

Running with Bulls

Cyber-crime threat landscape through the eyes of an ethical hacker

Charl Van der Walt
Chief Ethical Hacker, SecureData

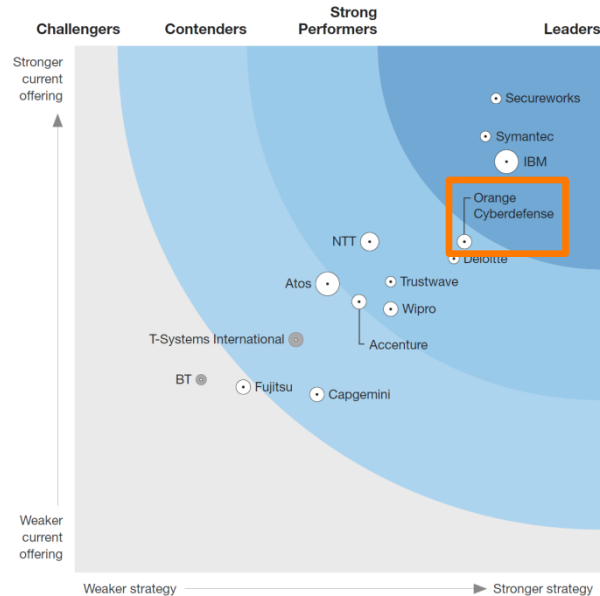
Thomas Gourgeon
Head of International
Business Development



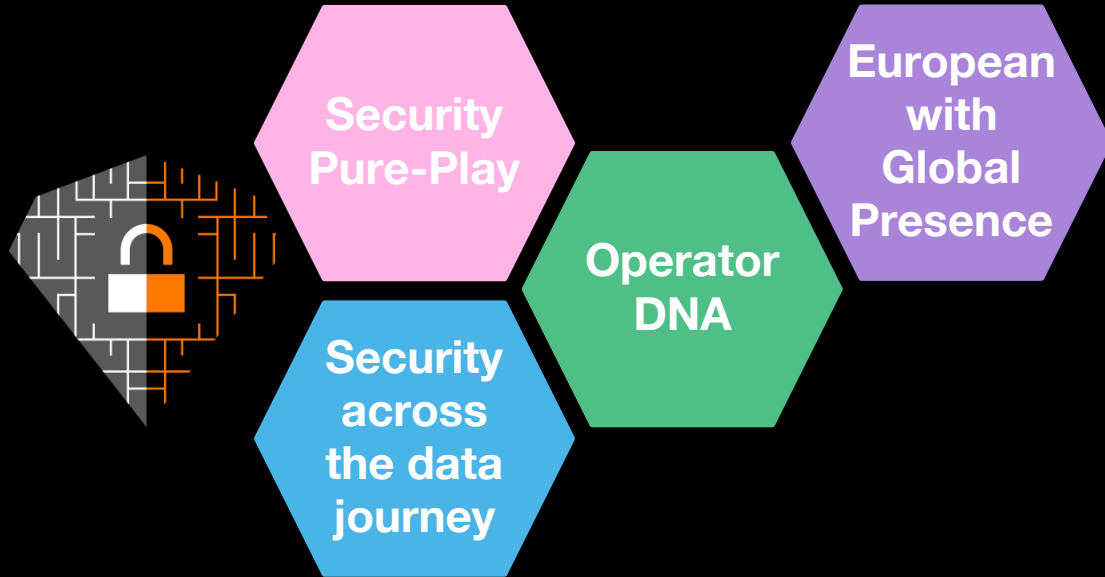
**Business
Services**



Unique positioning



European MSSP wave, Forrester



Accelerating our international development

SECUREDATA
TRUSTED CYBERSECURITY EXPERTS

**Largest independent managed
security services provider in the UK**



200 people



24/7 UK CyberSOC
with 50 engineers



40 consultants/analysts



12 talks at major
conferences in last 2 years



Lions & Bulls*** in Cyberspace

Charl van der Walt



@charlvdwalt





SENSEPOST

For more information please contact us

T: +44 (0)1622 723400 E: info@secdata.com www.secdata.com

SECUREDATA
TRUSTED CYBERSECURITY EXPERTS





SENSEPOST

For more information please contact us

T: +44 (0)1622 723400

E: info@secdata.com

www.secdata.com

SECUREDATA
TRUSTED CYBERSECURITY EXPERTS



We need better technology.

We need smarter people.

We need stricter regulation.

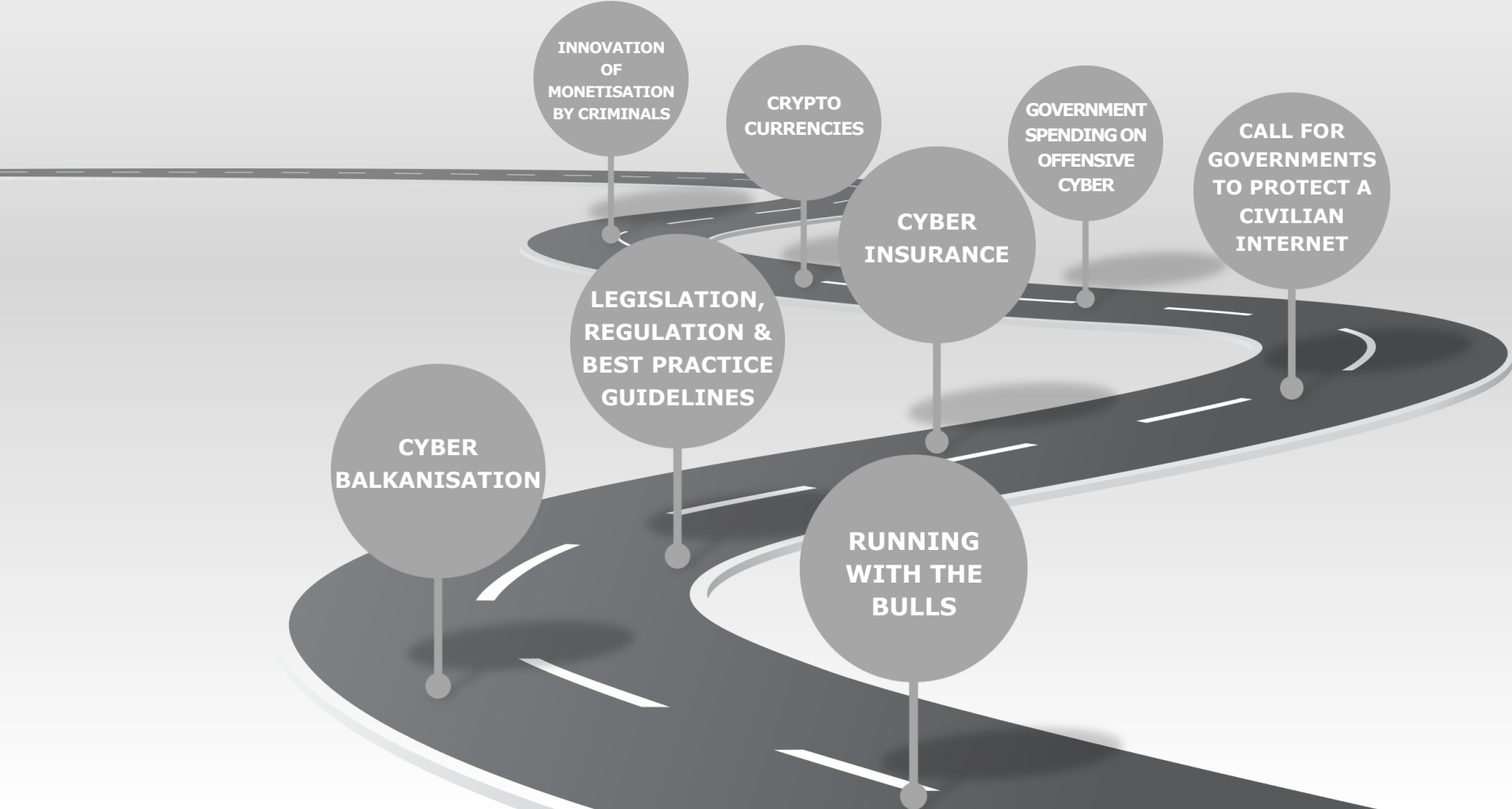
We need more collaboration.

