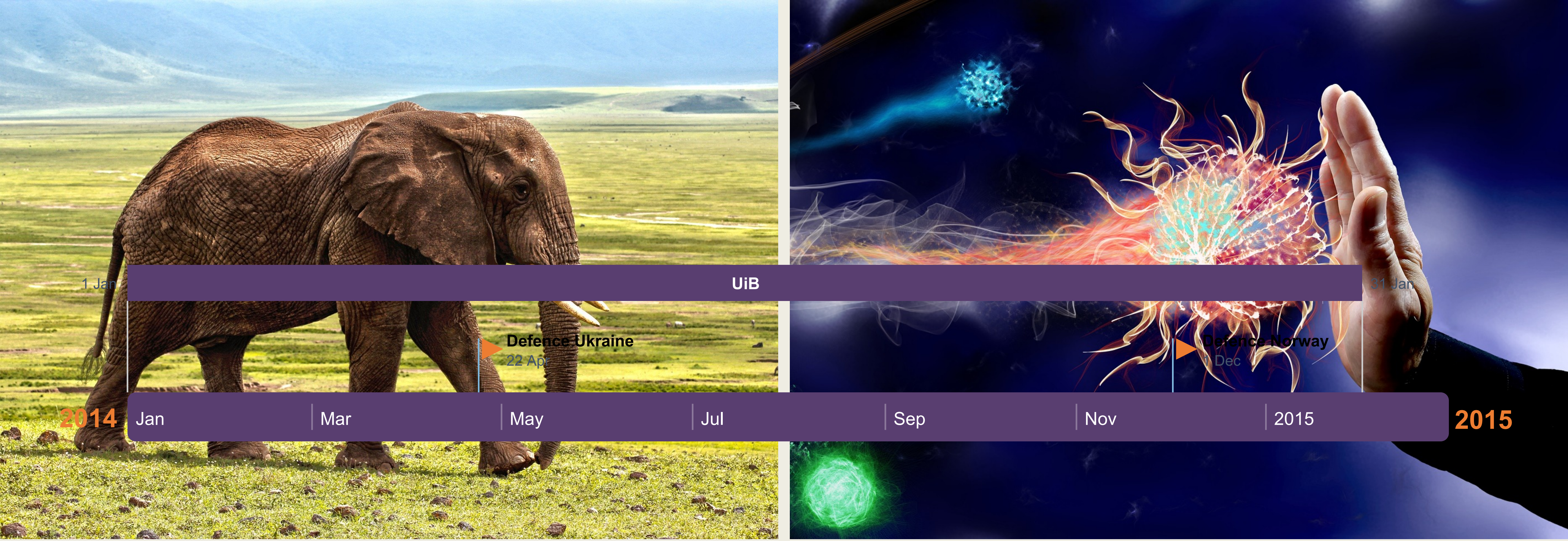
TIME-LAPSE IN INDUSTRY: 5 YEARS IN 40 MINUTES

Oleksandr Kazymyrov

whoami

I received a Ph.D. degree in Information Security, and I am co-author of Ukrainian national standards for block cipher and hash function (DSTU 7624:2014 and DSTU 7564:2014). I am an expert in network security with several certifications such as CISSP, E|CEH (Certified Ethical Hacker) and E|CES (Certified Encryption Specialist). In addition, as a technical test manager / test analyst at EVRY, I have gained expertise in various areas of information security (i.e., security and risk management, network security, penetration testing, and operation of critical and security systems). My current position is Information Security Manager with the overall responsibility of information security in G2 Ocean, Grieg Star and Gearbulk.



1 Jan

UiB

31 Jan

Defence Ukraine
22 Apr

Defence Norway
1 Dec

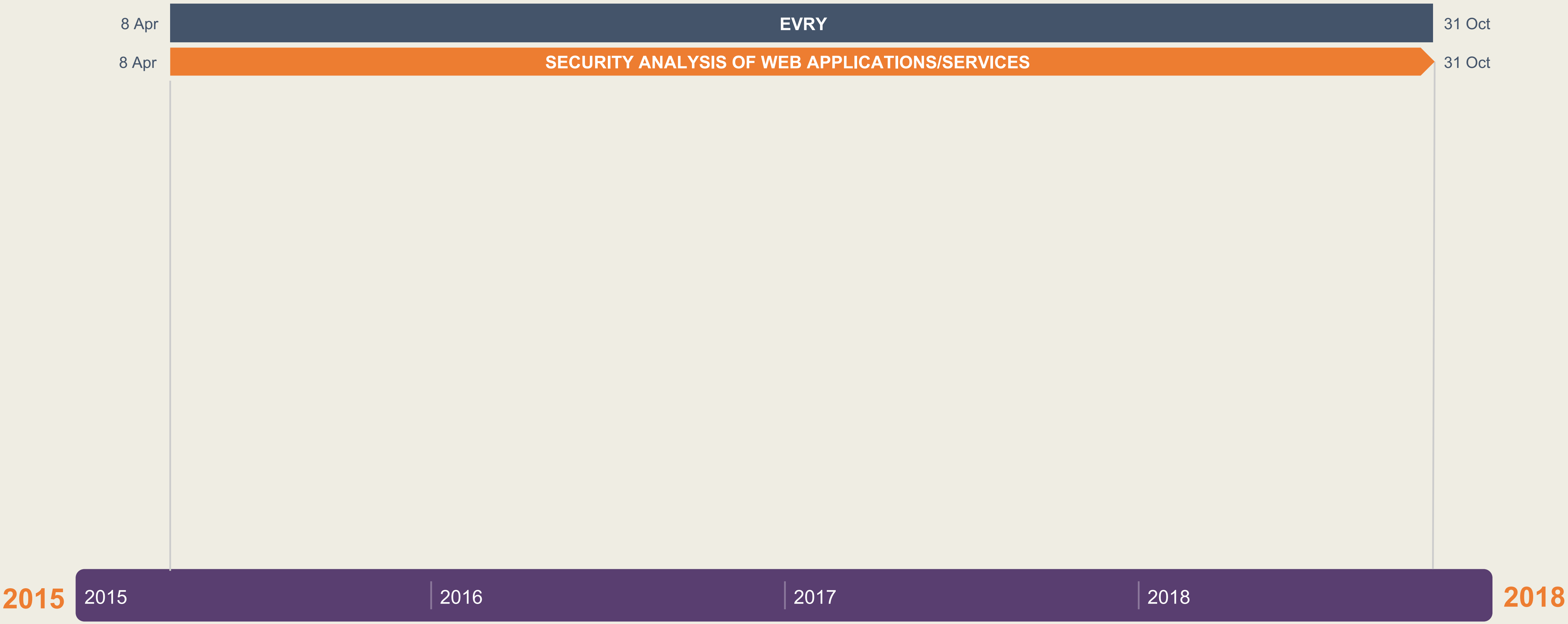
2014 Jan | Mar | May | Jul | Sep | Nov | 2015 2015

DEFENSE

UNIVERSITATIS BERGENSIS
UNIVERSITATIS BERGENSIS
Georgy Ivanov

GRADUATION

Live in EVRY



8 Apr EVRY 31 Oct

8 Apr SECURITY ANALYSIS OF WEB APPLICATIONS/SERVICES 31 Oct

2015 2015 2016 2017 2018 2018

OWASP TOP TEN

THEN 2013

- A1 – SQL injection
- A2 – Broken Authentication and Session Management
- A3 – Cross Site Scripting (XSS)
- A4 – Insecure Direct Object references
- A5 – Security Misconfigurations
- A6 – Sensitive Data exposure
- A7 – Missing Function Level Access Control
- ☒ A8 – Cross-Site Request Forgery (CSRF)
- A9 – Using components with Known Vulnerabilities
- ☒ A10 – Unvalidated Redirects and Forwards

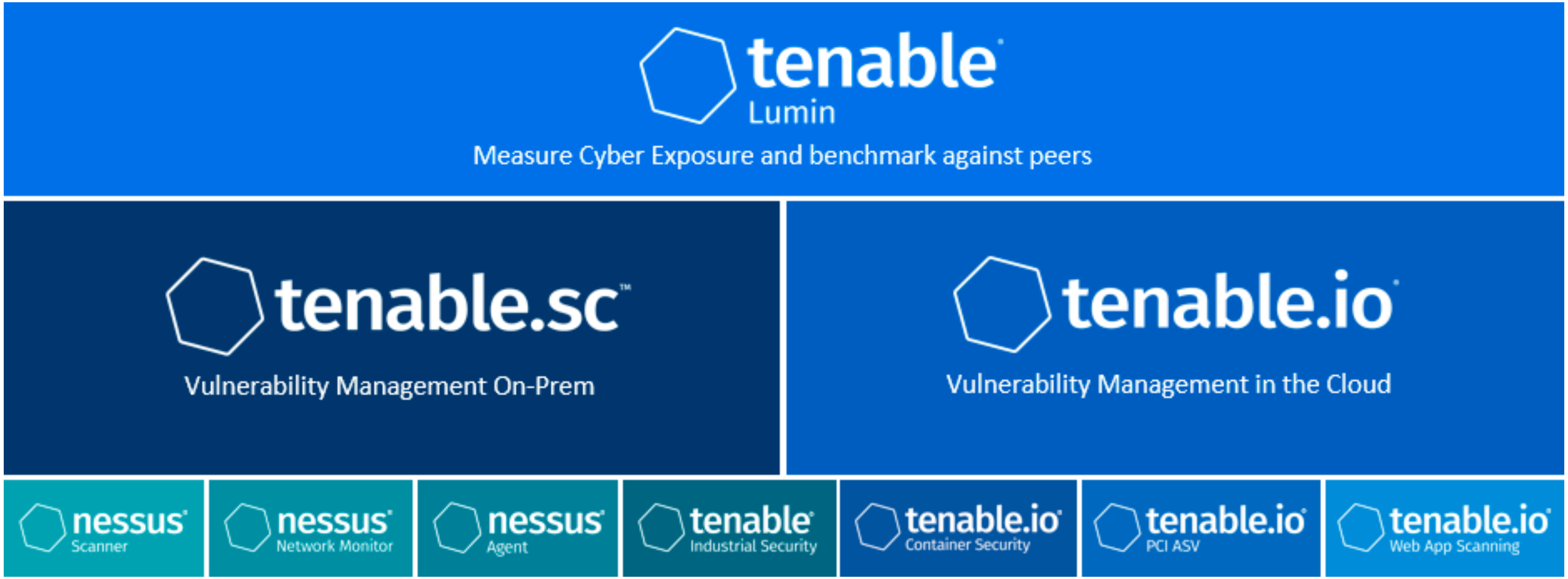
NOW 2017

- A1 – Injection
- A2 – Broken Authentication
- A3 – Sensitive Data Exposure ↑
- A4 – XML External Entities (XEE New!
- A5 – Broken Access Control
- A6 – Security Misconfigurations ↓
- A7 – Cross Site Scripting (XSS)
- New! A8 – Insecure Deserialization
- A9 – Using components with Known Vulnerabilities
- A10 – Insufficient logging and monitoring New!

Source: OWASP.org

	Applicability	Building			Building, Configuration, Deployment Assurance and Verification			Assurance and Verification	
Level 1	🟨 All apps		🟨 Secure Coding	🟨 Standards and checklists	🟨 Secure & Peer Code Review	🟨 DevSecOps	🟨 Unit and Integration Tests	🟩 Penetration Testing	🟨 DAST
Level 2	🟩 All apps	🟩 Security Architecture and Reviews	🟩 Secure Coding	🟩 Standards and checklists	🟩 Secure & Peer Code Review	🟩 DevSecOps	🟩 Unit and Integration Tests	🟩 Hybrid Reviews	🟨 SAST
Level 3	🟩 High Assurance	🟩 Security Architecture and Reviews	🟩 Secure Coding	🟩 Standards and checklists	🟩 Secure & Peer Code Review	🟩 DevSecOps	🟩 Unit and Integration Tests	🟩 Hybrid Reviews	🟨 SAST

Legend	🟨 Acceptable	🟩 Suitable



tenable Lumin

Measure Cyber Exposure and benchmark against peers

tenable.sc™

Vulnerability Management On-Prem

tenable.io

Vulnerability Management in the Cloud

nessus Scanner

nessus Network Monitor

nessus Agent

tenable Industrial Security

tenable.io Container Security

tenable.io PCI ASV

tenable.io Web App Scanning

Summary

15,776,265 matches in 13 targets

319,864 matches with prohibited data

11,394 matches with test data

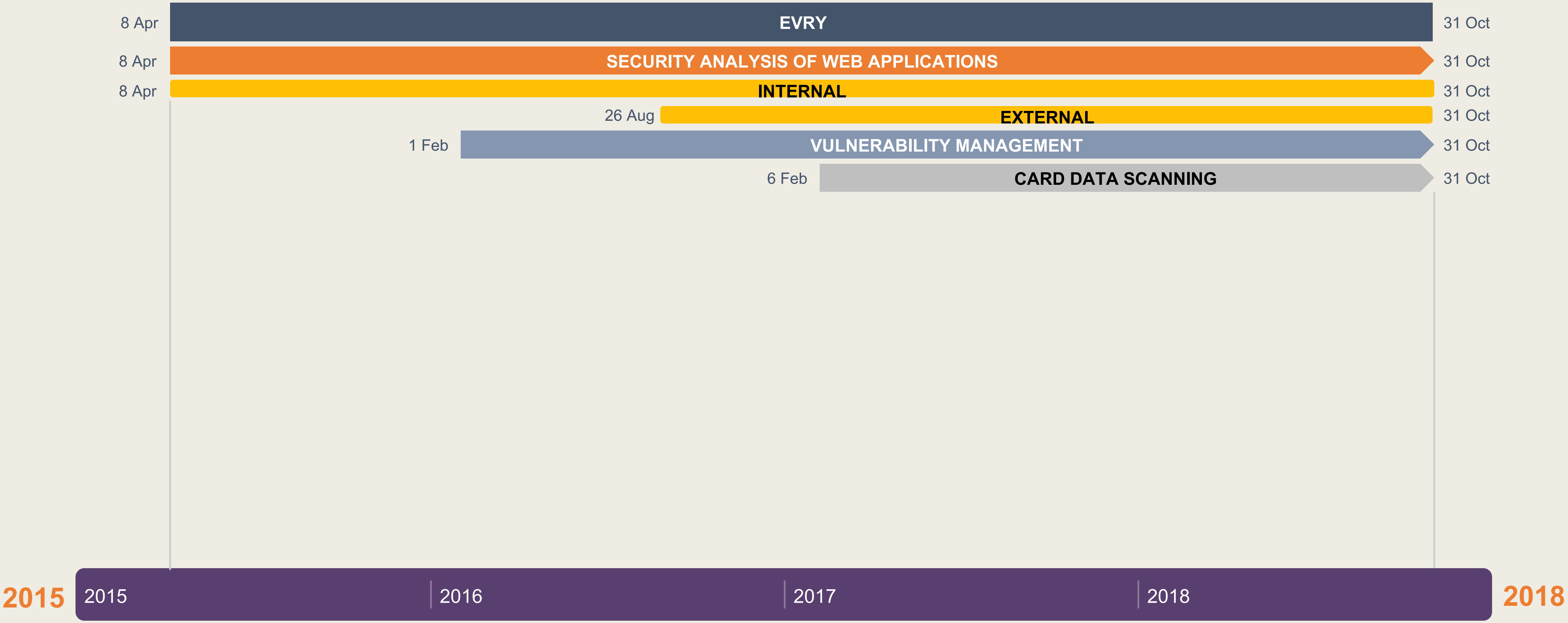
Target Types

dropbox	11,128,089
file	4,956,635
memory	10,576

File Formats

ZIP Archive	71,533
Microsoft Office Document	71,050
Microsoft Access Database	68,798
MIME Email	9,487
Adobe Portable Document	6,940
Outlook Mail Database	4,239
JPG Image	750
SQLite Database	582
DBase Database	572
7Zip intermediate stream	164
UNIX Tape Archive	148
GZip Archive	103
WAV Media	49
Outlook Express Database	39

