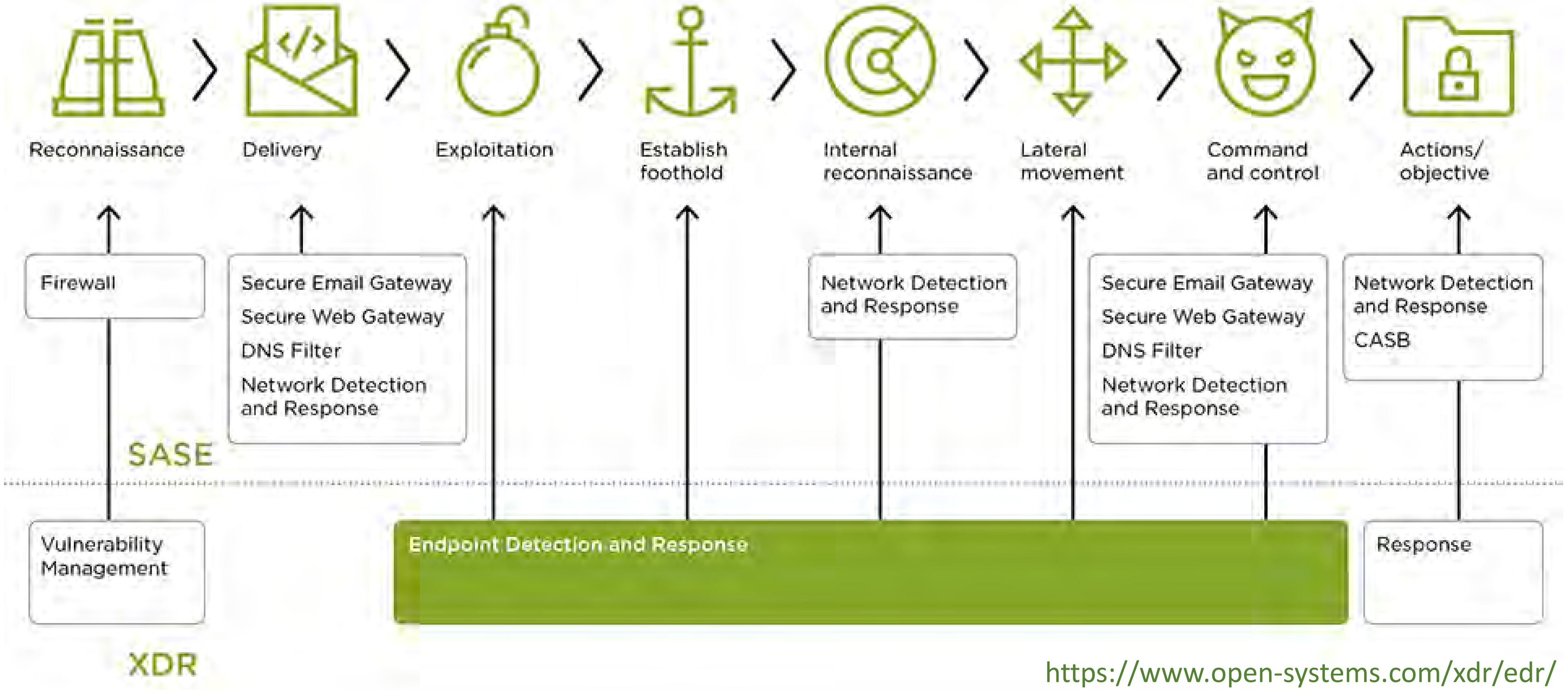
Forensics and Remediation

Root cause analysis and in-depth remediation



Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 12 techniques	Defense Evasion 37 techniques	Credential Access 14 techniques	Discovery 25 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Replication Through Removable Media	Native API	BITS Jobs	Process Injection (8/11)	Obfuscated Files or Information (5/5)	Credentials from Password Stores (3/3)	System Information Discovery	Replication Through Removable Media	Screen Capture
Drive-by Compromise	Windows Management Instrumentation	Hijack Execution Flow (7/11)	Access Token Manipulation (5/5)	Deobfuscate/Decode Files or Information	Network Sniffing	File and Directory Discovery	Lateral Tool Transfer	Data from Local System
Valid Accounts (2/4)	Command and Scripting Interpreter (7/8)	Traffic Signaling (0/1)	Exploitation for Privilege Escalation	Modify Registry	OS Credential Dumping (8/8)	Process Discovery	Exploitation of Remote Services	Audio Capture
Exploit Public-Facing Application	Exploitation for Client Execution	Valid Accounts (2/4)	Hijack Execution Flow (7/11)	Process Injection (8/11)	Brute Force (3/4)	System Network Configuration Discovery	Taint Shared Content	Archive Collected Data (3/3)
External Remote Services	Shared Modules	Account Manipulation (1/4)	Valid Accounts (2/4)	Rootkit	Steal Web Session Cookie	System Owner/User Discovery	Remote Services (6/6)	Clipboard Data
Hardware Additions	Scheduled Task/Job (3/6)	Browser Extensions	Boot or Logon Autostart Execution (8/12)	Indicator Removal on Host (5/6)	Two-Factor Authentication Interception	Query Registry	Software Deployment Tools	Video Capture
Phishing (2/3)	Software Deployment Tools	Boot or Logon Autostart Execution (8/12)	Group Policy Modification	Access Token Manipulation (5/5)	Unsecured Credentials (4/6)	System Network Connections Discovery	Internal Spearphishing	Automated Collection