We suck.

We need better analogies.



You can outrun some of the
bulls some of the time, but you
can't outrun all of the bulls all of
the time.





**INNOVATION
OF
MONETISATION
BY CRIMINALS**

**CRYPTO
CURRENCIES**

**GOVERNMENT
SPENDING ON
OFFENSIVE
CYBER**

**CALL FOR
GOVERNMENTS
TO PROTECT A
CIVILIAN
INTERNET**

**CYBER
INSURANCE**

**LEGISLATION,
REGULATION &
BEST PRACTICE
GUIDELINES**

**CYBER
BALKANISATION**

**RUNNING
WITH THE
BULLS**

“I think it is just a temporary trend until someone finds a better idea to make money easier”

eWeek 2012



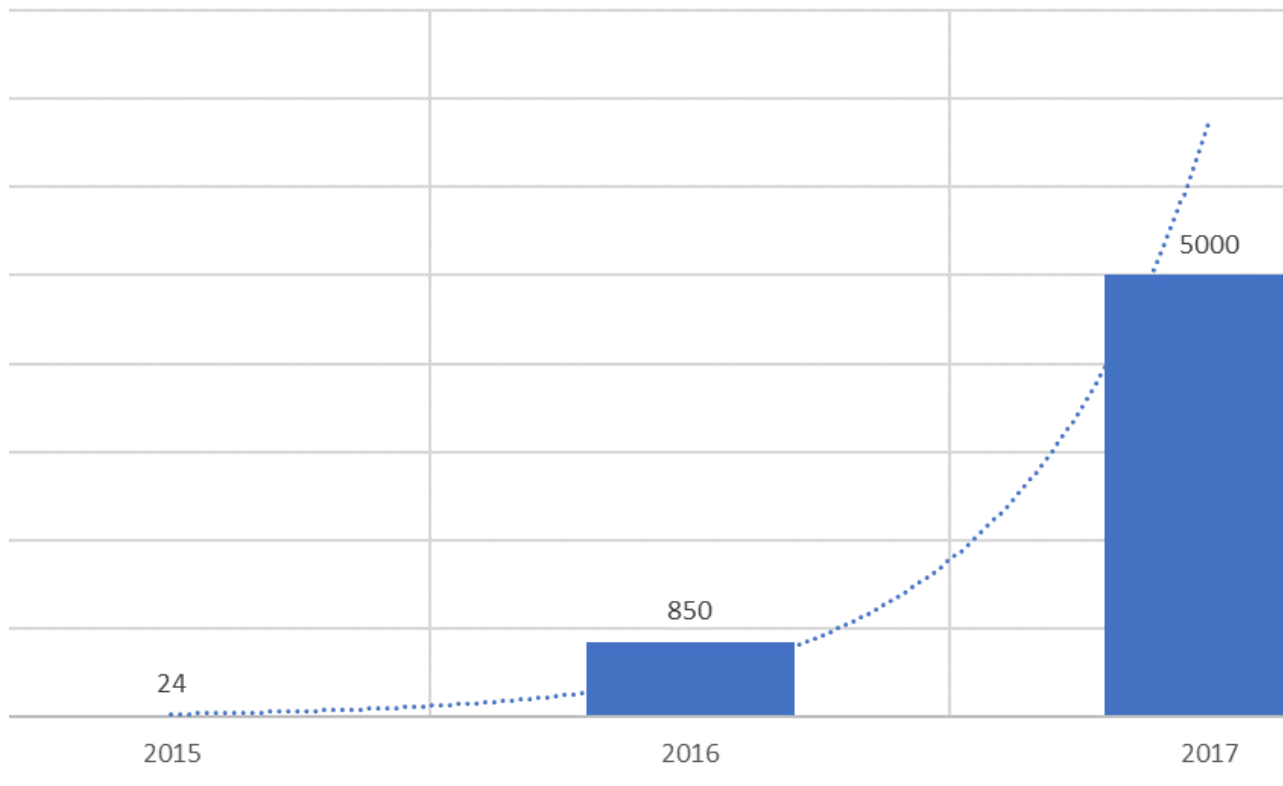
- Ukash
- PaySafeCard
- MoneyPak
- CashU
- Gift Card
- iTunes Vouchers

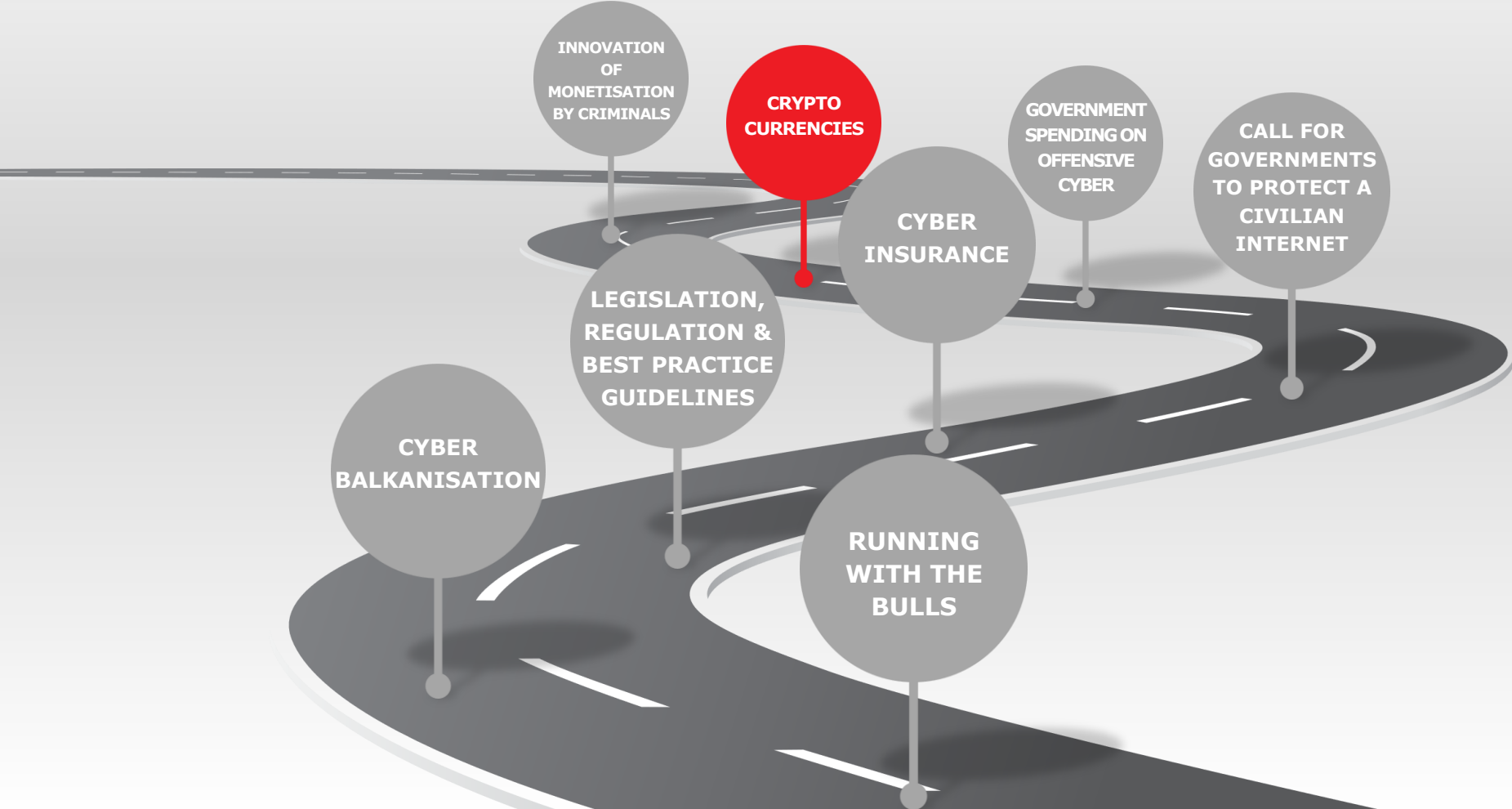


NEW RANSOMWARE SCAM ACCEPTS BITCOIN PAYMENT



Est. Global Ransomware Payments (in millions of dollars)







A Crypto Miner
for your Website

HASHES/S
11.7

TOTAL
356

THREADS
2 + / -



Monetize Your Business With Your **yourdomain.com** Would Like To Use
Your Computing Power

You can support **yourdomain.com** by allowing them to use your processor for calculations. The calculations are securely executed in your Browser's sandbox. You don't need to install anything.