Live in EVRY



8 Apr EVRY 31 Oct

8 Apr SECURITY ANALYSIS OF WEB APPLICATIONS 31 Oct

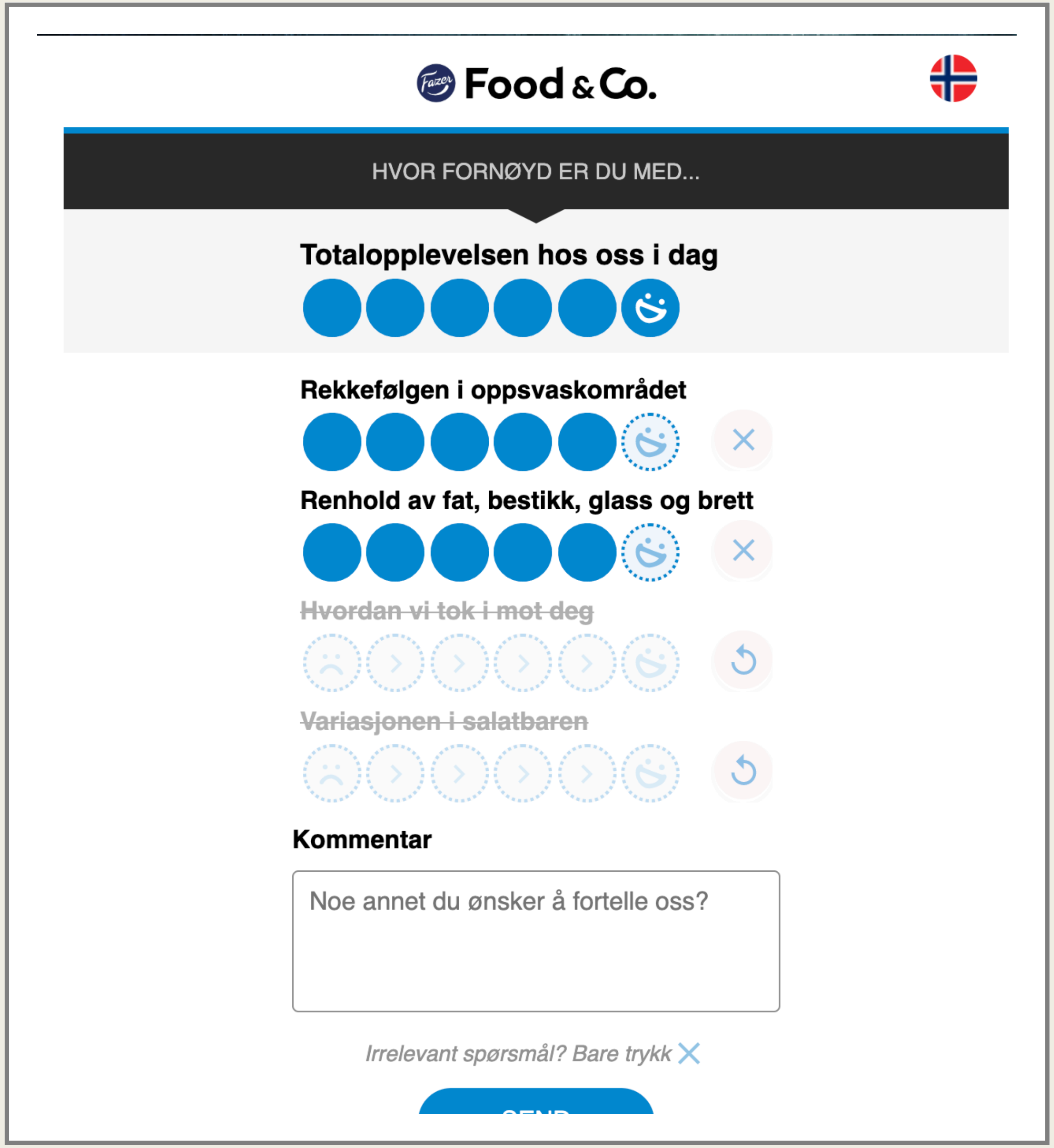
8 Apr INTERNAL 31 Oct

26 Aug EXTERNAL 31 Oct

1 Feb VULNERABILITY MANAGEMENT 31 Oct

6 Feb CARD DATA SCANNING 31 Oct

2015 2015 2016 2017 2018 2018



Food & Co.

HVOR FORNØYD ER DU MED...

Totalopplevelsen hos oss i dag

Rekkefølgen i oppsvaskområdet

Renhold av fat, bestikk, glass og brett

~~Hvordan vi tok i mot deg~~

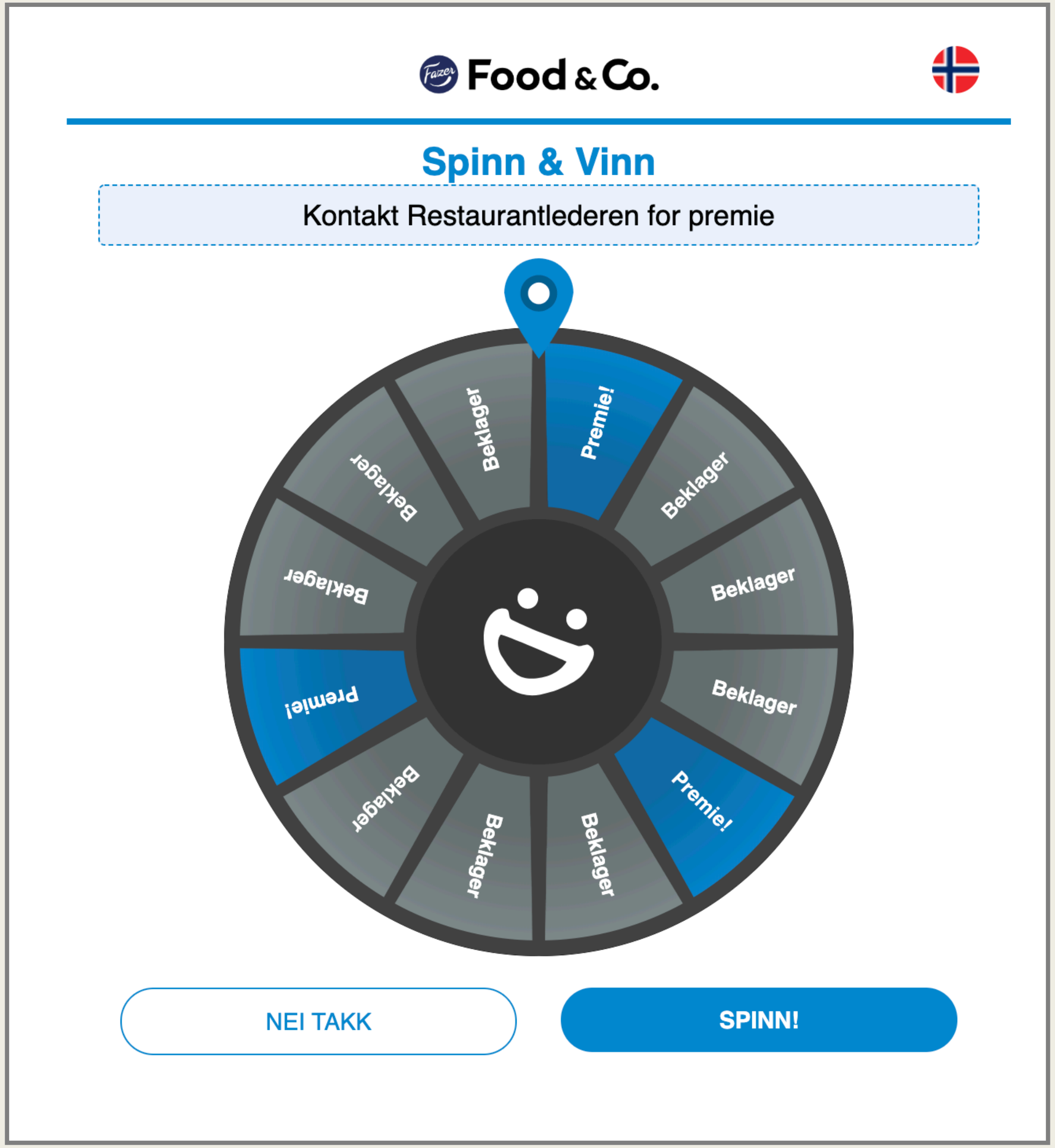
~~Variasjonen i salatbaren~~

Kommentar

Noe annet du ønsker å fortelle oss?

Irrelevant spørsmål? Bare trykk ✕

SEND



Food & Co.