Supply Chain Compromise (1/3)	Inter-Process Communication (2/2)	Compromise Client Software Binary	Scheduled Task/Job (3/6)	Virtualization/Sandbox Evasion (3/3)	Exploitation for Credential Access	System Time Discovery	Remote Service Session Hijacking (1/2)	Data from Removable Media
Trusted Relationship	System Services (2/2)	External Remote Services	Abuse Elevation Control Mechanism (4/4)	BITS Jobs	Forced Authentication	System Service Discovery	Use Alternate Authentication Material (2/4)	Man in the Browser
	User Execution (2/2)	Scheduled Task/Job (3/6)	Boot or Logon Initialization Scripts (3/5)	Hijack Execution Flow (7/11)	Input Capture (3/4)	Peripheral Device Discovery		Data from Network Shared Drive
		Boot or Logon Initialization Scripts (3/5)	Create or Modify System Process (4/4)	Masquerading (5/6)	Man-in-the-Middle (1/2)	Remote System Discovery		Data from Cloud Storage Object
		Create Account (2/3)	Event Triggered Execution (10/15)	Traffic Signaling (0/1)	Modify Authentication Process (3/4)	Application Window Discovery		Data from Configuration Repository (0/2)
		Create or Modify System Process (4/4)		Valid Accounts (2/4)	Steal Application Access Token	Network Service Scanning		Data from Information Repositories (1/2)
		Event Triggered Execution (10/15)		Indirect Command Execution	Steal or Forge Kerberos Tickets (3/4)	Network Share Discovery		Data Staged (1/2)
		Implant Container Image		Group Policy Modification		Software Discovery (1/1)		Email Collection (2/3)
		Office		Rogue Domain Controller		Network Sniffing		Input Capture (3/4)
				XSL Script Processing		Domain Trust Discovery		Man-in-the-
				Abuse Elevation Control Mechanism (4/4)				
				Direct Volume Access				