INTEGRATE COINHIVE ON YOUR V

Note: if you are on a mobile device, this may drain your battery.



Spam Protection

Rate limit actions on your site



Monetize

Allow for this session




Cancel

powered by  coinhive – [more info](#)

SUCURI



Hacked Websites Mine Cryptocurrencies

   [SucuriSecurity](#) | [sucuri.net](#)

Hacked Websites Mine Cryptocurrencies

SEPTEMBER 22, 2017  DENIS.SINEGUBKO  



A Crypto Miner
for your Website

HASHES/S
11.7

TOTAL
356

THREADS
2 + / -



Monetize Your Business With Your Users' CPU Power

INTEGRATE COINHIVE ON YOUR WEBSITE



Spam Protection

Rate limit actions on your site



Link Forwarding

Monetize shortlinks to your content

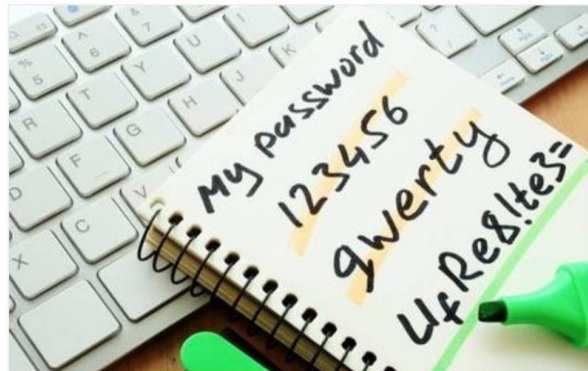
Security

Coin Hive hacked via old password to move manic miners' Monero into miscreants' pockets

Credential leaked from Kickstarter hack used to hijack Cloudflare DNS

By [Iain Thomson in San Francisco](#) 24 Oct 2017 at 19:52

7 SHARE ▼



Monero miner maker Coin Hive was hacked so that websites using its code inadvertently redirected their generated cryptocurrency to miscreants – after the outfit forgot to change an old password.