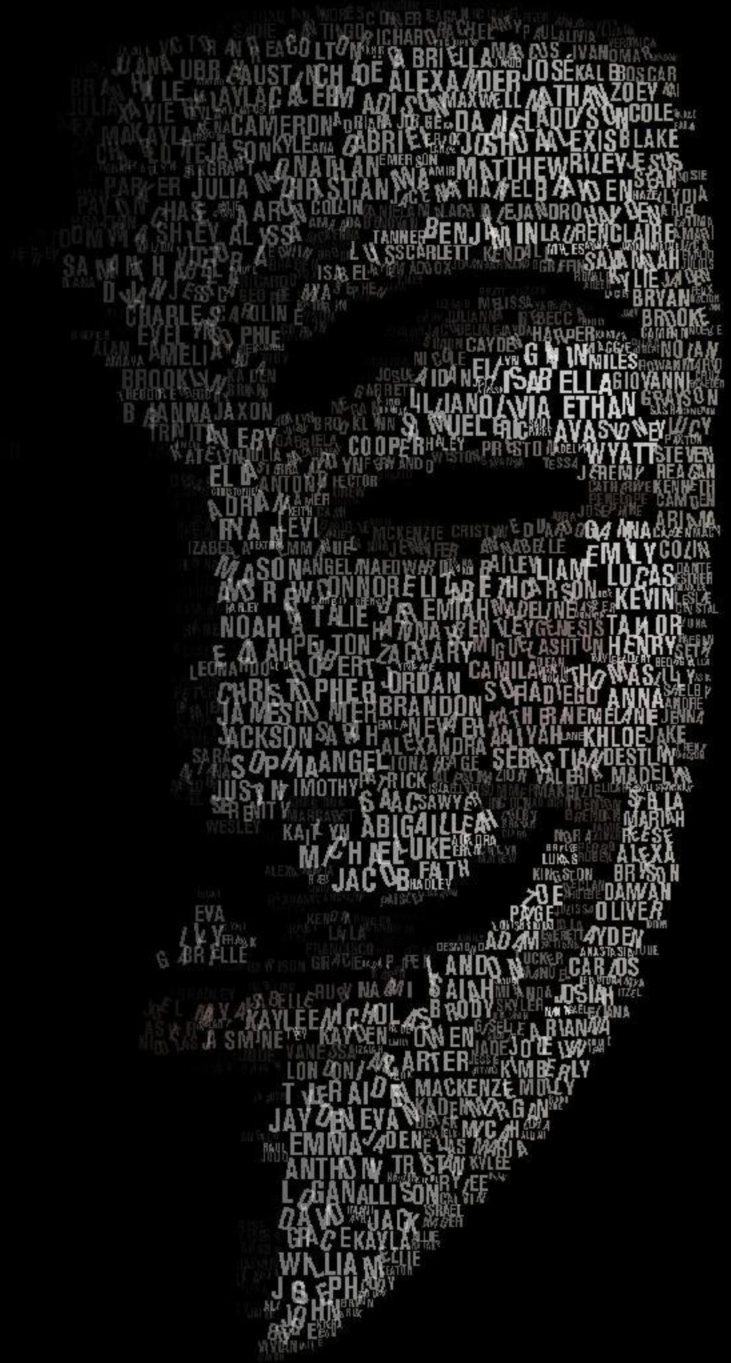
Spinn & Vinn

Kontakt Restaurantlederen for premie

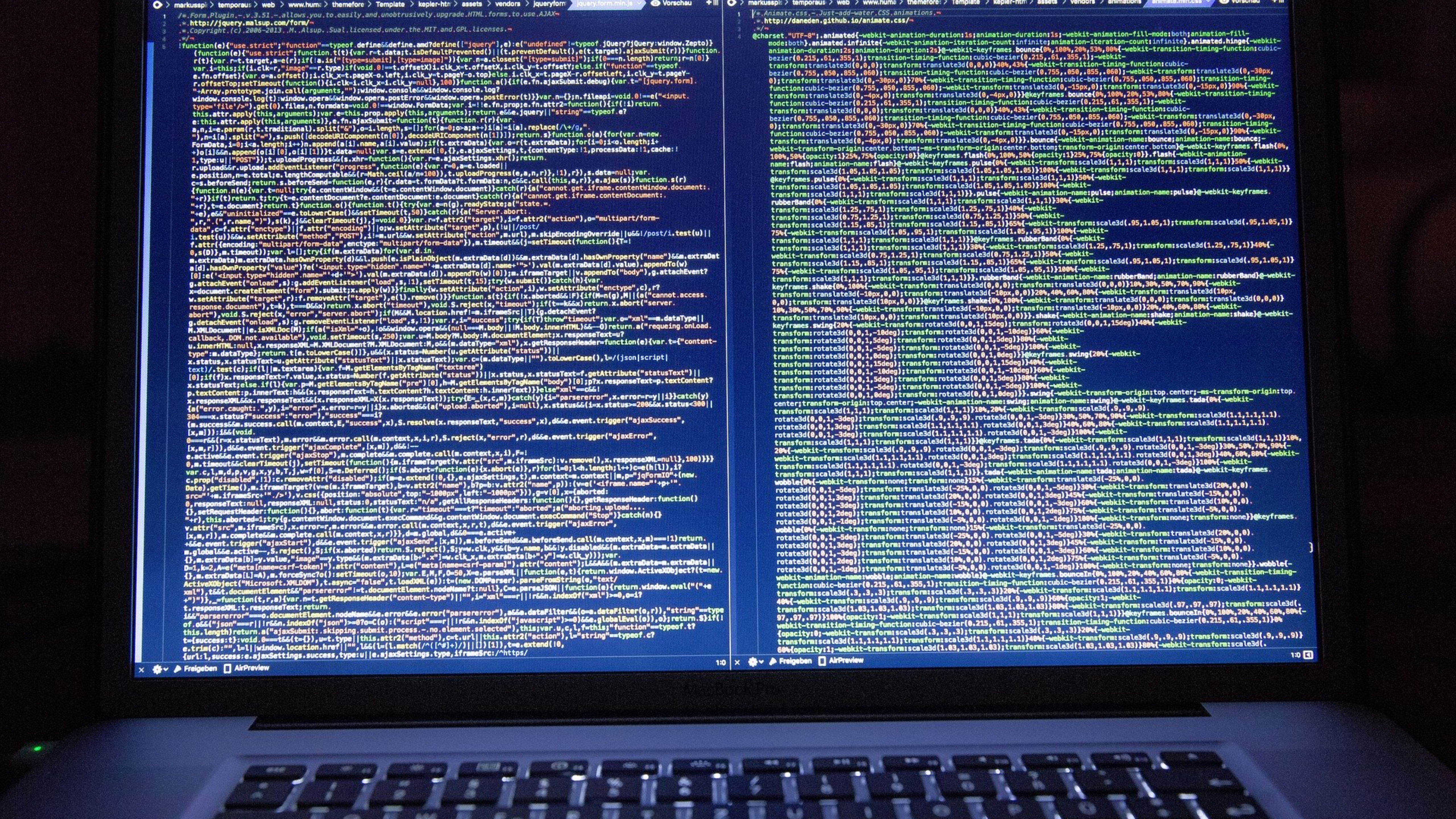
NEI TAKK

SPINN!

CYBER
SECURITY
dark web
corporations
servers
internet
wikileaks
backdoor
remote administration tools
SSL
government
cross site scripting
information technology
privacy
trojan
bitcoin
porn
adwares
root
data
spoofing
data dump
keylogger
antivirus
blackhat
whitehat
database
social engineering
financial institutions
denial of service
cyberspace
anonymous
hackers
firewall
worms
script kids
malwares
distributed denial of service
defacement
encryption
world wide web
surveillance
stuxnet
warez
access
activism


RICHARD
ALEXANDER
JOSE
ZOEY
MAXWELL
COLE
CAMERON
ALEXIS
BLAKE
MATTHEW
JULIA
ALYSSA
BENJAMIN
CLAIRE
SAMANTHA
BRYAN
CHARLES
BROOKE
NOLAN
MILES
ISABELLA
GIOVANNI
BROOKLYN
JAXON
ETHAN
GRAYSON
COOPER
WYATT
STEVEN
EMILY
COLIN
LUCAS
MASON
KEVIN
NOAH
HENRY
BRANDON
ANNA
JACKSON
KHLOE
JAKE
SEBASTIAN
MADELYN
ANGEL
TIMOTHY
JUSTIN
WESLEY
ABIGAIL
MARIAH
REESE
ALEXA
JACOB
BRYSON
DAMIAN
PAIGE
OLIVER
EVA
ADAM
AYDEN
LANDON
CARLOS
ISAIAH
JOSIAH
KAYLEE
NICHOLAS
BRODY
JASMINE
CARTER
KIMBERLY
MACKENZIE
JAYDEN
EMMA
ANTHONY
TRISTAN
LOGAN
ALLISON
DAVID
JACK
GRACE
KAYLA
WILLIAM
JOSEPH
JOHN

HACKED



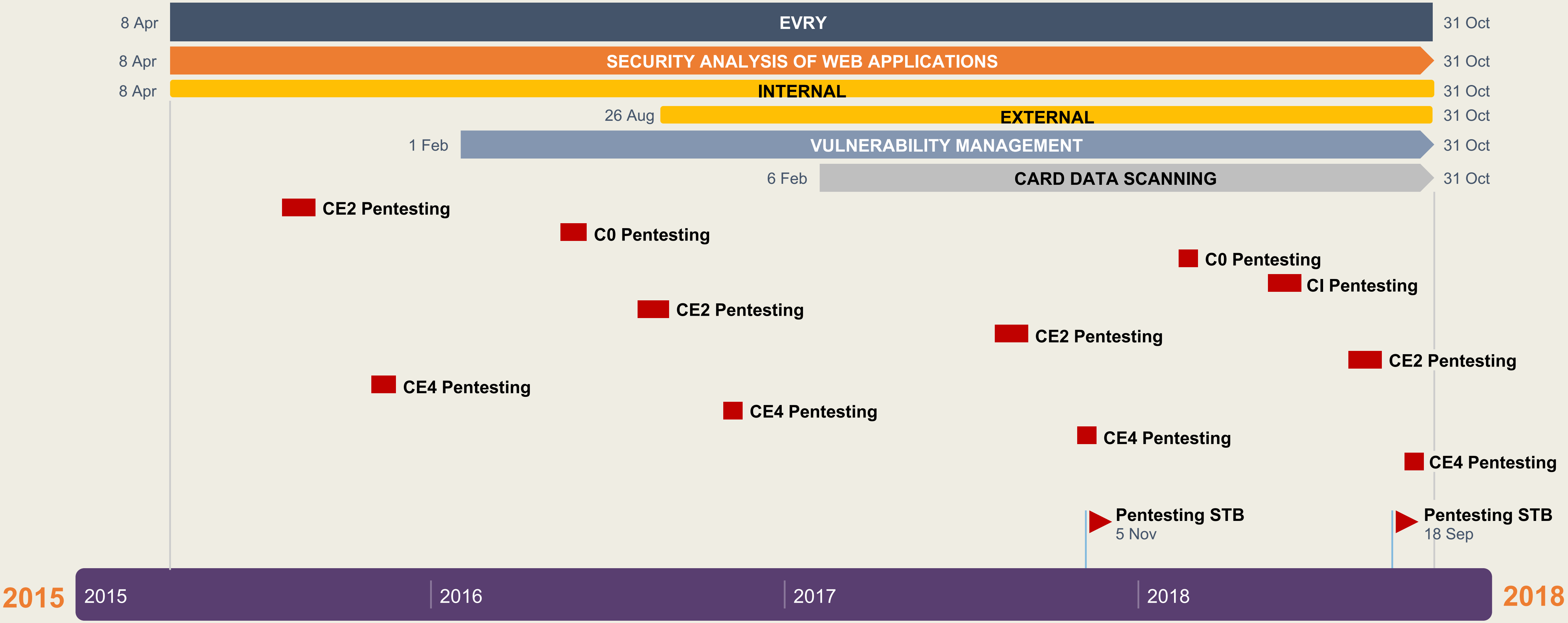
```
/*.Form.Plugin.-.v.3.51.-.allows.you.to.easily.and.unobtrusively.upgrade.HTML.forms.to.use.AJAX
 *.http://jquery.malsup.com/form/
 *.Copyright.(c).2006-2013..M..Alsup..Dual.licensed.under.the.MIT.and.GPL.licenses.
 */
!function(e){"use.strict";"function"==typeof.define&&define.amd?define(["jquery"],e):e("undefined"!=typeof.jQuery?jQuery:window.Zepto)}
```

```
/*.Animate.css.-.Just-add-water.CSS.animations
 *.http://daneden.github.io/animate.css/
 */
@charset."UTF-8";.animated{-webkit-animation-duration:1s;animation-duration:1s;-webkit-animation-fill-mode:both;animation-fill-mode:both}
```

markusspi › temporaus › web › www.hum › themefore › Template › kepler-htn › assets › vendors › jqueryform › jquery.form.min.js
Vorschau
Freigeben
AirPreview
1:0
markusspi › temporaus › web › www.hum › themefore › Template › kepler-htm › assets › vendors › animations › animate.min.css
Vorschau
Freigeben
AirPreview
1:0

SUCCESS

Live in EVRY


8 Apr
EVRY
31 Oct
8 Apr
SECURITY ANALYSIS OF WEB APPLICATIONS
31 Oct
8 Apr
INTERNAL
31 Oct
26 Aug
EXTERNAL
31 Oct
1 Feb
VULNERABILITY MANAGEMENT
31 Oct
6 Feb
CARD DATA SCANNING
31 Oct
CE2 Pentesting
C0 Pentesting
C0 Pentesting
CI Pentesting
CE2 Pentesting
CE2 Pentesting
CE2 Pentesting
CE4 Pentesting
CE4 Pentesting
CE4 Pentesting
CE4 Pentesting
Pentesting STB
5 Nov
Pentesting STB
18 Sep
2015
2015
2016
2017
2018
2018