Mitre att&ck® matrix

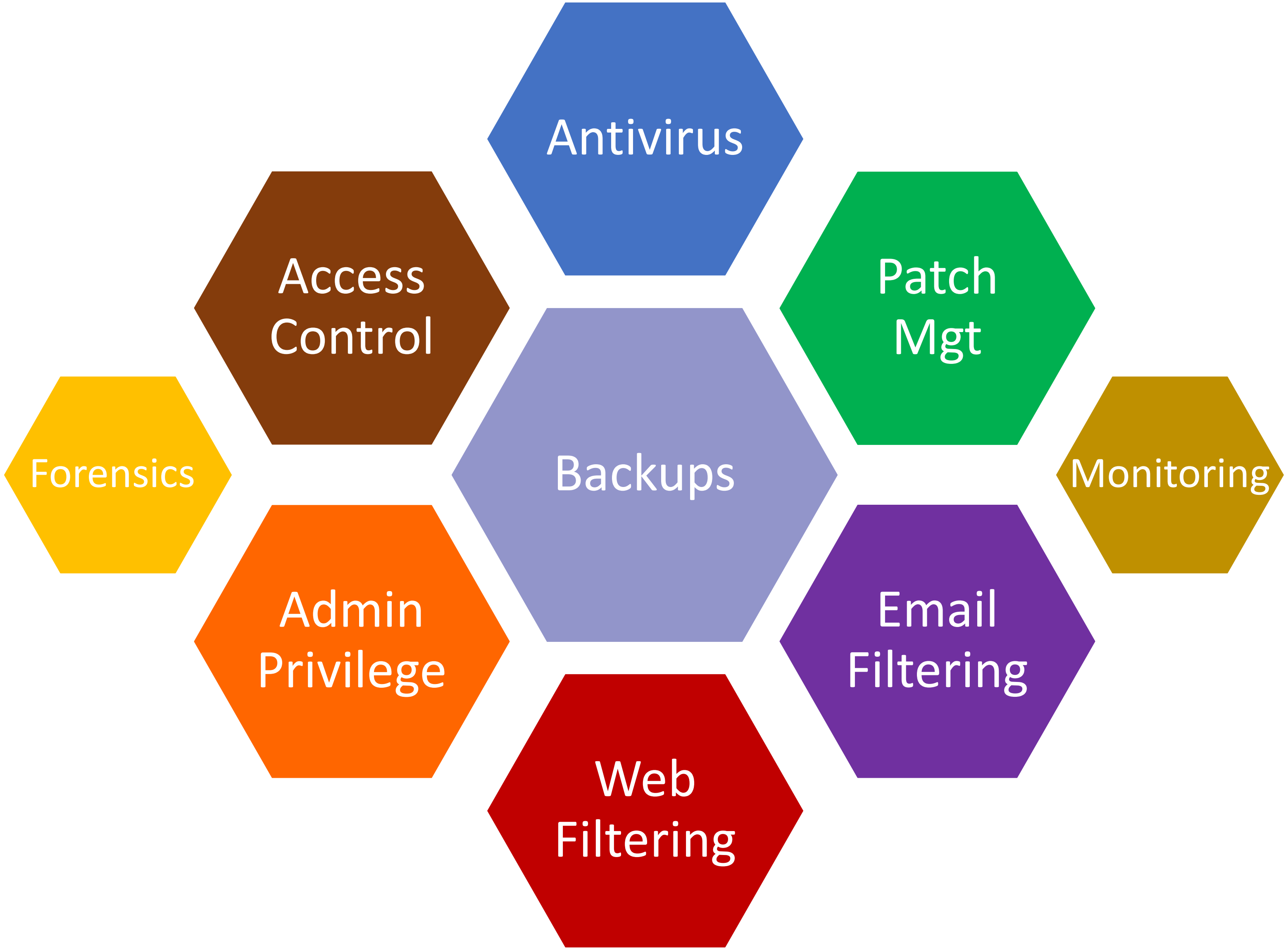


https://www.open-systems.com/xdr/edr/

SentinelOne cybereason HEIMDAL SECURITY SOPHOS FIREEYE

Endpoint detection and response (EDR)