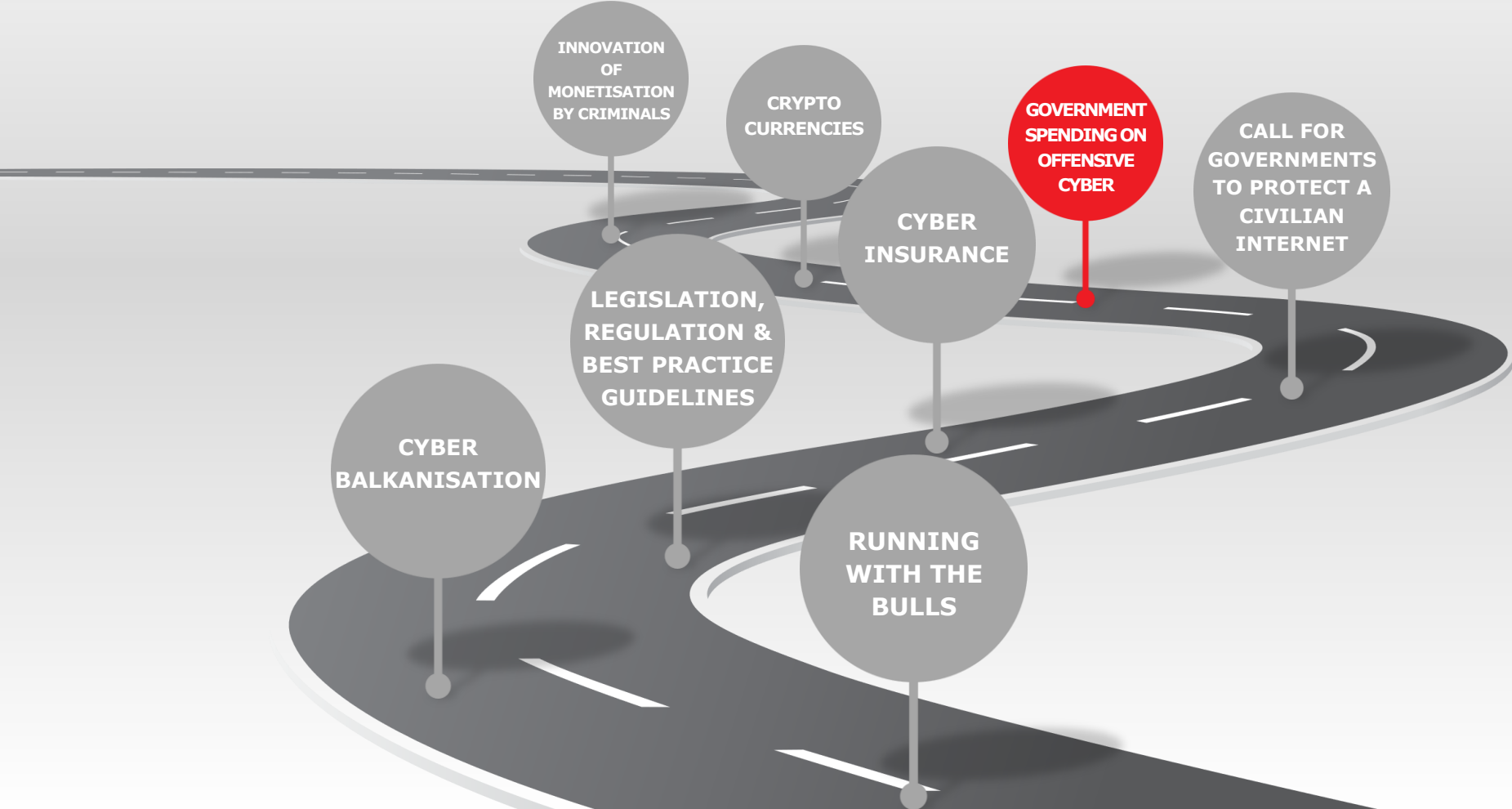


SENSEPOST

For more information please contact us

T: +44 (0)1622 723400 E: info@secdata.com www.secdata.com

SECUREDATA
TRUSTED CYBERSECURITY EXPERTS





SENSEPOST

For more information please contact us

T: +44 (0)1622 723400

E: info@secdata.com

www.secdata.com

SECUREDATA
TRUSTED CYBERSECURITY EXPERTS

URGENT
PETYA RANSOMWARE
MASSIVE GLOBAL ATTACK

Unprecedented new threats, attacks & compromises



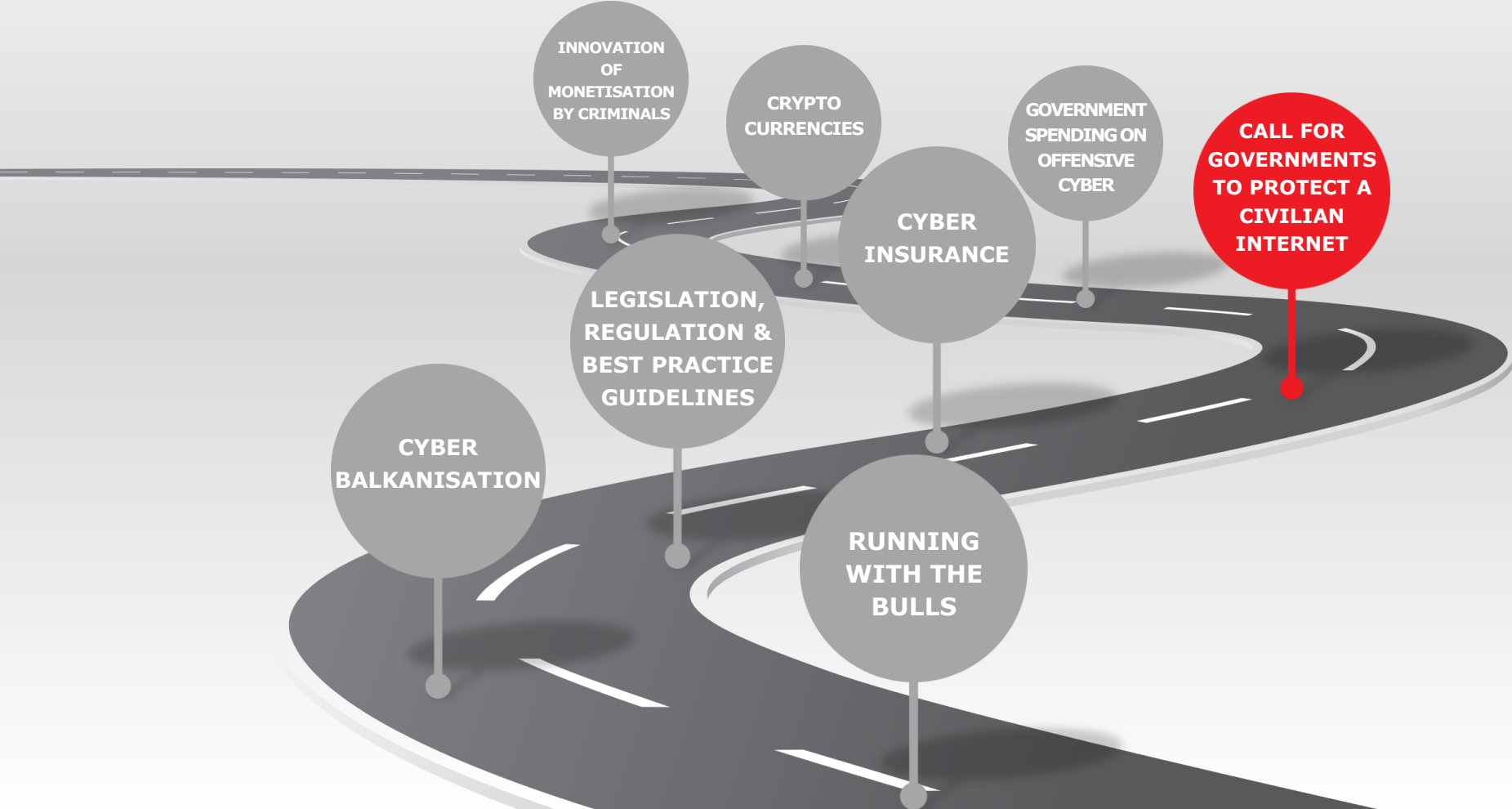
Government hacking investment leak into the civilian space



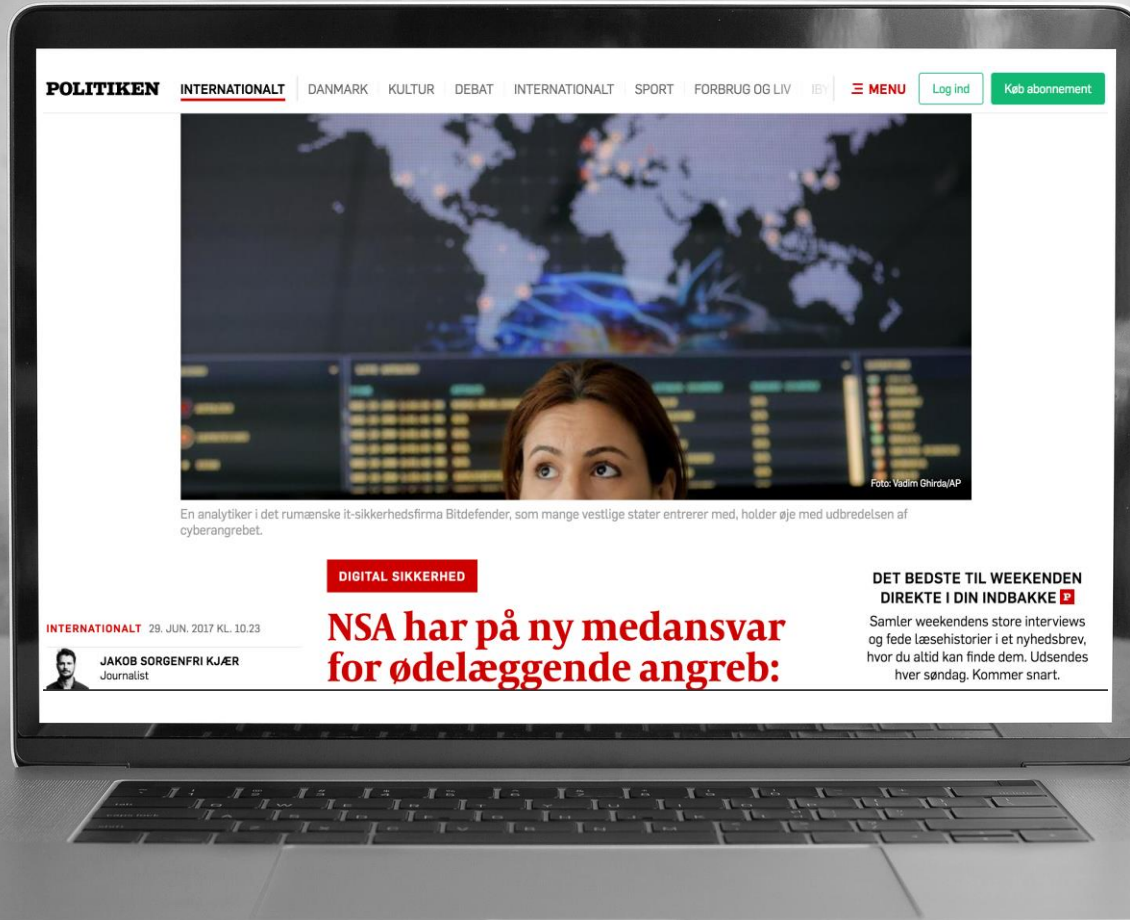
New types and levels of cybercrime are enabled by cryptocurrencies



A Cybercrime ecosystem hungry for new revenues



"We see unstable airports, we see people who are unable to purchase their rye bread or fuel for their cars because NSA developed a cyber weapon, which is now being abused by criminals."



[HOME](#)[ABOUT US](#)[NEWSROOM](#)[INCIDENTS](#)[RESOURCES](#)[TICSA](#)