E|CES™

EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST

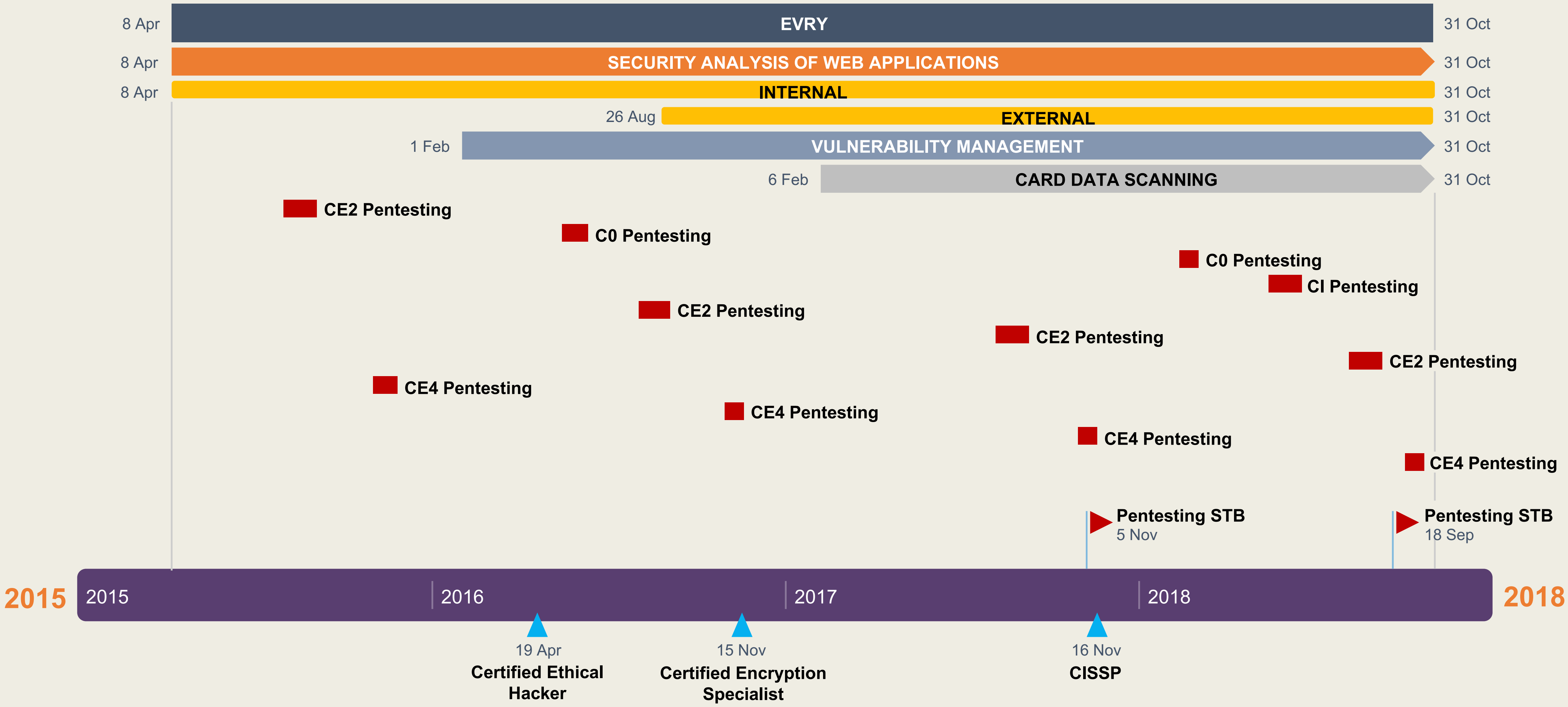
C|EH™

Certified | Ethical Hacker

CISSP®

CERTIFICATIONS

Live in EVRY

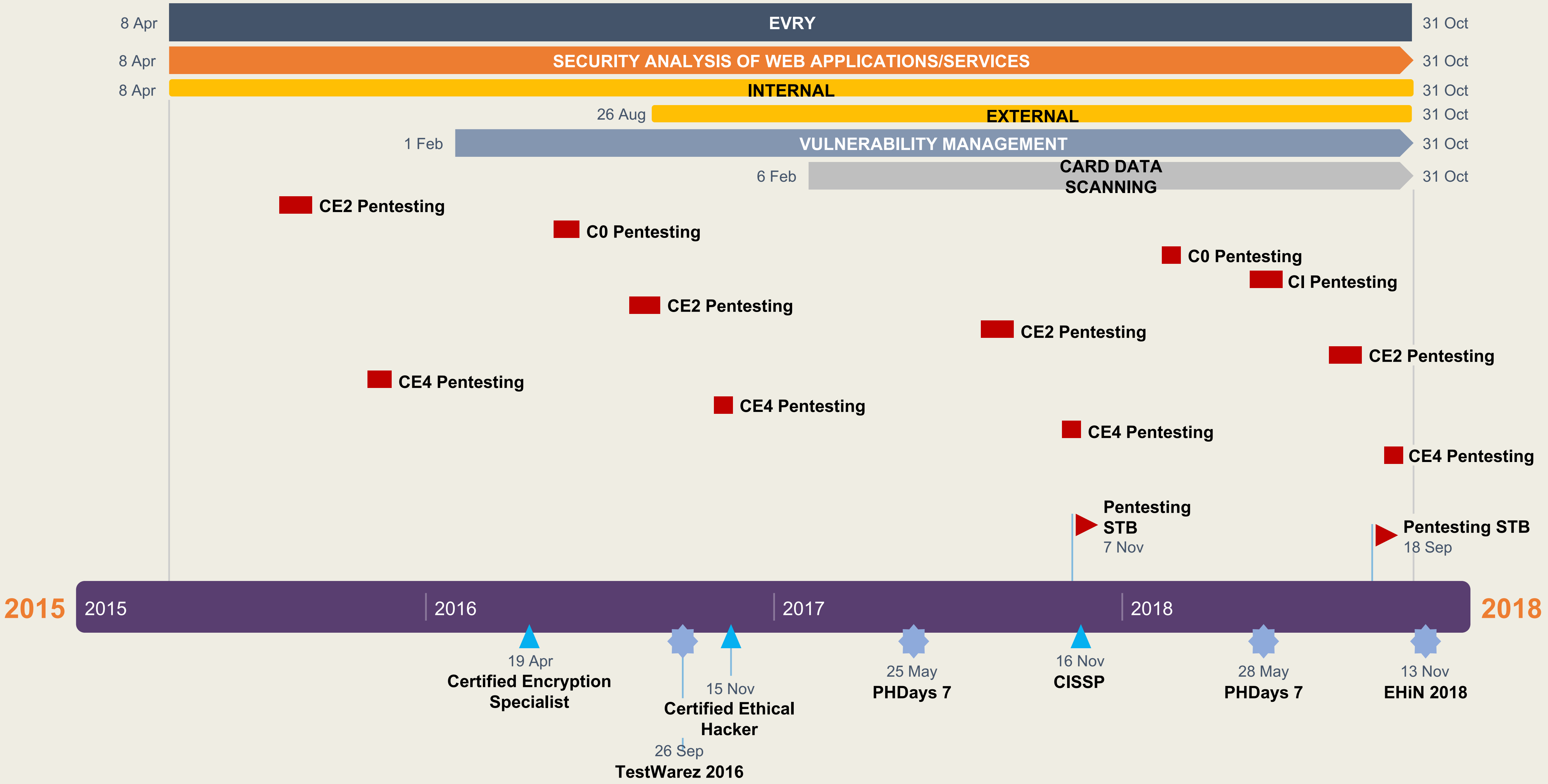


8 Apr
EVRY
31 Oct
8 Apr
SECURITY ANALYSIS OF WEB APPLICATIONS
31 Oct
8 Apr
INTERNAL
31 Oct
26 Aug
EXTERNAL
31 Oct
1 Feb
VULNERABILITY MANAGEMENT
31 Oct
6 Feb
CARD DATA SCANNING
31 Oct
CE2 Pentesting
C0 Pentesting
C0 Pentesting
CI Pentesting
CE2 Pentesting
CE2 Pentesting
CE2 Pentesting
CE4 Pentesting
CE4 Pentesting
CE4 Pentesting
CE4 Pentesting
Pentesting STB
5 Nov
Pentesting STB
18 Sep
2015
2015
2016
2017
2018
2018
19 Apr
Certified Ethical Hacker
15 Nov
Certified Encryption Specialist
16 Nov
CISSP

Talks

- EHiN 2018
  Kan krypto gjøre at hvor data lagres blir uvesentlig?
- NDC Oslo 2018
  Getting benefits of OWASP ASVS at initial phases
- PHDays 7
  Jumping from Tenable's SecurityCenter CV to production environments
- TestWarez 2016
  OWASP ASVS for NFTaaS in Financial Services