Conclusion



Antivirus

Access Control

Patch Mgt

Forensics

Backups

Monitoring

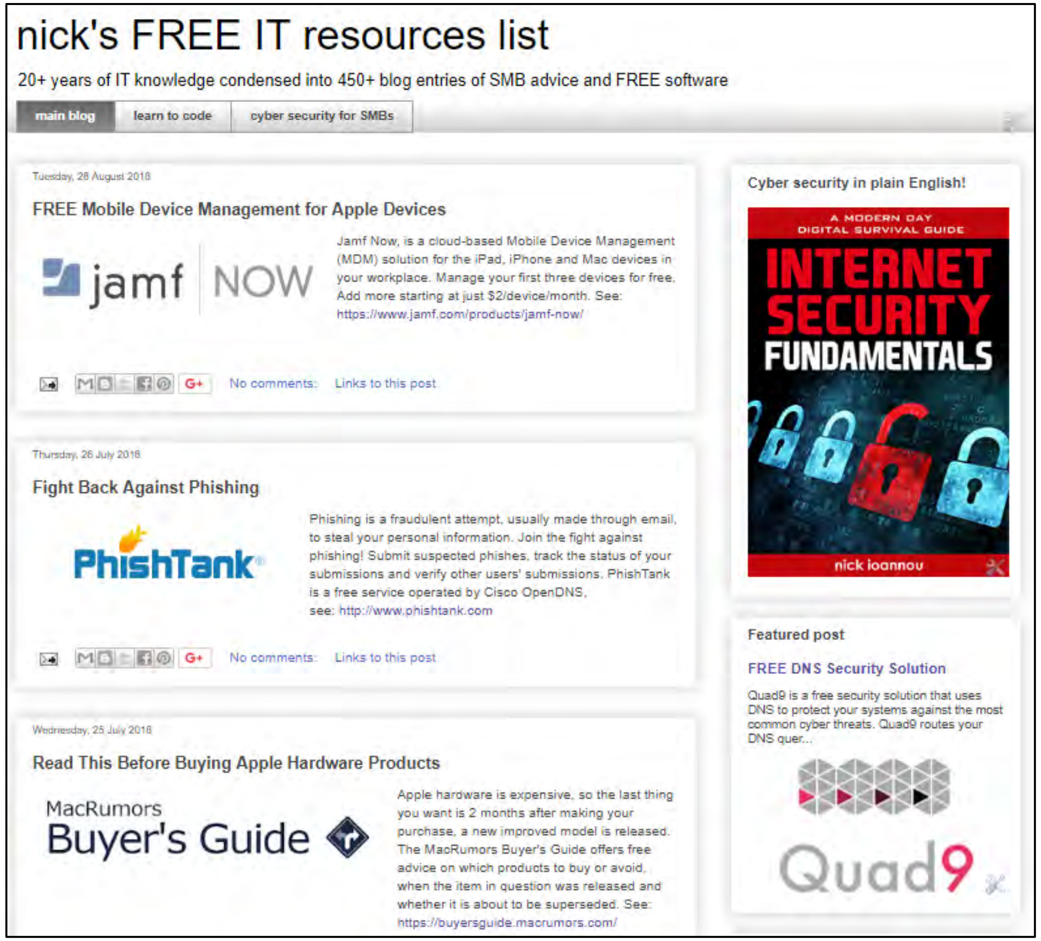
Admin Privilege

Email Filtering

Web Filtering

9 areas for true cover

There is no secret ingredient


jamf NOW
PhishTank
MacRumors Buyer's Guide
A MODERN DAY DIGITAL SURVIVAL GUIDE
INTERNET SECURITY FUNDAMENTALS
nick ioannou
Quad9

nick's FREE IT resources list

20+ years of IT knowledge condensed into 450+ blog entries of SMB advice and FREE software

main blog | learn to code | cyber security for SMBs

Tuesday, 28 August 2018

FREE Mobile Device Management for Apple Devices

Jamf Now, is a cloud-based Mobile Device Management (MDM) solution for the iPad, iPhone and Mac devices in your workplace. Manage your first three devices for free. Add more starting at just $2/device/month. See: https://www.jamf.com/products/jamf-now/

No comments: Links to this post

Thursday, 26 July 2018

Fight Back Against Phishing

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. Join the fight against phishing! Submit suspected phishes, track the status of your submissions and verify other users' submissions. PhishTank is a free service operated by Cisco OpenDNS. see: http://www.phishtank.com

No comments: Links to this post

Wednesday, 25 July 2018

Read This Before Buying Apple Hardware Products

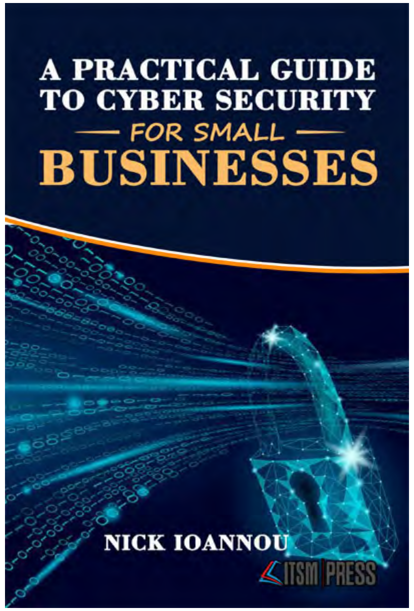
Apple hardware is expensive, so the last thing you want is 2 months after making your purchase, a new improved model is released. The MacRumors Buyer's Guide offers free advice on which products to buy or avoid, when the item in question was released and whether it is about to be superseded. See: https://buyersguide.macrumors.com/

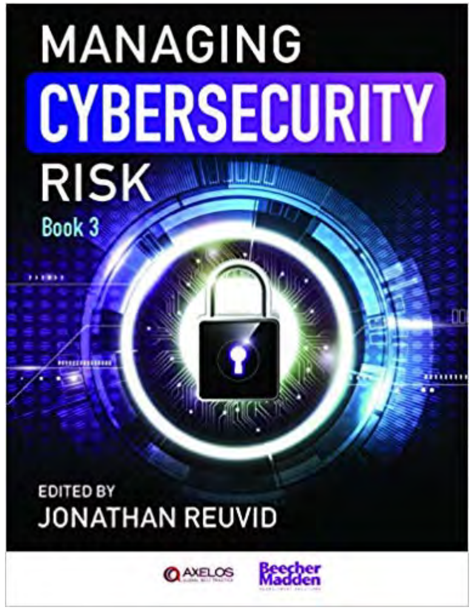
Cyber security in plain English!