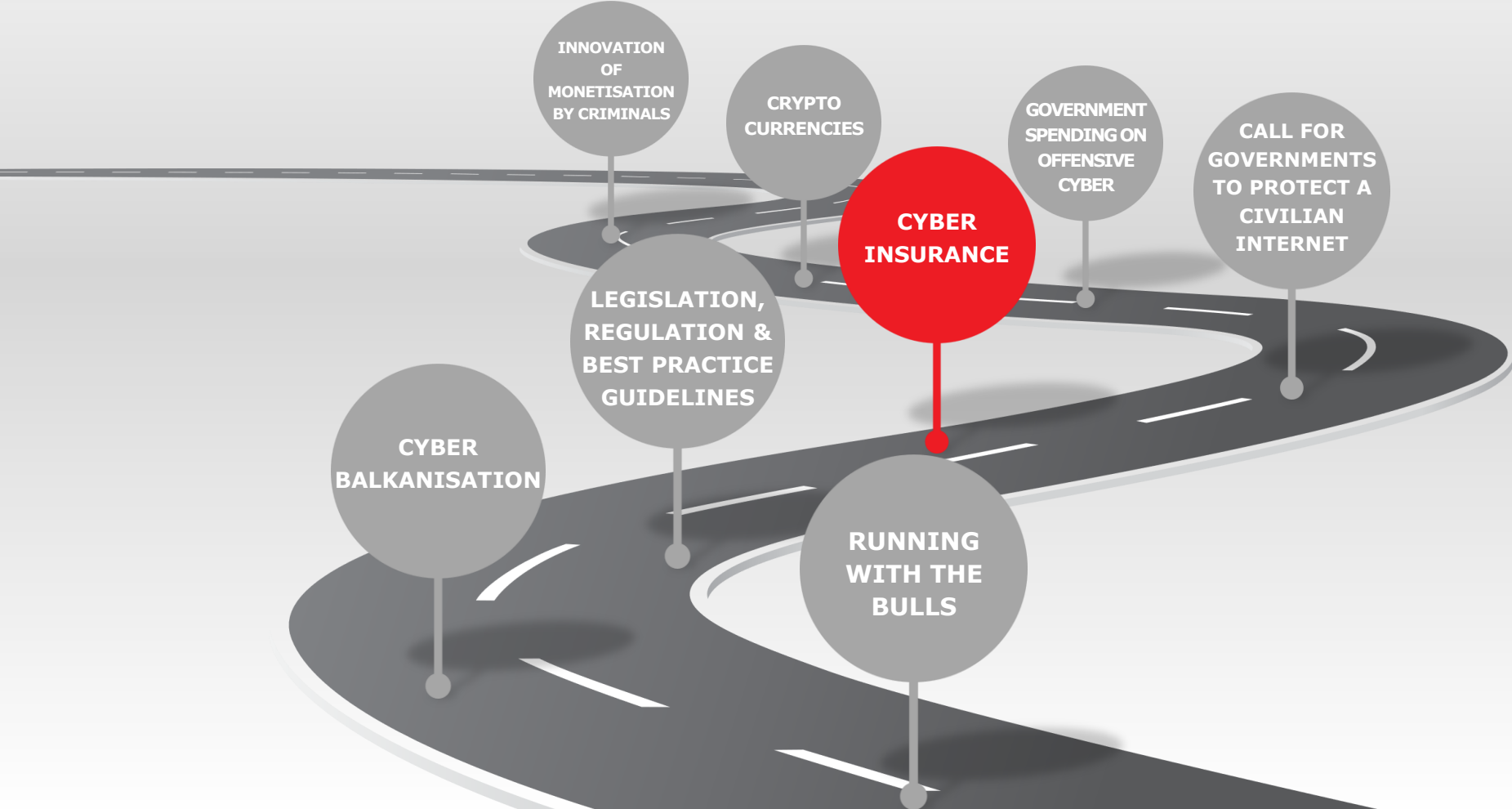
ABOUT THE NATIONAL CYBER SECURITY CENTRE

The New Zealand National Cyber Security Centre (NCSC) provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.



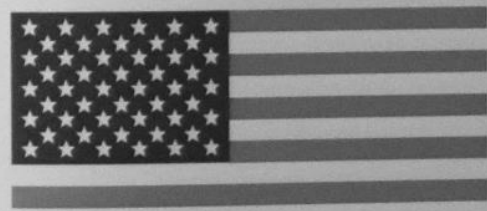
to protect New Zealand's most significant organizations, To protect their networks from the types of threats **which are typically beyond the capability of commercially available tools**, and from threats which could potentially impact on the effective functioning of government administration or key economic sectors.

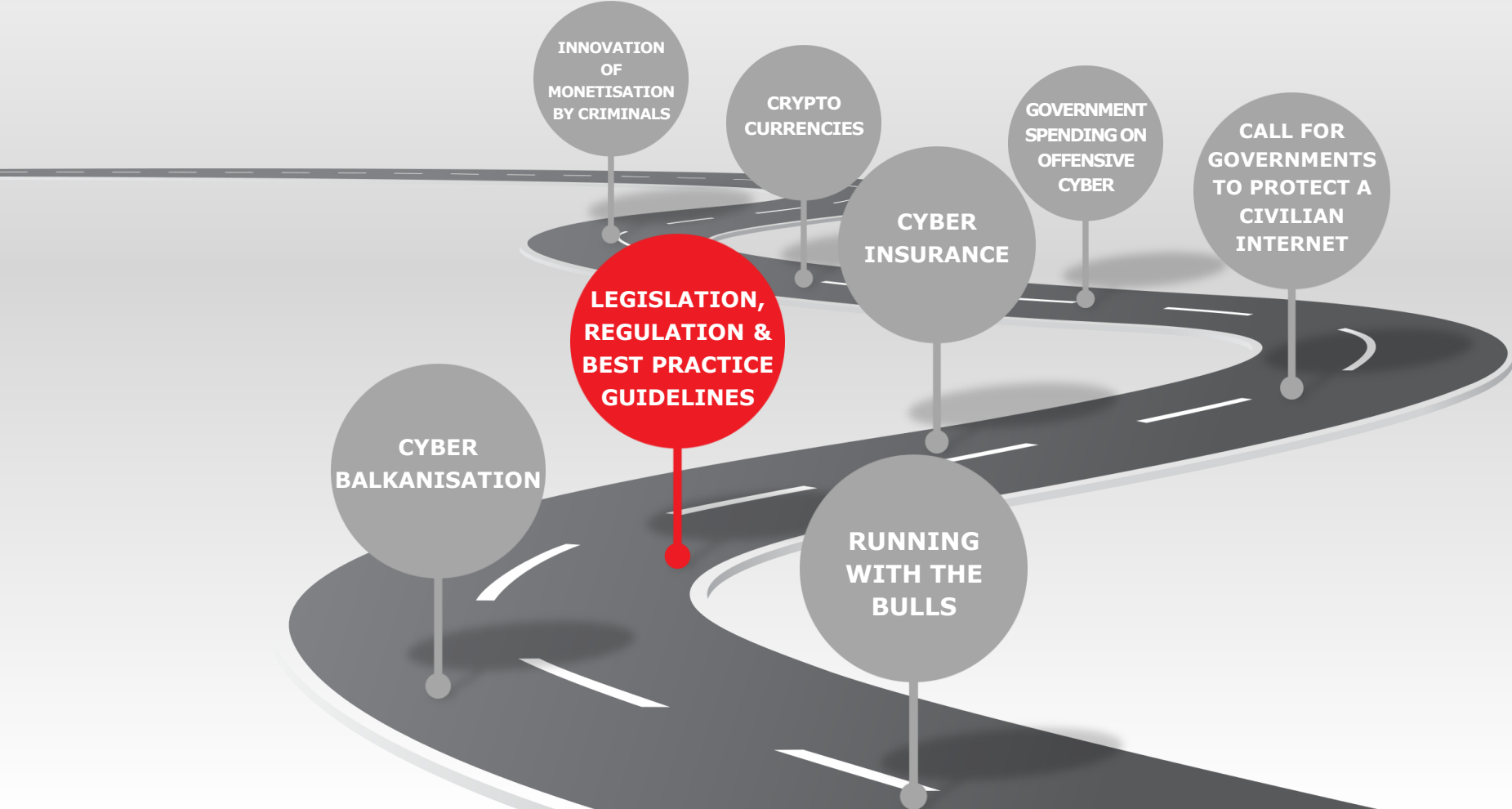






Congressman
Ed Perlmuter
Representative
Colorado
7th District







“The level of risk associated with the GDPR has catapulted data protection into the boardroom”.