Live in EVRY



8 Apr EVRY 31 Oct

8 Apr SECURITY ANALYSIS OF WEB APPLICATIONS/SERVICES 31 Oct

8 Apr INTERNAL 31 Oct

26 Aug EXTERNAL 31 Oct

1 Feb VULNERABILITY MANAGEMENT 31 Oct

6 Feb CARD DATA SCANNING 31 Oct

CE2 Pentesting

C0 Pentesting

C0 Pentesting

CI Pentesting

CE2 Pentesting

CE2 Pentesting

CE2 Pentesting

CE4 Pentesting

CE4 Pentesting

CE4 Pentesting

CE4 Pentesting

Pentesting STB
7 Nov

Pentesting STB
18 Sep

2015 2015 2016 2017 2018 2018

19 Apr
Certified Encryption Specialist

15 Nov
Certified Ethical Hacker

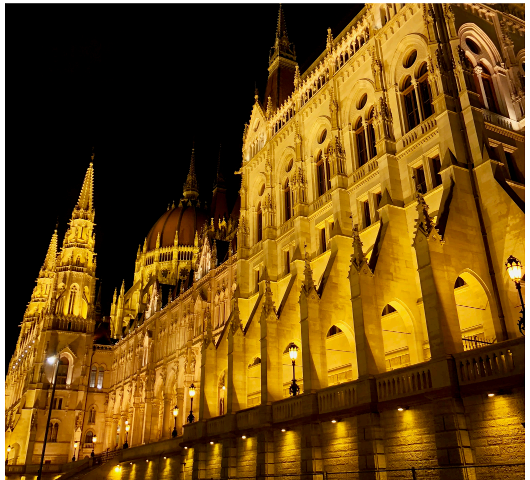
26 Sep
TestWarez 2016

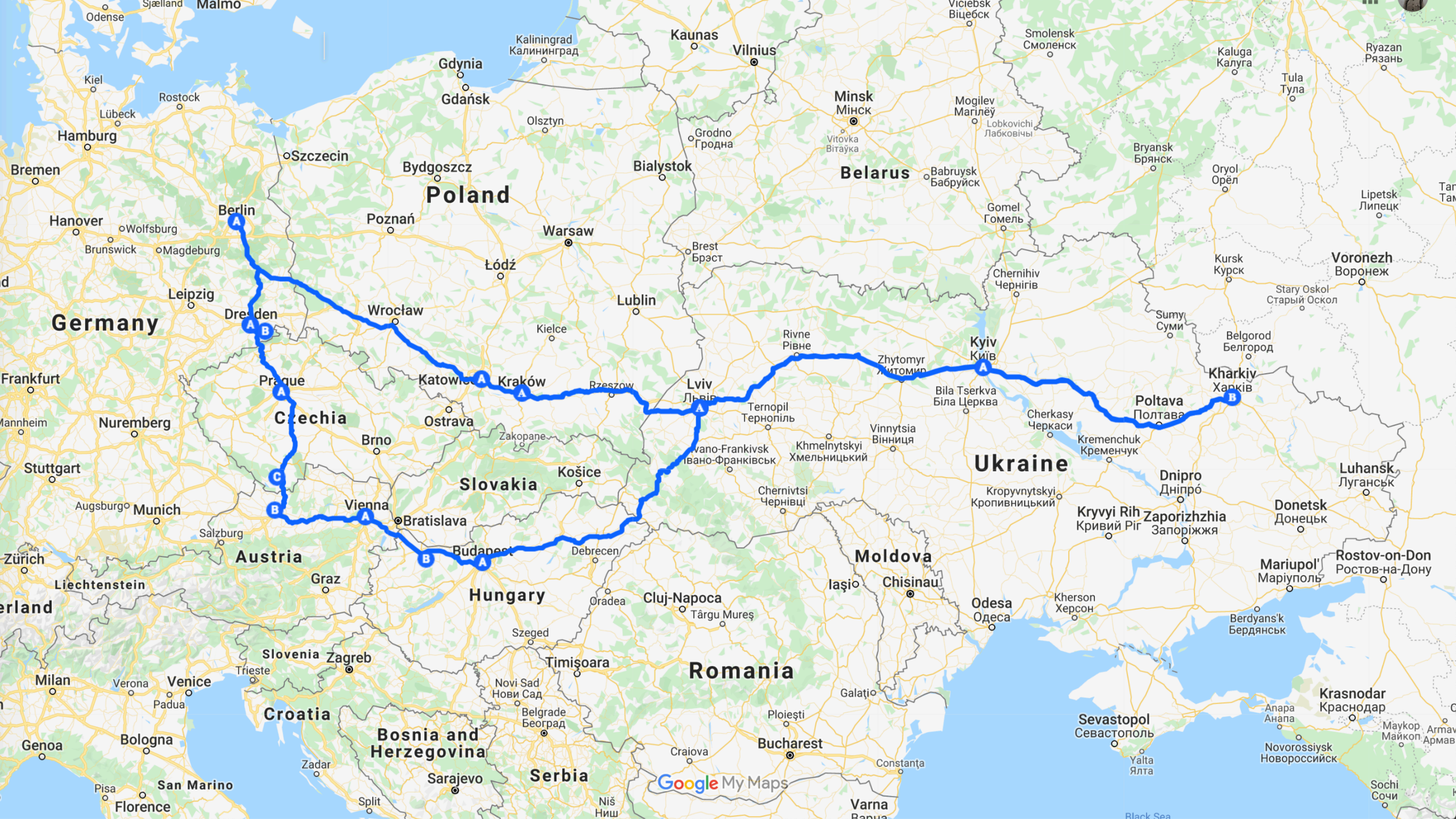
25 May
PHDays 7

16 Nov
CISSP

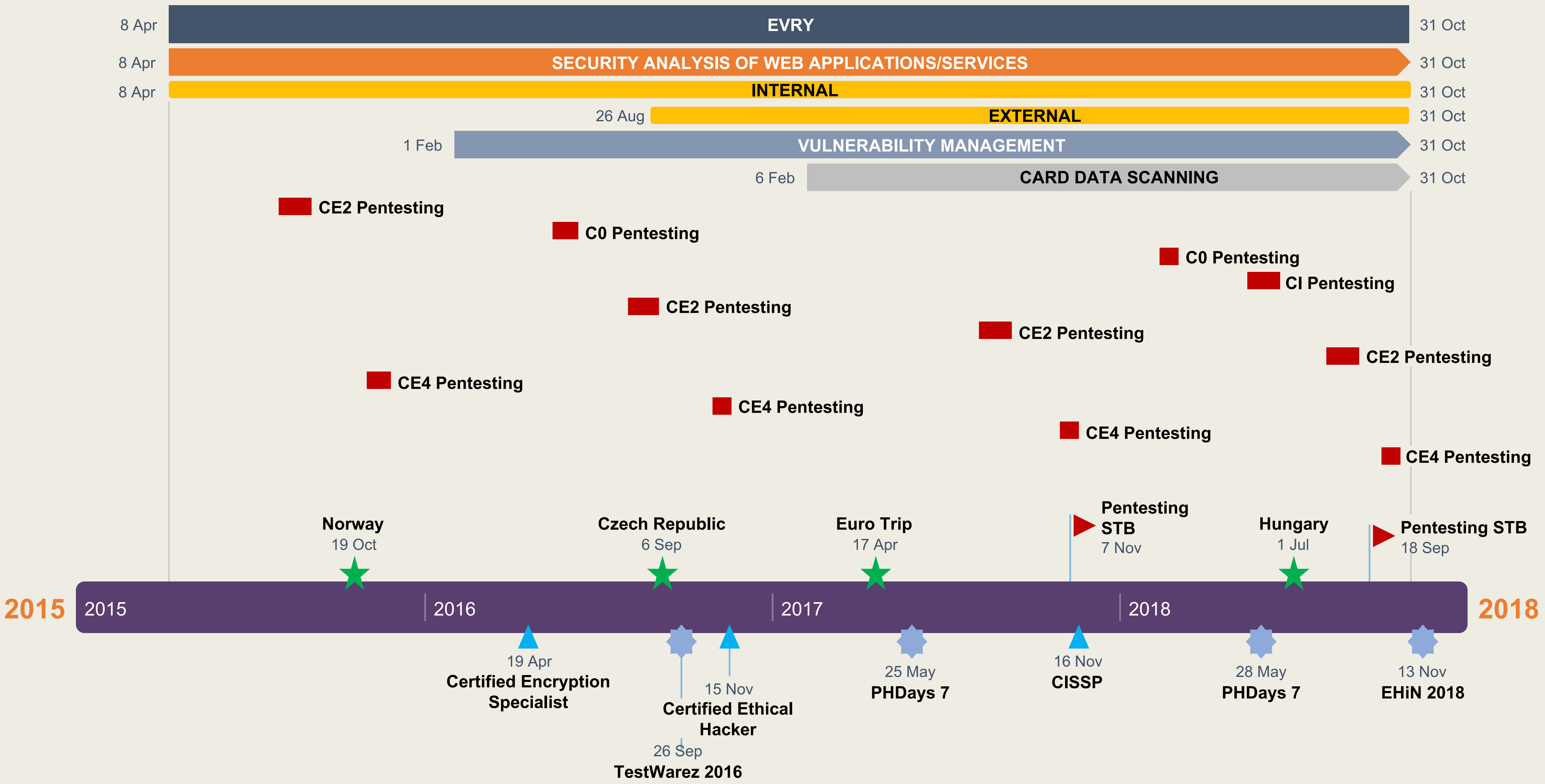
28 May
PHDays 7

13 Nov
EHiN 2018




Odense
Sjælland
Malmö
Kaliningrad
Калининград
Kaunas
Vilnius
Viciebsk
Віцебск
Smolensk
Смоленск
Ryazan
Рязань
Kaluga
Калуга
Tula
Тула
Gdynia
Gdańsk
Kiel
Rostock
Lübeck
Hamburg
Olsztyn
Grodno
Гродна
Minsk
Мінск
Vitovka
Вітаўка
Mogilev
Магілёў
Lobkovichi
Лабковічы
Bryansk
Брянск
Oryol
Орёл
Bremen
Szczecin
Bydgoszcz
Bialystok
Belarus
Babruysk
Бабруйск
Lipetsk
Липецк
Tam
Там
Poland
Berlin
Hanover
Wolfsburg
Brunswick
Magdeburg
Poznań
Warsaw
Brest
Брэст
Gomel
Гомель
Łódź
Kursk
Курск
Voronezh
Воронеж
Chernihiv
Чернігів
Stary Oskol
Старый Оскол
Leipzig
Lublin
Germany
Dresden
Wrocław
Kielce
Sumy
Суми
Rivne
Рівне
Belgorod
Белгород
Kyiv
Київ
Zhytomyr
Житомир
Kharkiv
Харків
Frankfurt
Prague
Katowice
Kraków
Rzeszów
Lviv
Львів
Ternopil
Тернопіль
Bila Tserkva
Біла Церква
Poltava
Полтава
Cherkasy
Черкаси
Mannheim
Czechia
Ostrava
Nuremberg
Zakopane
Vinnytsia
Вінниця
Kremenchuk
Кременчук
Brno
Khmelnytskyi
Хмельницький
Ivano-Frankivsk
Івано-Франківськ
Stuttgart
Slovakia
Košice
Ukraine
Luhansk
Луганськ
Dnipro
Дніпро
Chernivtsi
Чернівці
Kropyvnytskyi
Кропивницький
Vienna
Bratislava
Augsburg
Munich
Donetsk
Донецьк
Kryvyi Rih
Кривий Ріг
Zaporizhzhia
Запоріжжя
Salzburg
Budapest
Debrecen
Moldova
Austria
Zürich
Rostov-on-Don
Ростов-на-Дону
Mariupol'
Маріуполь
Liechtenstein
Graz
Chisinau
Iași
Odesa
Одеса
Kherson
Херсон
Hungary
Oradea
Cluj-Napoca
Târgu Mureș
Berdyans'k
Бердянськ
Szeged
Slovenia
Zagreb
Timișoara
Trieste
Milan
Verona
Venice
Padua
Novi Sad
Нови Сад
Romania
Galați
Krasnodar
Краснодар
Sevastopol
Севастополь
Anapa
Анапа
Croatia
Belgrade
Београд
Ploiești
Bologna
Genoa
Maykop
Майкоп
Bosnia and Herzegovina
Novorossiysk
Новороссийск
Yalta
Ялта
Bucharest
Zadar
Craiova
Constanța
Serbia
Sarajevo
Pisa
San Marino
Sochi
Сочи
Florence
Split
Niš
Ниш
Varna
Black Sea
Google My Maps
A
B
C

Live in EVRY



8 Apr EVRY 31 Oct

8 Apr SECURITY ANALYSIS OF WEB APPLICATIONS/SERVICES 31 Oct

8 Apr INTERNAL 31 Oct

26 Aug EXTERNAL 31 Oct

1 Feb VULNERABILITY MANAGEMENT 31 Oct

6 Feb CARD DATA SCANNING 31 Oct

CE2 Pentesting

C0 Pentesting

C0 Pentesting

CI Pentesting

CE2 Pentesting

CE2 Pentesting

CE2 Pentesting

CE4 Pentesting

CE4 Pentesting

CE4 Pentesting

CE4 Pentesting

Norway 19 Oct

Czech Republic 6 Sep

Euro Trip 17 Apr

Pentesting STB 7 Nov

Hungary 1 Jul

Pentesting STB 18 Sep

2015 | 2015 | 2016 | 2017 | 2018 | 2018

19 Apr **Certified Encryption Specialist**

26 Sep **TestWarez 2016**

15 Nov **Certified Ethical Hacker**

25 May **PHDays 7**

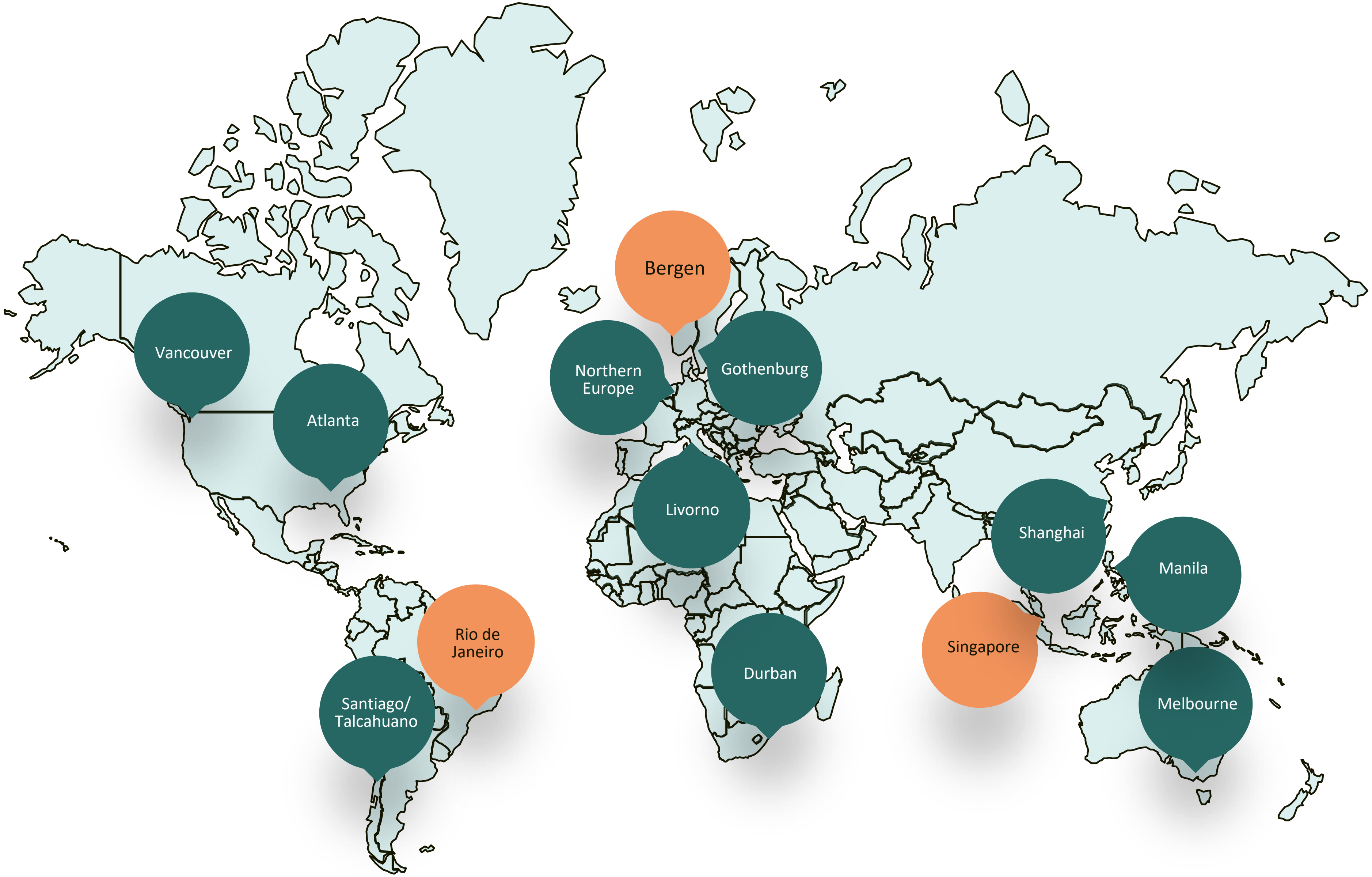
16 Nov **CISSP**

28 May **PHDays 7**

13 Nov **EHiN 2018**

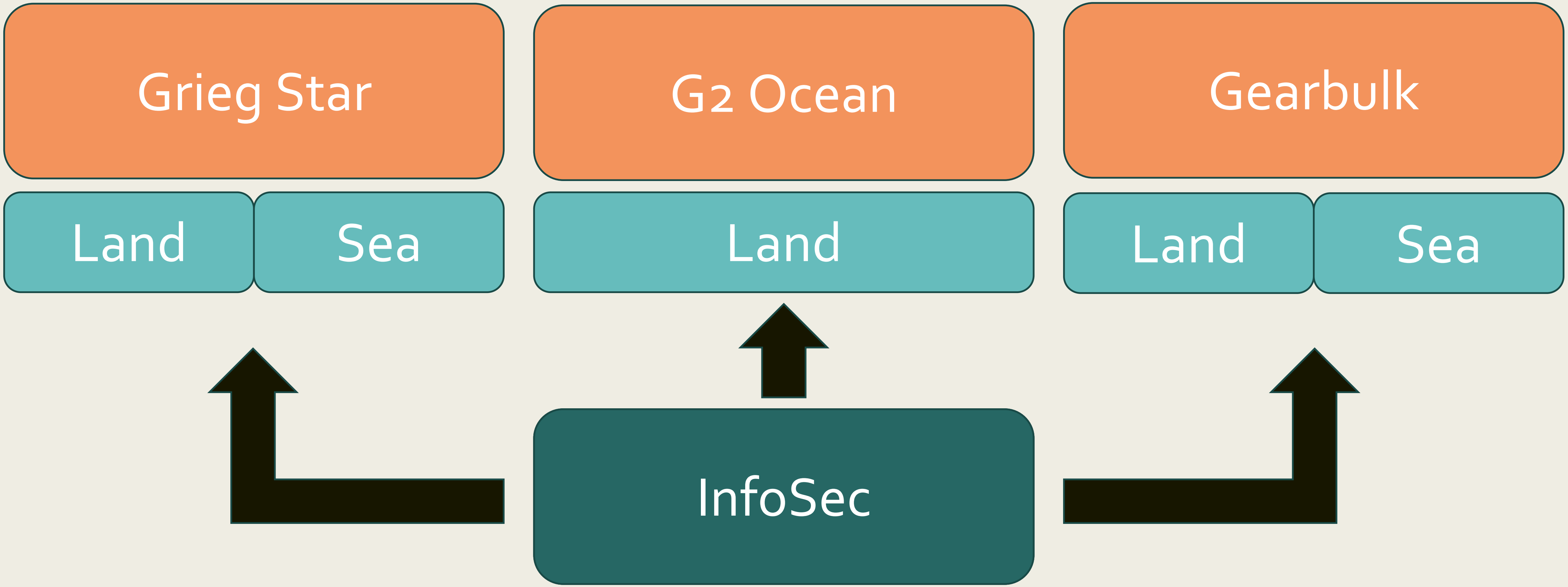
G2 OCEAN

PIONEERING SUSTAINABLE SHIPPING SOLUTIONS


Bergen
Vancouver
Atlanta
Northern Europe
Gothenburg
Livorno
Shanghai
Manila
Rio de Janeiro
Santiago/ Talcahuano
Durban
Singapore
Melbourne

UnITy

What is UnITy?