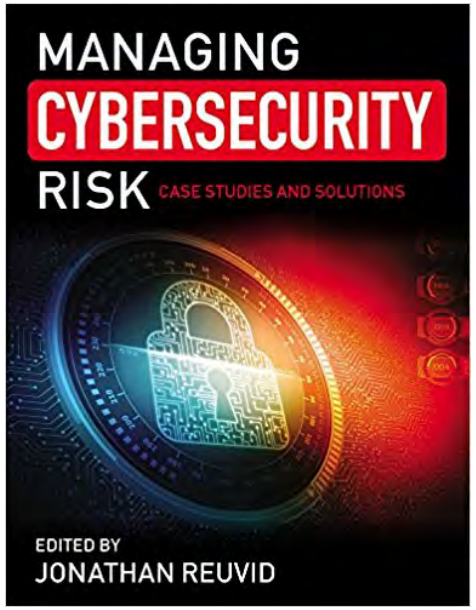
Featured post

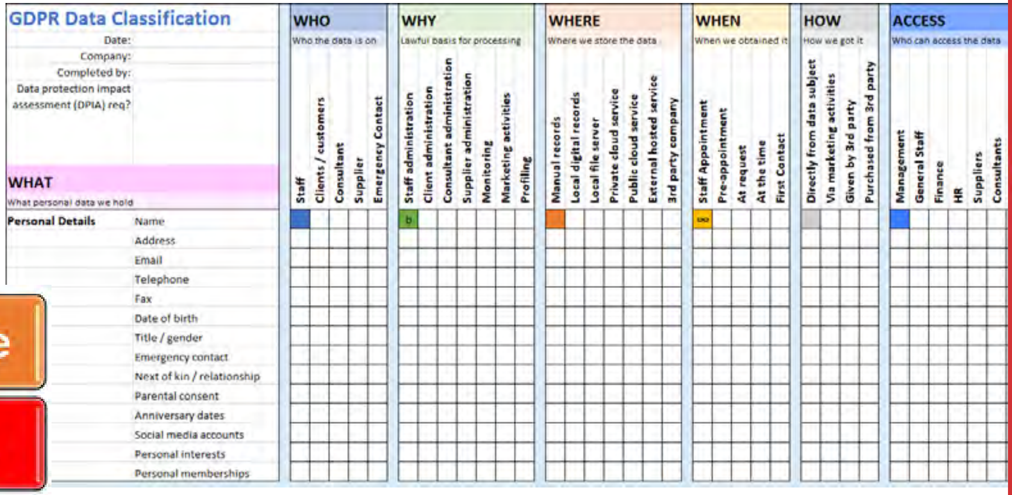
FREE DNS Security Solution

Quad9 is a free security solution that uses DNS to protect your systems against the most common cyber threats. Quad9 routes your DNS quer...









GDPR Data Classification

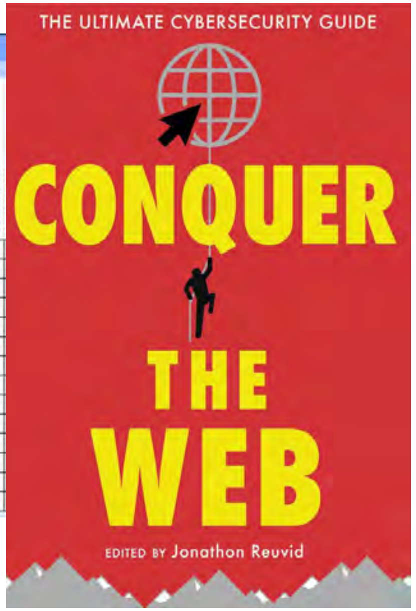
Date:

Company:

Completed by:

Data protection impact assessment (DPIA) req?

WHAT		WHO					WHY							WHERE							WHEN					HOW				ACCESS					
What personal data we hold		Who the data is on					Lawful basis for processing							Where we store the data							When we obtained it					How we got it				Who can access the data					
		Staff	Clients / customers	Consultant	Supplier	Emergency Contact	Staff administration	Client administration	Consultant administration	Supplier administration	Monitoring	Marketing activities	Profiling	Manual records	Local digital records	Local file server	Private cloud service	Public cloud service	External hosted service	3rd party company	Staff Appointment	Pre-appointment	At request	At the time	First Contact	Directly from data subject	Via marketing activities	Given by 3rd party	Purchased from 3rd party	Management	General Staff	Finance	HR	Suppliers	Consultants
Personal Details	Name	🟦					b							🟧							🟨					▨				🟦					
	Address																																		
	Email																																		
	Telephone																																		
	Fax																																		
	Date of birth																																		
	Title / gender																																		
	Emergency contact																																		
	Next of kin / relationship																																		
	Parental consent																																		
	Anniversary dates																																		
	Social media accounts																																		
	Personal interests																																		
	Personal memberships																																		



What | Who | Why | Where

When | How | Access | Risk

For more security resources and advice see:

www.booleanlogical.com