Jane Finlayson-Brown – Allen & Overy

4%

Fines for non-compliance and data breaches will soar under GDPR, reaching up to 4% of a company's global turnover

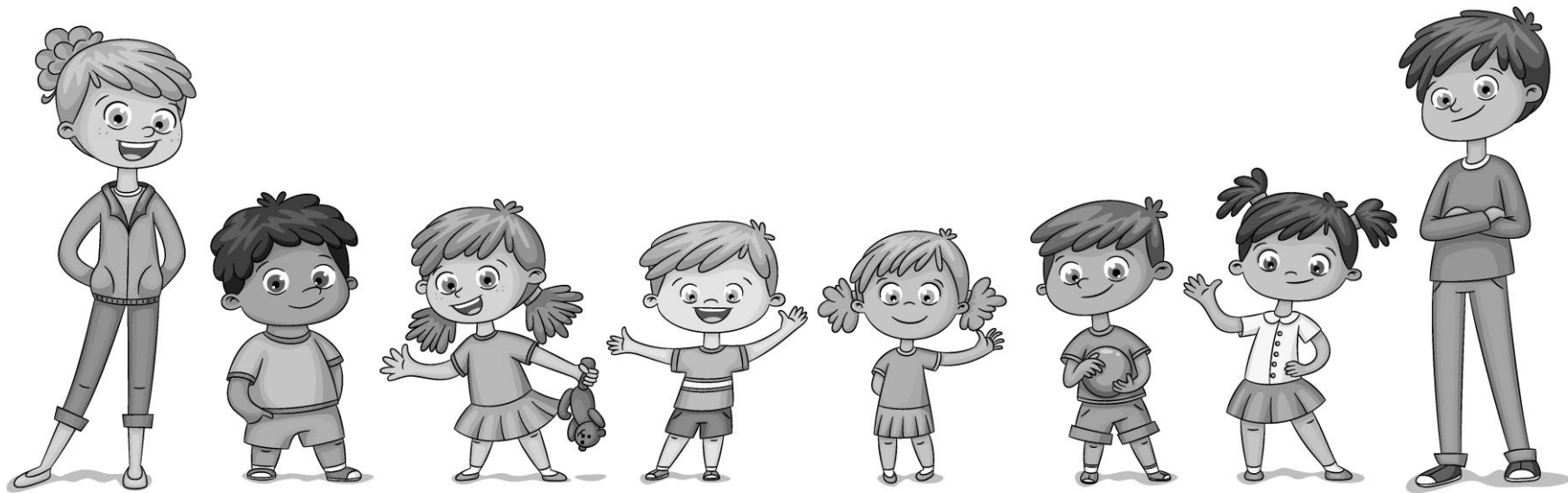
£90m

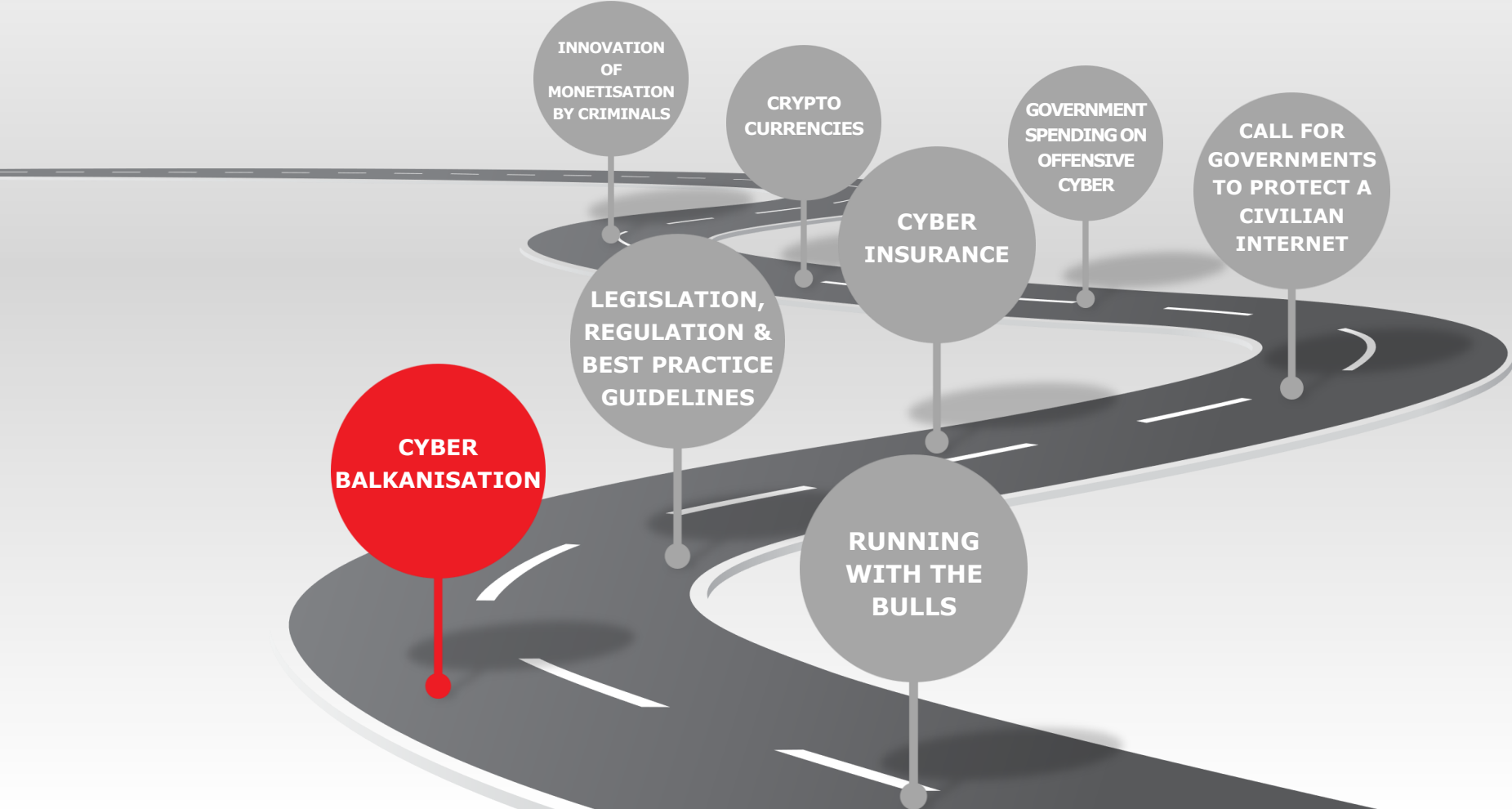
Had the TalkTalk breach occurred under GDPR, the company could have faced fines of up to £90 million

72h

Organisations will be required to inform regulators within 72 hours. When it's in the interest of consumers, regulators will also release news of the breach publicly

Kindergarten!





Balkanization

Bal·kan·ize [bawl-kuh-nahyz]

verb (used with object), Bal·kan·ized, Bal·kan·iz·ing.

1. to divide (a country, territory, etc.) into small, quarrelsome, ineffectual states.

Thursday, March 23, 2017

Five Reasons I Want China Running Its Own Software

China Wants To Replace Microsoft, Apple, And Android Software By October



American software with indigenous or semi-indigenous alternatives. I then reply via Twitter that I love the idea with a thumbs up. This post will list the top five reasons why I want China and other likely targets of American foreign intelligence collection to run their own software.

- 1. Many (most?) non-US software companies write lousy code.** The US is by no means perfect, but our developers and processes generally appear to be superior to foreign indigenous efforts. Cisco vs Huawei is a good example. Cisco has plenty of problems, but it has processes in place to manage them, plus secure code development practices. Lousy indigenous code means it is easier for American intelligence agencies to penetrate foreign targets. (An example of a foreign country that excels in writing code is Israel, but thankfully it is not the same sort of priority target like China, Russia, or North Korea.)
- 2. Many (most?) non-US enterprises are 5-10 years behind US security practices.** Even if a foreign target runs decent native code, the IT processes maintaining that code are lagging compared to American counterparts. Again, the US has not solved this problem by any stretch of the imagination. However, relatively speaking, American inventory management, patch management, and security operations have the edge over foreign intelligence targets. Because non-US enterprises running indigenous code will not necessarily be able to benefit from American expertise (as they might if they were running American code), these deficiencies will make them easier targets for foreign exploitation.

3. Foreign targets running foreign code is win-win for American intel and enterprises. The current vulnerability equities process (VEP) puts American intelligence agencies in a quandary. The IC develops a zero-day exploit for a vulnerability, say for use against Cisco routers. American and Chinese organizations use Cisco routers. Should the IC sit on the vulnerability in order to maintain access to foreign targets, or should it release the vulnerability to Cisco to enable patching and thereby protect American and foreign systems?

This dilemma disappears in a world where foreign targets run indigenous software. If the IC identifies a vulnerability in Cisco software, and the majority of its targets run non-Cisco software, then the IC is more likely (or should be pushed to be more likely) to assist with patching the vulnerable software. Meanwhile, the IC continues to exploit Huawei or other products at its leisure.