Grieg Star

Land

Sea

G2 Ocean

Land

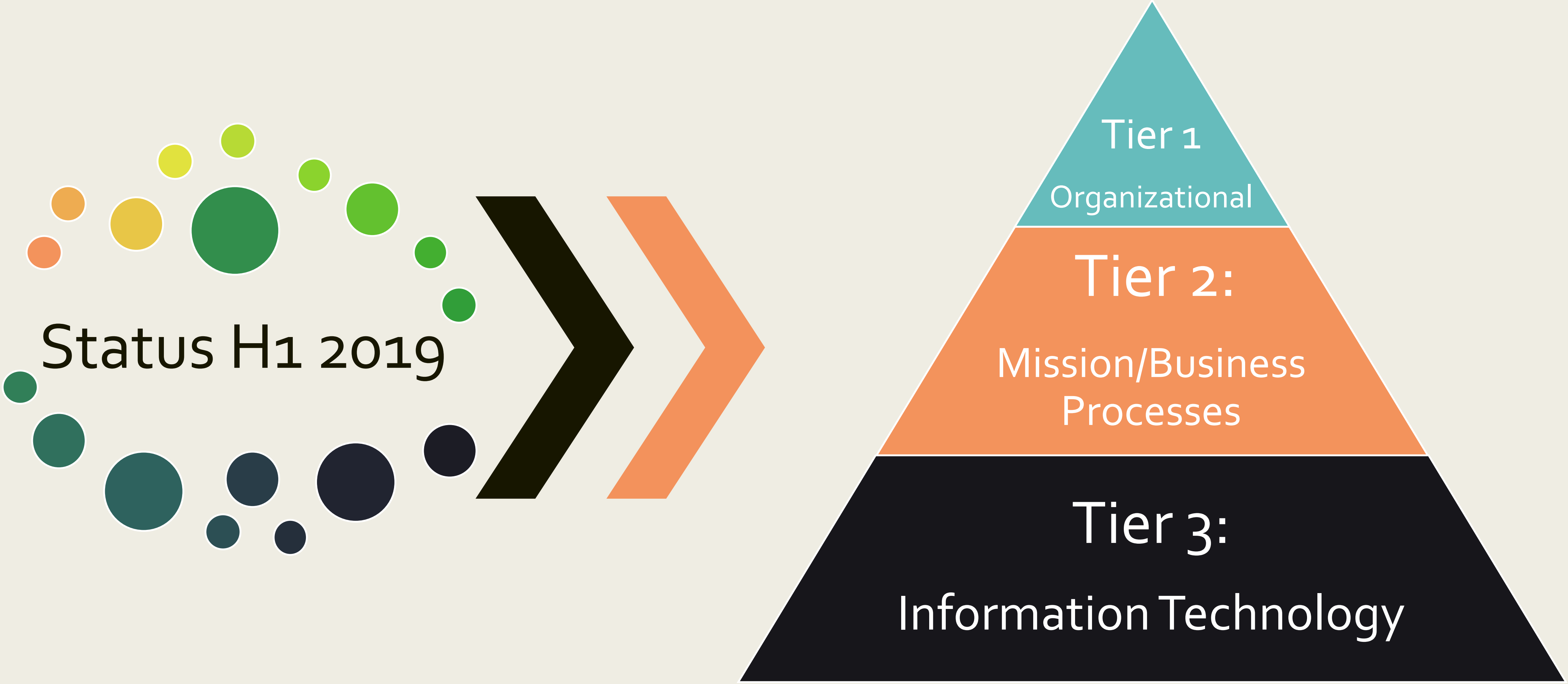
Gearbulk

Land

Sea

InfoSec

Metamorphosis



Status H1 2019

Tier 1

Organizational

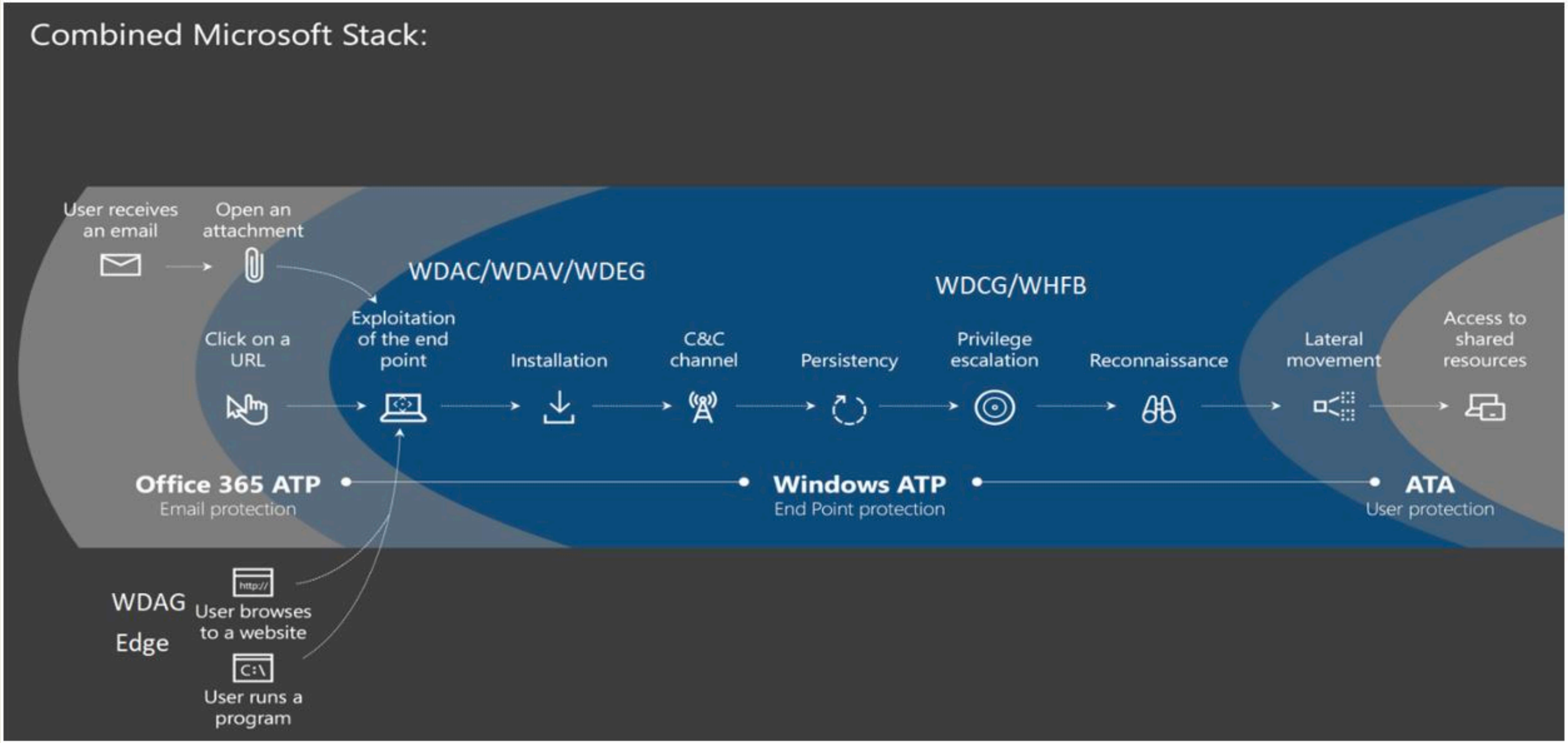
Tier 2:

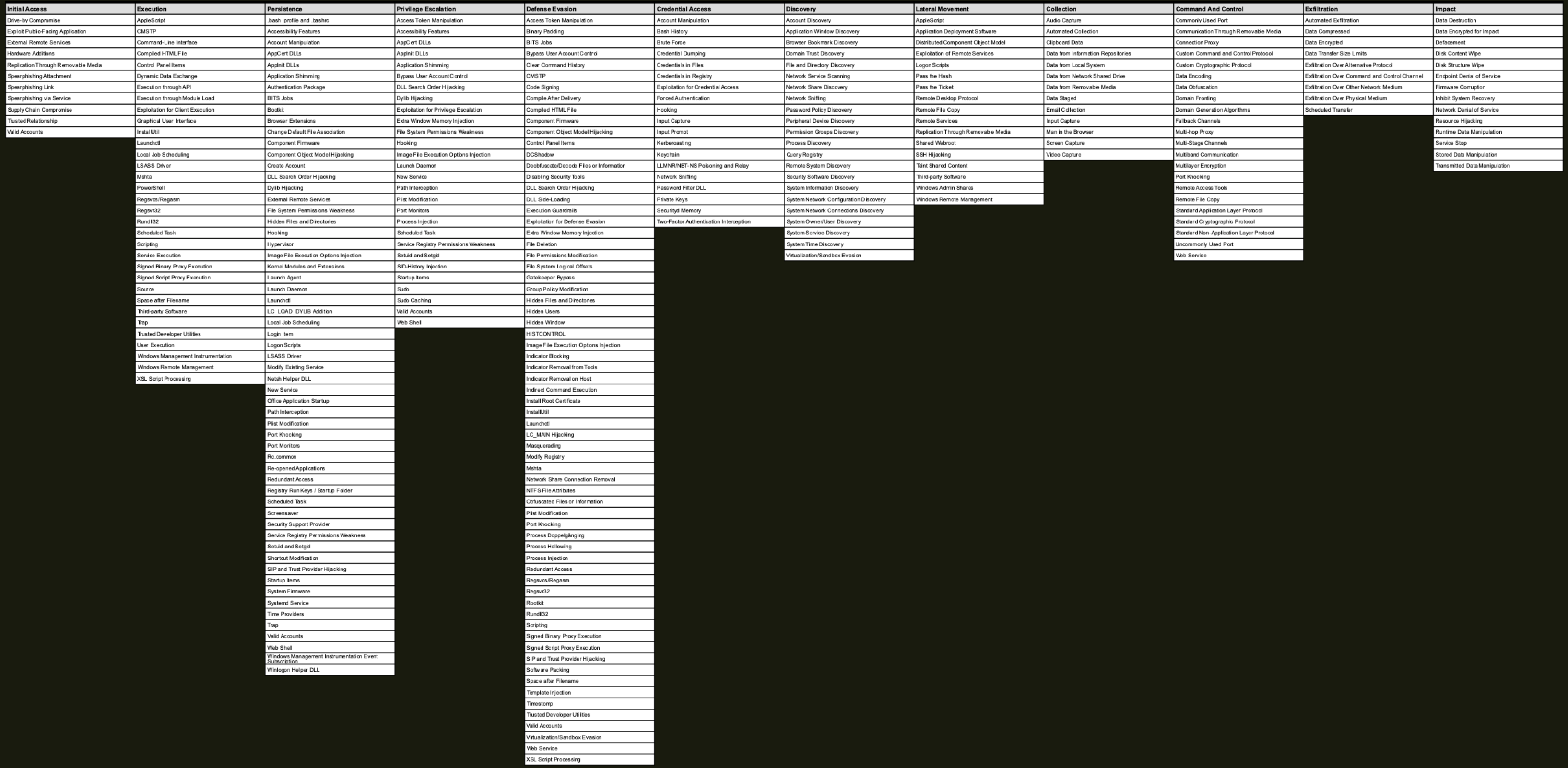
Mission/Business Processes

Tier 3:

Information Technology

The Cyber Kill Chain





Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelgänging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

MITRE ATT&CK

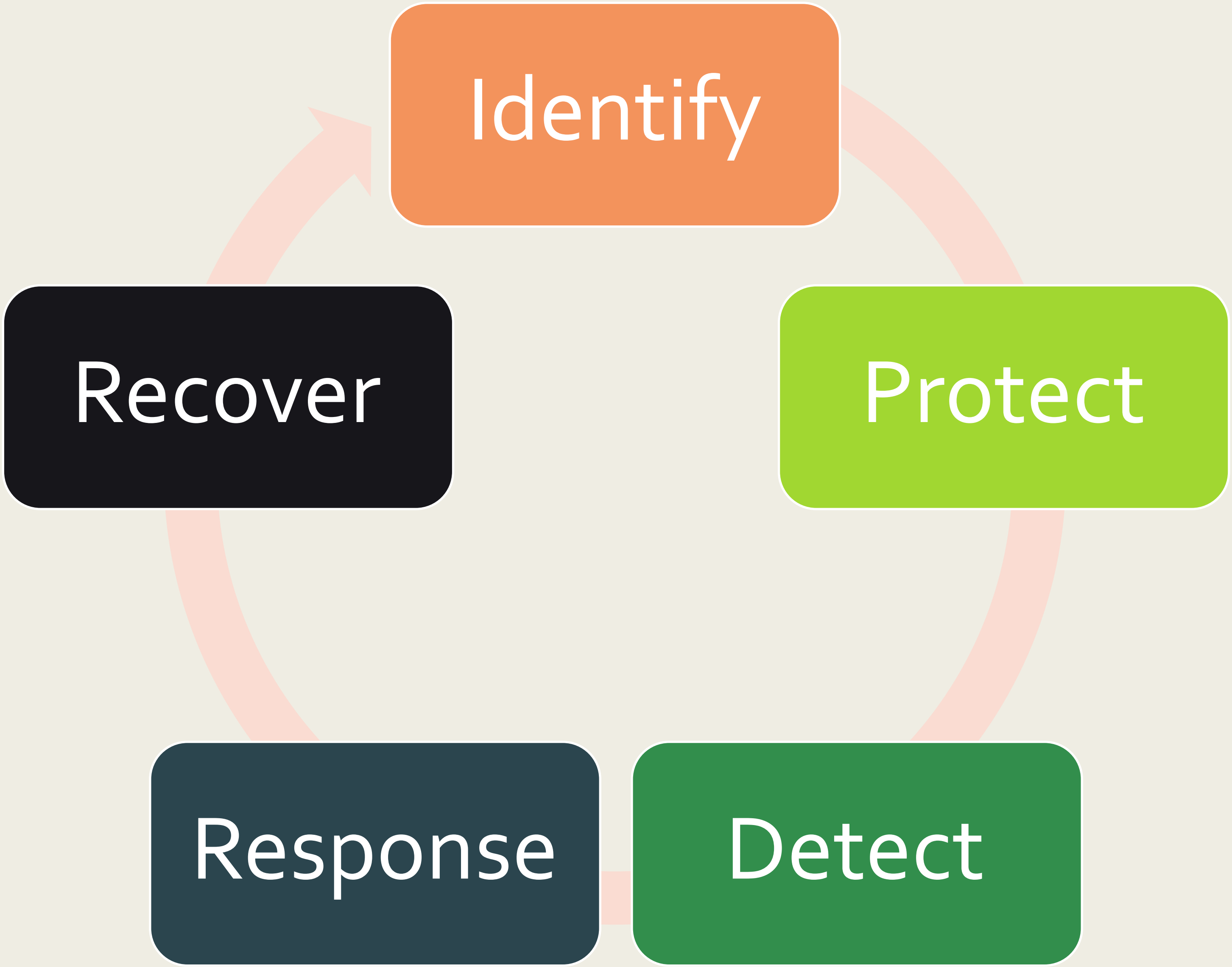
Enterprise Techniques: 244

Mobile Techniques: 67

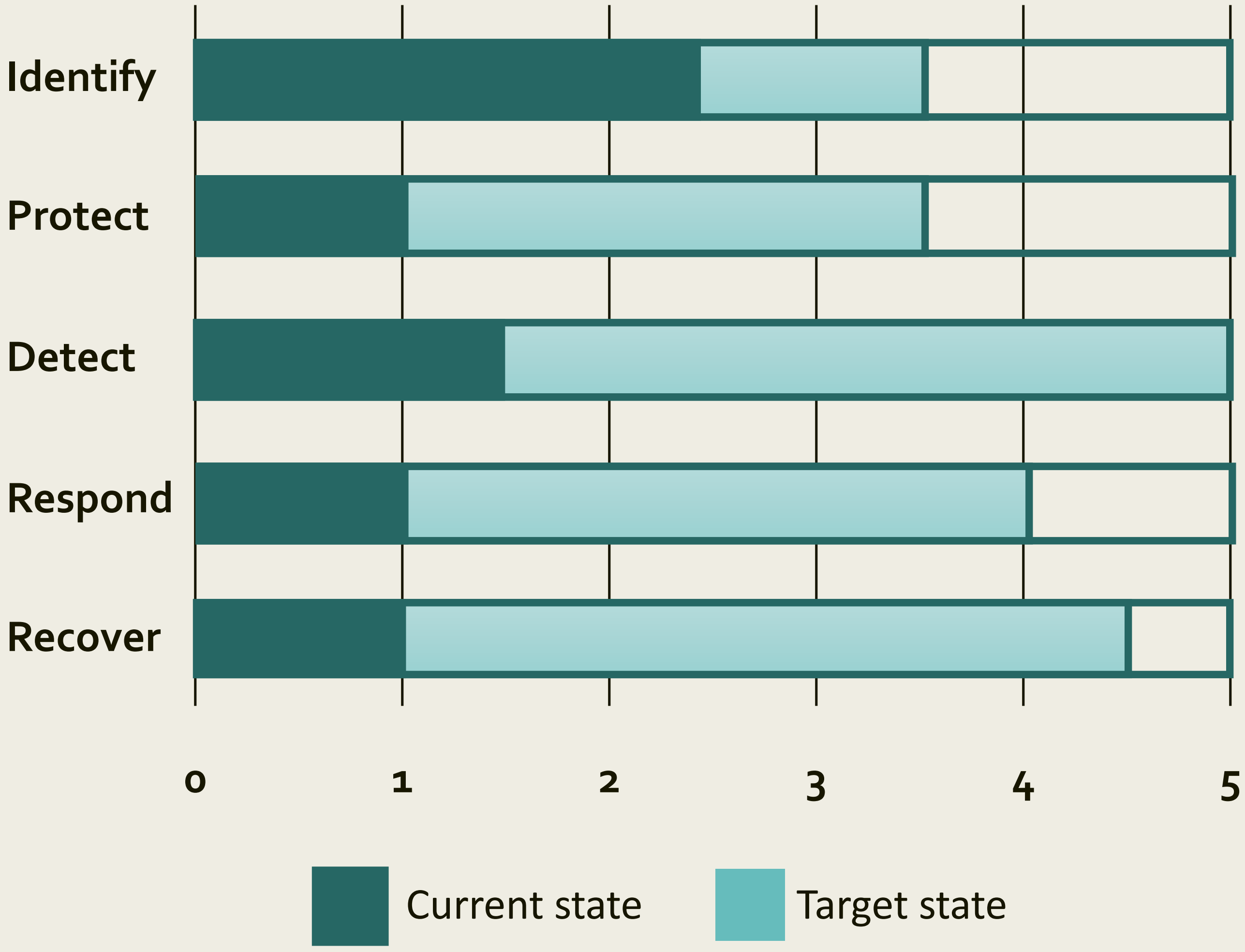
PRE-ATT&CK Techniques: 174

https://mitre-attack.github.io/attack-navigator/enterprise/#

NIST Cybersecurity Framework

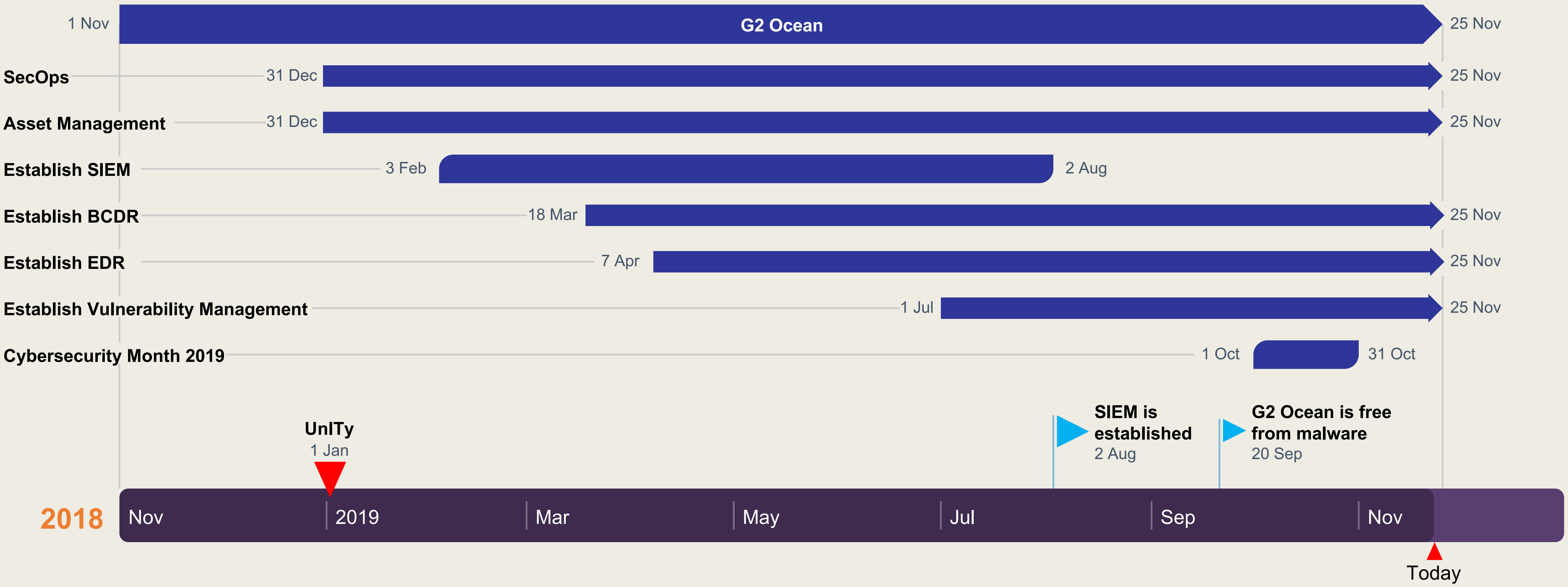


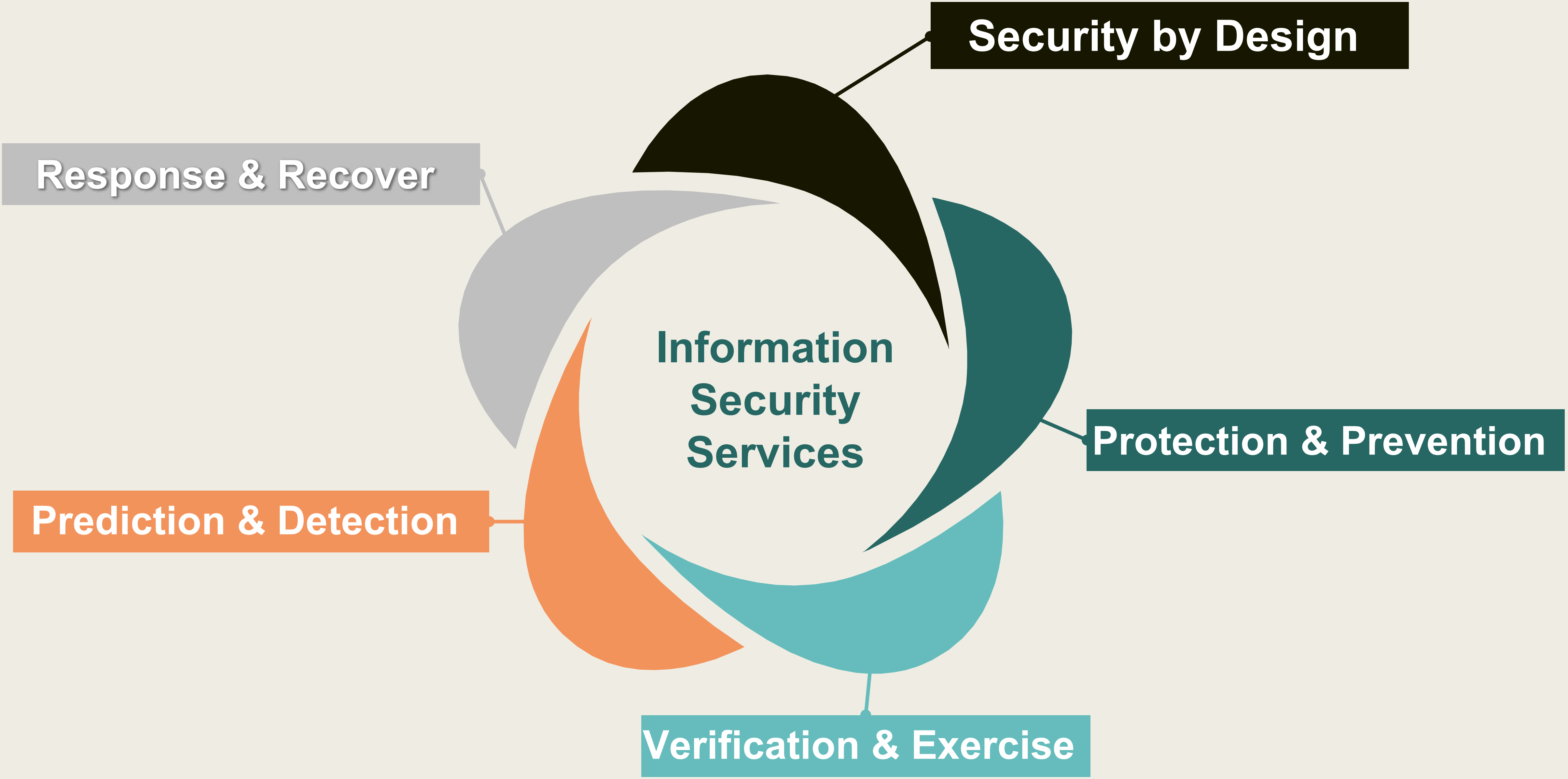
Maturity of Information Security



FUNCTION	CATEGORY	CIS CONTROL
Identify	Asset Management	CIS Control 1, 2
	Business Environment	
	Governance	
	Risk Assessment	CIS Control 3
	Risk Management Strategy	
	Supply Chain Risk Management	
Protect	Identity Management, Authentication, and Access Control	CIS Control 4, 9, 11, 12, 13, 14, 16
	Awareness and Training	CIS Control 4, 17
	Data Security	CIS Control 1, 2, 13, 14, 18
	Information Protection Processes and Procedures	CIS Control 3, 5, 7, 10, 11
	Maintenance	CIS Control 4, 12
	Protective Technology	CIS Control 4, 6, 8, 11, 13, 14, 16
Detect	Anomalies and Events	CIS Control 6, 9, 12, 19
	Security Continuous Monitoring	CIS Control 3, 8, 19
	Detection Processes	CIS Control 6
Respond	Response Planning	CIS Control 19
	Communications	CIS Control 19
	Analysis	CIS Control 3, 19
	Mitigation	CIS Control 3, 19
	Improvements	CIS Control 19
Recover	Recovery Planning	CIS Control 19
	Improvements	CIS Control 19
	Communications	CIS Control 19