Blogging Since 8 Jan 2003

TAOSECURITY
THE WAY OF DIGITAL SECURITY™

TaoSecurity Gear



Get Mugs and More at TeePublic

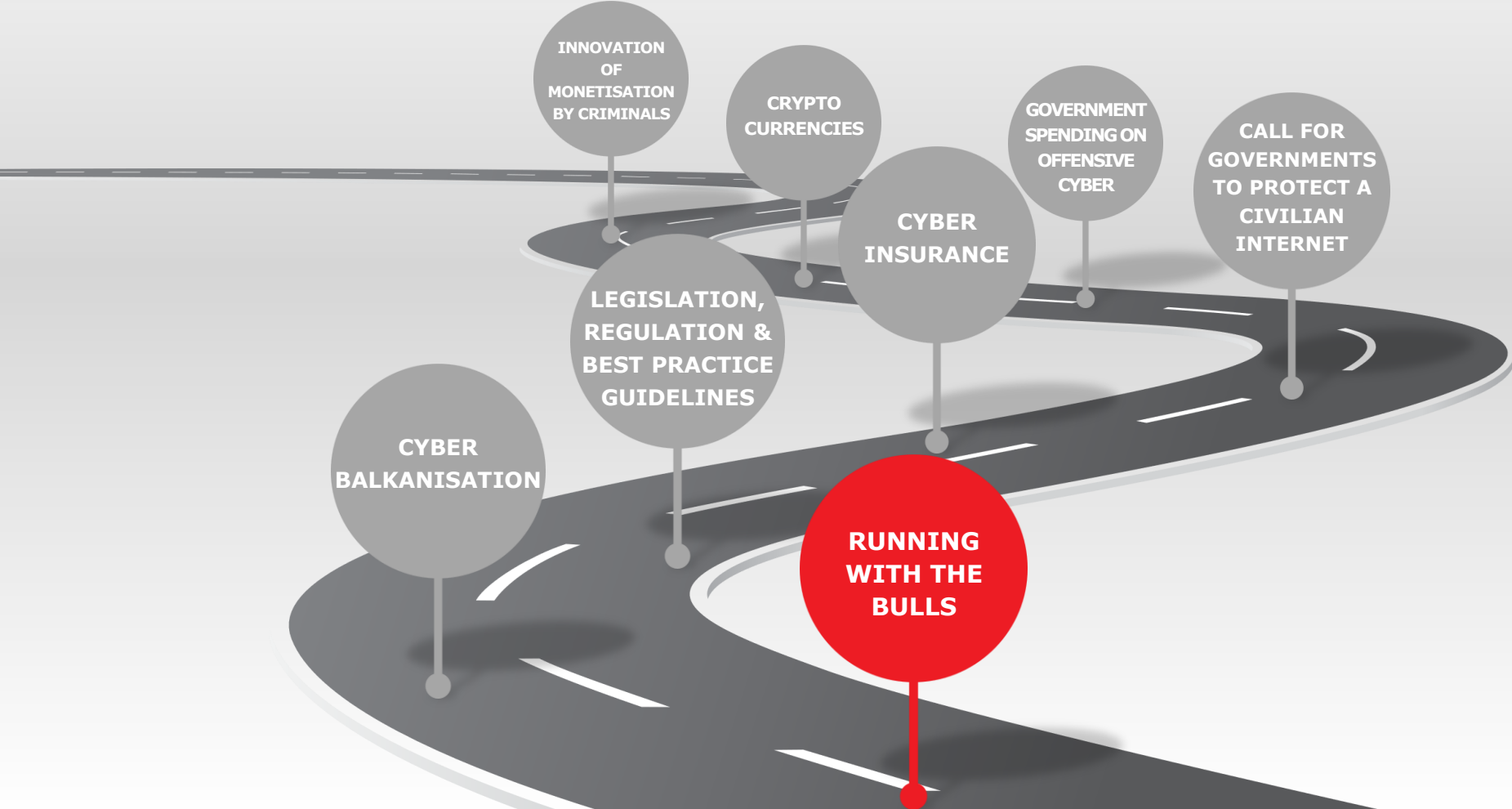
About Me



RICHARD BEJTlich

[View my complete profile](#)

twitter.com/taosecurity





An abstract network diagram with numerous grey nodes of varying sizes connected by thin grey lines, set against a light grey background with some white dots.

In a mature defense strategy
detection has a place

WHY DETECTION

1 DEFENSE

Any good enterprise strategy needs to cover Assessment, Protection, Detection & Response.

Are we doing everything we could to track contemporary threats and realities?

2 COMPLIANCE

Increasingly being demanded as a best practice by standards and regulations.

In the case of a breach can we claim that we took all reasonable steps to protect our assets?

3 READINESS

Data collection and correlation is as much about investigation as it is about detection.

Are we in a position to rapidly perform triage in the event of a compromise?



Threat Detection in practice



1. Know your Enemy
2. Know your Self
3. People & Principles trump Technology

KNOW THY SELF, KNOW THY ENEMY.
A THOUSAND BATTLES, A THOUSAND VICTORIES.

An abstract network diagram consisting of numerous nodes (dots) of varying sizes and colors (grey, black, white) connected by thin, light grey lines. The nodes are distributed across the frame, with a higher density of connections on the right side, creating a complex web-like structure.

Know Your Enemy

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Image File Execution Options Injection			Forced Authentication	Network Share Discovery	AppleScript		Man in the Browser	Exfiltration Over Physical Medium	Multi-hop Proxy
Plist Modification			Hooking	System Time Discovery	Third-party Software		Browser Extensions		Domain Fronting
Valid Accounts			Password Filter DLL	Peripheral Device Discovery	Windows Remote Management		Video Capture	Exfiltration Over Command and Control Channel	Data Encoding
DLL Search Order Hijacking			LLMNR/NBT-NS Poisoning	Account Discovery	SSH Hijacking	LSASS Driver	Audio Capture	Scheduled Transfer	Remote File Copy
AppCert DLLs	Process Doppelgänger		Securityd Memory	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Automated Collection	Data Encrypted	Multi-Stage Channels
Hooking	Mshsa		Private Keys	System Information Discovery	Pass the Ticket	Local Job Scheduling	Clipboard Data		Web Service
Startup Items	Hidden Files and Directories		Keychain		Replication Through Removable Media	Trap	Email Collection	Exfiltration Over Other Network Medium	Standard Non-Application Layer Protocol
Launch Daemon	Launchctl		Input Prompt	Security Software Discovery	Windows Admin Shares	Source	Screen Capture	Exfiltration Over Alternative Protocol	Communication Through Removable Media
Dylib Hijacking	Space after Filename		Bash History	System Network Connections Discovery	Remote Desktop Protocol	Launchctl	Data Staged		Multi-layer Encryption
Application Shimming	LC_MAIN Hijacking		Two-Factor Authentication Interception		Pass the Hash	Space after Filename	Input Capture	Data Transfer Size Limits	Standard Application Layer Protocol
Appinit DLLs	HISTCONTROL		Account Manipulation	System Owner/User Discovery	Exploitation of Vulnerability	Execution through Module Load	Data from Network Shared Drive	Data Compressed	Commonly Used Port
Web Shell	Hidden Users		Replication Through Removable Media	System Network Configuration Discovery	Shared Webroot	Regsvcs/Regasm	Data from Local System		Standard Cryptographic Protocol
Service Registry Permissions Weakness	Clear Command History		Input Capture		Ligon Scripts	InstallUtil	Data from Removable Media		Custom Cryptographic Protocol
Scheduled Task	Gatekeeper Bypass		Network Sniffing	Application Window Discovery	Remote Services	Regsvr32			Data Obfuscation
New Service	Hidden Window		Credential Dumping	Network Service Scanning	Application Deployment Software	Execution through API			Custom Command and Control Protocol
File System Permissions Weakness	Deobfuscate/Decode Files or Information		Brute Force	Query Registry	Remote File Copy	PowerShell			Connection Proxy
Path Interception	Trusted Developer Utilities		Credentials in Files	Remote System Discovery	Taint Shared Content	Rundll32			Uncommonly Used Port
Accessibility Features	Regsvcs/Regasm			Permission Groups Discovery		Scripting			Multiband Communication
Port Monitors				Process Discovery		Graphical User Interface			Failback Channels
Screensaver	Exploitation of Vulnerability			System Service Discovery		Command-Line Interface			
LSASS Driver	Extra Window Memory Injection					Scheduled Task			
Browser Extensions	Access Token Manipulation					Windows Management Instrumentation			
Local Job Scheduling	Bypass User Account Control					Trusted Developer Utilities			
Re-opened Applications	Process Injection					Service Execution			
Rc.common	SID-History Injection	Component Object Model							
Login Item	Sudo	Hijacking							
LC_LOAD_DYLIB Addition	Setuid and Setgid	InstallUtil							
Launch Agent		Regsvr32							
Hidden Files and Directories		Code Signing							
.bash_profile and .bashrc		Modify Registry							
Trap		Component Firmware							
Launchctl		Redundant Access							
Office Application Startup		File Deletion							
Create Account		Timestamp							
External Remote Services		NTFS Extended Attributes							
Authentication Package		Process Hollowing							
Netsh Helper DLL		Disabling Security Tools							
Component Object Model Hijacking		Rundll32							
Redundant Access		DLL Side-Loading							
		Indicator Removal on Host							

attack.mitre.org

Reconnaissance

Weaponization

Delivery

Exploitation

Installation

Command & Control

Actions on Objectives

An abstract network diagram consisting of numerous nodes (dots) of varying sizes and colors (gray, black, white) connected by thin, light gray lines. The nodes are distributed across the frame, with a higher density of connections on the right side, creating a complex web-like structure.

Know Your Self

MAYBE MORE OF THIS?

Testing canary files & LR — Sent

charl van der walt
Testing canary files & LR
To: Etienne Greeff


Sent - SensePost 11:46 CV

Hello All,

Please would you help me out by saving this file and opening it up for me.? Its just a call-back. nothing malicious!

Thanks.

./charl

 token_test.xlsx

token_test

Search Sheet

Home Insert Page Layout Formulas Data Review View Share

Paste Font Alignment Number Conditional Formatting Format as Table Cells Editing

A1 :ffff:10.200.10.164

	A	B	C	D	E	F	G	H	I	J	K
1	ffff:10.200	216	2437								
2	RMTCAS01	188	17964								
3	RMTCAS01	140	17059								
4	ffff:10.200	63	205								
5	10.200.10.1	59	1227								
6	10.200.10.1	50	1242								
7	10.200.10.1	42	1022								
8	RMT-SYSG	41	3032543								
9	RMTROS07	38	9160								
10	RMT-SYSG	37	2291398								
11	RMTROS02	36	8852								
12	RMTROS04	33	16713								
13	rmtrsh01	29	633								
14	RMTROS0C	28	372								
15	rmtrsh01	22	626								
16	RMTROS01	20	3668								
17	RMTROS0C	19	344								
18	10.200.10.1	19	1646								
19	ffff:10.10	17	71								
20	ffff:10.200	17	80								
21	10.200.10.1	16	454								
22	10.200.10.1	16	1802								
23	ffff:102.11	13	29								
24	rmtrsh08 (13	254								
25	rmtrsh08	13	145								
26	rmtrsh02	13	200								
27	ffff:10.200	12	53								
28	ffff:10.200	12	38								
29	rmtrshue0	11	690								
30											
31											
32											
33											
34											
35											
36											
37											
38											
39											
40											
41											
42											
43											

Ready Sheet1 100%

DECEPTION & TRAPS

LogRhythm Dashboards Alarms Cases Searches Reports

Search...

BGL Suspicious IP 2.125.177.154

Evidence

LOGS (VIEW IN ANALYZER)

SD-van der Walt, Charl added a set of logs 08/15/2017 2:40 pm

Add Note Add Logs Add File

Tags

Select Tags

Associated Cases

Select a Case

History

Alarms

Live Data

Card Grid

In the last 1 hours Alarm Status: Any Entity: Any Alarm Rule: Any Risk: Any Notification List: Any Alarm Group: Any Alarm Id: Any

Check Visible

Sort By Date Triggered (Desc)

19 AIE: SD: Repeat Offender 08/24/2017 4:19:42 pm Id: 1841980 SmartResponse Succeeded

33 AIE: CSC: External DNS Observed 08/24/2017 4:18:18 pm Id: 1841979 SmartResponse Succeeded

45 AIE: Lateral: Account Added to Admin Group 08/24/2017 4:17:53 pm Id: 1841978 SmartResponse Succeeded

19 AIE: SD: Suspicious Web Activity 08/24/2017 4:15:24 pm Id: 1841974 SmartResponse Succeeded

85 AIE: SD: File Canary Trigger 08/24/2017 4:15:10 pm Id: 1841973 SmartResponse Succeeded

85 AIE: SD: File Canary Trigger 08/24/2017 4:15:10 pm Id: 1841972 SmartResponse Succeeded

19 AIE: SD: Repeat Offender 08/24/2017 4:14:42 pm Id: 1841971 SmartResponse Succeeded

67 LogRhythm AI Engine Heartbeat Missed 08/24/2017 4:13:57 pm Id: 1841968

67 AI Engine : Excessive Warnings 08/24/2017 4:13:57 pm Id: 1841969

67 SD: LogRhythm Component Excessive Warnings

85 AIE: SD: File Canary Trigger

85 AIE: SD: File Canary Trigger

You have no background tasks running.

Inspector

Id: 1841973 | AIE-SD: File Canary Trigger

Data, Comments & Details AI Engine Rule

Data

Alarm ID 1841973

Alarm Date 08/24/2017 4:15:10 pm

Alarm Name AIE: SD: File Canary Trigger

Classification Suspicious

Log Source AI Engine (AIEEngineID: 5) (1000349)

Common Event AIE: SD: File Canary Trigger

Direction Unknown

Entity (Origin) Global Entity

Entity (Impacted) SecureData-Lab

Host (Origin) 87.238.200.1

Object Mozilla/5.0 (Macintosh; Intel Mac OS X) Excel/0.0.0

URL /canary/allan_wuz_here_12345.png

Alarm Actions

Status Closed

Sub-Status: Monitor

Add To Case

Please Select Add

OR

New Case

MacBook



Every Marine a rifleman no more?

By: [Jeff Schogol](#), May 7, 2017 *(Photo Credit: Cpl. Jesus Sepulveda Torres/Marine Corps)*

Former Defense Secretary Ash Carter shocked the military last summer when he called for boosting the military's high-tech force by finding civilians who already have those vital skills like cyber security and offer them "lateral entry" into the military — a chance to skip boot camp and put on a uniform as a mid-career rank from Day One.

WHY MANAGED DETECTION

1 FOUR P'S

People, Process, Platform and Project Management are tedious and expensive if not core business.

Do we want to spend our time and effort doing the basics when modern security needs to be agile?

2 SKILL

Appropriate skills are incredibly difficult to identify, hire, equip and retain in a competitive market.

Do we have the resources, experience and environment to retain our own set of capabilities?

3 AGILITY

Threat detection is not plug-and-play and continuous investment is required to respond to new risks.

Do we have the environment to continuously extend and adapt our detection capability?

SELECTING A PARTNER

1 THE BASICS

Our mission is to the basics right, focusing on repeatable, managed processes and proven technology.

Can we confidently say that we've addressed the basics and know what we're getting?

2 SCOPE

Our offering leverages the best skills in the market but is also honest about fallibility.

Are we willing to trust any single technology or system for any part of our defensive strategy?

3 FIT

We are big enough to compete globally but small enough to be a trusted extension of your team.

Who can we trust to be personally available for all of our security needs?



"Questions?"

Charl van der Walt



@charlvdwalt

Come and see us:

Demo booths:

Orange
Cyberdefense

DiLAN

Partner Talks:



16:30 Balcony room





Thank you...
we're listening

**Companies thrive
on innovation.
We work to
shape yours.**