Live in G2 Ocean





Information Security Services

Security by Design

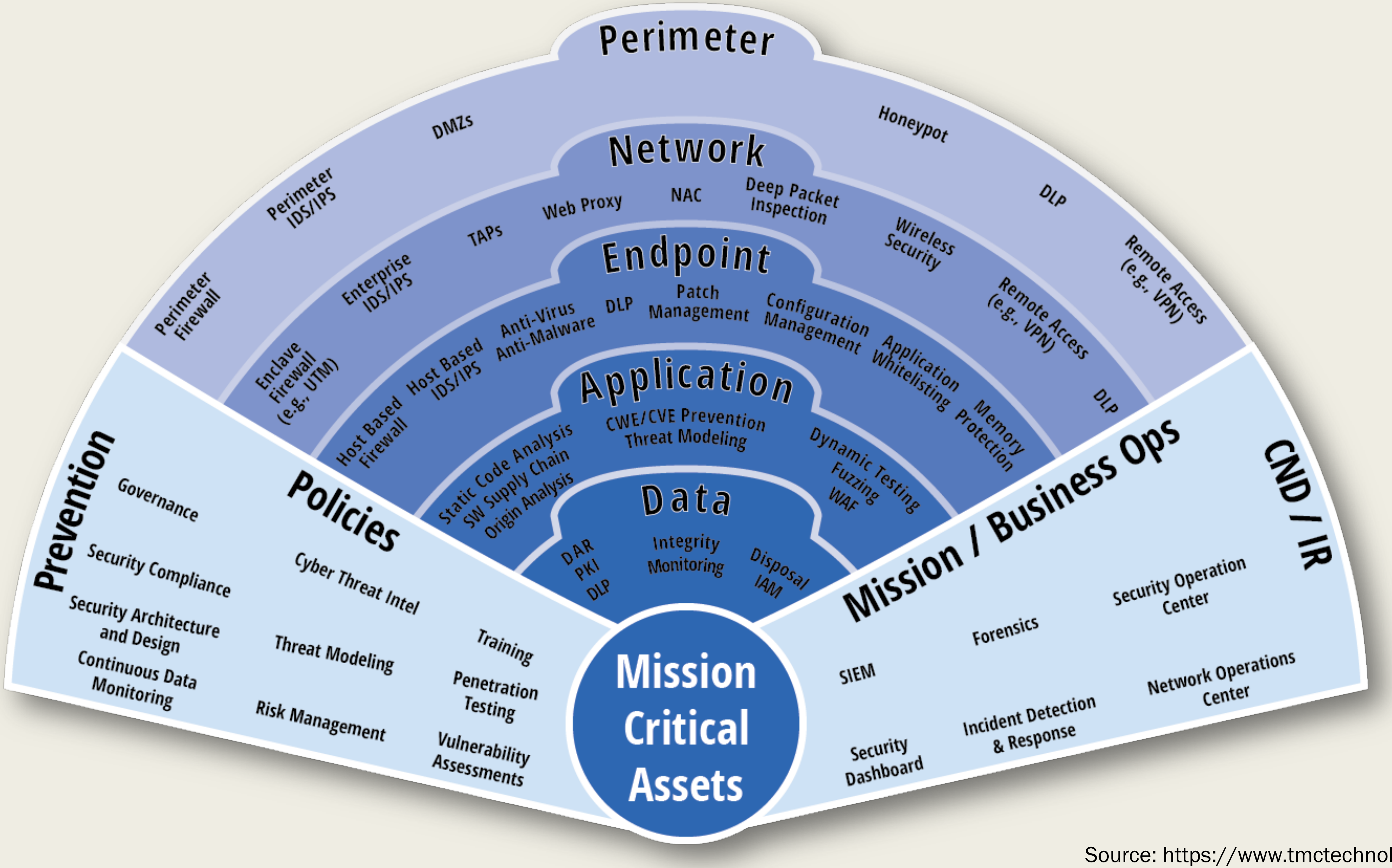
Protection & Prevention

Verification & Exercise

Prediction & Detection

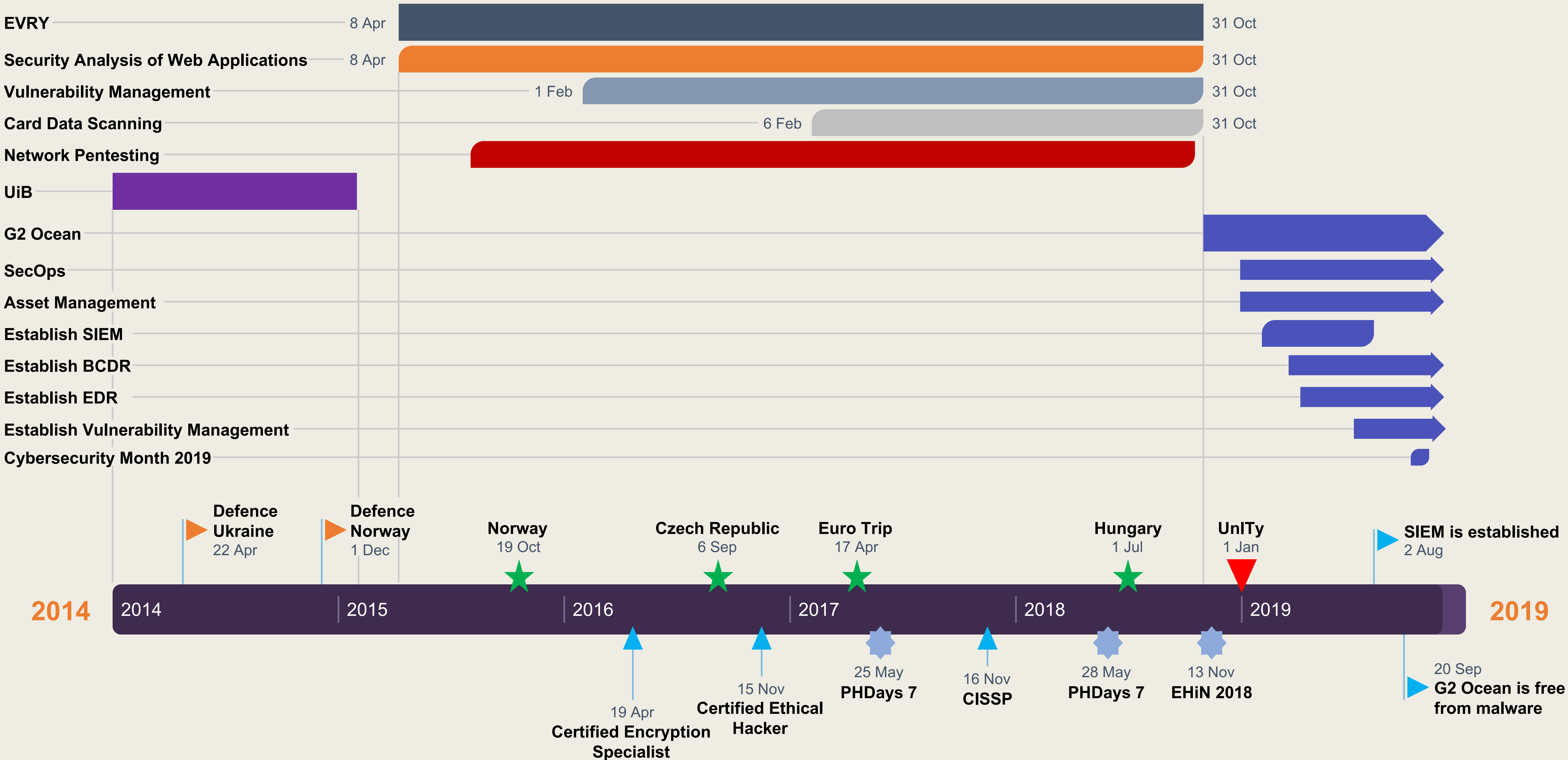
Response & Recover

Layered Security (Defence in Depth)



Source: https://www.tmctechnologies.com/cyber/

5 Years in 40 Minutes



CYBERSCAPE

Q4 2019

Network & Infrastructure Security

Advanced Threat Protection
Barracuda, BLUEHEXAGON, BLUVECTOR, Check Point, cisco, CORSA, FIREEYE, FORTINET, HUAWEI, HYSOLATE, JOESecurity, JUNIPER, lastline, McAfee, Metapacket, mimecast, OPSWAT, paloalto, REVERSING LABS, RESEC, Sasa Software, SONICWALL, SOPHOS, SPAMINA, Symantec, VMRAY, VOTIRO, WatchGuard

NAC
aruba, AUCONET, AXONIUS, cisco, Extreme, FORESCOUT, FORTINET, Genians, NETSHIELD, portnox, Trustwave

SDN
BlackRidge Technology, CERTES, Cybera, Cyxtera, NanoSec, SKYPORT SYSTEMS, TEMPERED, VERSA, zentera, zscaler

DDoS Protection
Akamai, Check Point, CLOUDFLARE, F5, FORTINET, imperva, neustar, NEXUSGUARD, NSFOCUS, ORACLE, SECURE64, StackPath

DNS Security
BLUECAT, cisco, CYREN, efficient iP, Infoblox, neustar, SECURE64, ThreatSTOP, Quad9, VERISIGN

Network Firewall
algosec, CATO NETWORKS, Check Point, cisco, CLAVISTER, endian, FIREMON, FORCEPOINT, FORTINET, Hillstone, HUAWEI, OPAQ, paloalto, SANGFOR, SONICWALL, SOPHOS, STORMSHIELD, tufin, untangle

Deception
ACALVIO, Attivo Networks, CounterCraft, CyberTrap, Cymmetria, Fidelis, illusive, PACKET VIPER, SMOKESCREEN, TRAPX

ICS + OT
APERIO, BAYSHORE, BELDEN, CLAROTY, CRITIFENCE, CyberX, CYBERBIT, DRAGOS, endian, FIRMITAS, FORESCOUT, HALO ANALYTICS, Indegy, dimension, NextNine, NOZOMI, OWL, PAS, PFP, radiflow, Rhebo, SCADAfence, sentryo

Network Analysis & Forensics
AWAKE, BRICATA, CGS, cisco, CloudShark, corelight, CORE, Corvil, DARKTRACE, ExtraHop, Fidelis, Gigamon, GREY CORTEX, IronNet, LUMETA, MixMode, NETSCOUT, paloalto, PERCH, Plixer, SecBI, SS8, utimaco, VECTRA, VERINT

Web Security
Akamai, aurionpro, AUTHENTIC8, Barracuda, CEQUENCE, Check Point, cisco, ContentKeeper, CYREN, DEFIANT, digicert, distil networks, ERICOM, F5, FORCEPOINT, FORTINET, GoSecure, GWAVA, iboss, Light Point Security, McAfee, Menlo Security, NAMOGOO, perimeterx, proofpoint, randed, Reblaze, SHAPE, SHIELDSQUARE, smoothwall, SOPHOS, SPAMINA, Symantec, TREND MICRO, Trustwave, unbotify, whiteops, zscaler

Endpoint Security

Endpoint Prevention
AhnLab, avast, Avecto, Avira, Barkly, BINARY DEFENSE, Bitdefender, BLUERIDGE, Bromium, BUFFERZONE, Carbon Black, Check Point, COMODO, CROWDSTRIKE, CYBERARK, cybereason, CYLANCE, deepinstinct, ENDGAME, ENSILO, ERICOM, ESET, F-Secure, Faronics, FORTINET, HYSOLATE, intego, ivanti, KASPERSKY, Malwarebytes, McAfee, Microsoft, MORPHISEC, NYOTRON, OPSWAT, paloalto, panda, PERCEPTION POINT, SentinelOne, SOPHOS, sparkcognition, STORMSHIELD, Symantec, TETHRIS, TREND MICRO, vmware, WEBROOT

Endpoint Detection & Response
BELDEN, BINARY DEFENSE, Bitdefender, Carbon Black, cisco, COMODO, CROWDSTRIKE, CYBERBIT, cybereason, CYBONET, CYLANCE, Cynet, DIGITAL GUARDIAN, dtex, ENDGAME, ENSILO, FENROR7, Fidelis, FIREEYE, FORCEPOINT, GoSecure, HUNTRESS, KASPERSKY, Malwarebytes, NEHEMIAH, nexthink, NYOTRON, paloalto, panda, promisec, RSA, secpod, SentinelOne, SOPHOS, Symantec, TANIUM, TETHRIS, WatchGuard, ziften

Application Security

WAF & Application Security
6scan, A10, Akamai, ALERT LOGIC, ARXAN, Barracuda, CEQUENCE, citrix, CLOUDFLARE, CONTRAST SECURITY, CyKick Labs, DBAPPSecurity, denyall, ergon, F5, FORTINET, imperva, NETSPI, onapsis, ORACLE, Penta Security, portshift, POSITIVE TECHNOLOGIES, PURESEC, Qualys, radware, RAPID7, Reblaze, riverbed, SUCURI, SEWORKS, SHAPE, Signal Sciences, sqreen, StackPath, TEMPLARBIT, THREATX, TREND MICRO, Trustwave, VERACODE, Vicarius, wallarm, waratek, WhiteHat

Application Security Testing
acunetix, Assert Security, beyond security, bugcrowd, BUGFINDERS, CAST, CHECKMARX, ERPScan, Fasoo, hackerone, IBM, MICRO FOCUS, N-Stalker, NowSecure, PARASOFT, PERFORCE, PORTSWIGGER, Qualys, RAPID7, SecurityCompass, SiteLock, snyk, sonarsource, Synack, SYNOPSYS, tenable, Trustwave, VIRTUALFORGE, VERACODE, WhiteHat, WhiteSource

MSSP

Traditional MSSP
at&t, Atos, BAE SYSTEMS, BT, CenturyLink, Clone Systems, CSC, Hewlett Packard Enterprise, IBM, FORESITE, MegaPath, NTT, nuspire, OPTIV, orange, Secureworks, Symantec, Trustwave, verizon, wipro

Advanced MSS & MDR
ADT, ALERT LOGIC, ANITIAN, ARCTIC WOLF, AVERTIUM, Booz Allen Hamilton, CI Security, CRITICALSTART, CYBERHAT, CyberProof, CYDERES, deepwatch, digital hands, Eleven Paths, eSENTIRE, expel, FIREEYE, GoSecure, HERJAVEC, IntelSecure, KUDELSKI SECURITY, mka cyber, MOSAIC451, Netwatch, OBRELA, PALADION, PROFICIO, RAPID7, Raytheon, redcanary, RELIAQUEST, root9b, UNISYS

Data Security

Encryption
baffle, boxcryptor, CipherCloud, CLOUDMASK, COVERTIX, CryptoMove, CYPHERIX, YPHRE, DATALOCKER, ENVEIL, Fortanix, KeyNexus, MENTIS, AnCrypted Cloud, NuCypher, PKWARE, SecurityFirst, STORMSHIELD, THALES, TREND MICRO, virtru, WINMAGIC

DLP
clearswift, CODE42, DIGITAL GUARDIAN, Fidelis, FORCEPOINT, GTB Technologies, INFOWATCH, McAfee, SEARCHINFORM, SOMANSA, Symantec, ZECURION

Data Privacy
Actifile, BigID, COVATA, D.DAY LABS, ETHYCA, INTEGRIS, minereye, nuix, OneTrust, SecuPi, SPIRION, SYTORUS, TITUS, TrustArc, trusthub, very good security, wirewheel

Data Centric Security
BlueTalon, CODE42, Datex, dataphy, DB CyberTech, druva, egress, global velocity, IONIC, opentext, PRIVITAR, SECLORE, SPIRION, StorageCraft, THINAIR, VARONIS, VERA

Mobile Security
appdome, BETTER, BlueCedar, Check Point, cellrox, COMMUNITAKE, CyberAdapt, deepinstinct, eMune, Fyde, INPEDIO, KOOLSPAN, Lookout, mobileiron, NowSecure, NUBO, pradeo, PSafe, SaltDNA, silent circle, SOTI, Symantec, TeleSign, TESKALABS, tigertext, TRUSTLOOK, VAULTO, vmware, wandera, wickr, ZIMPERIUM

Risk & Compliance

Risk Assessment & Visibility
AXONIUS, Balbix, cavirin, Coalition, cyber OBSERVER, CyberCube, cyber GRX, cytegic, DELVE, eclypsium, FIREMON, InnoSec, KENNA Security, NEHEMIAH, NOPSEC, OPAQ, Outpost24, panaseer, PREVALENT, REDSEAL, riskrecon, RISKSENSE, SKYBOX, tenable, UpGuard, VENAFI, zeguro

Security Ratings
BITSIGHT, corax, FICO, GUIDEWIRE, NormShield, Panorays, PREVALENT, RiskLens, riskrecon, SecurityScorecard

Pen Testing & Breach Simulation
ATTACKIQ, Cobalt, CRONUS, CYBERHAT, CYCOGNITO, CYMULATE, DEPTH, Komodo Consulting, MAZEBOLT, NOPSEC, PCYSYS, PICUS, RAPID7, SafeBreach, SCYTHE, VERODIN, XM Cyber

GRC
algosec, Apptega, esecure, Galvanize, InformationShield, LockPath, MetricStream, netwrix, Onspring, RESOLVER, riskonnect, RSA, SAI GLOBAL, tufin

Security Awareness & Training
Barracuda, COFENSE, CyberVista, IMMERSIVELABS, KnowBe4, PHISHLABS, proofpoint, RANGEFORCE, SANS, SECURITY INNOVATION, the security awareness company

Identity & Access Management

Authentication
Acceptto, Auth0, averon, BehavioSec, BIOCATCH, Callsign, Centrify, CLEF, CORE SECURITY, DUO, EXOSTAR, FORGEROCK, FUDO SECURITY, Google, HYPR, IDEE, imprivata, INTRINSIC ID, JUMIO, nok nok, pindrop, plainID, SASSPASS, SaferPass, SECRET DOUBLE OCTOPUS, SECUREKEY, SECUREDTOUCH, SECUREPUSH, ShoCard, SILVERFORT, tascent, ThreatMetrix, TRANSMIT SECURITY, TransUnion, TRUSONA, UNBOUND, UNIFYID, UNIKEN, V-KEY, VIRGIL

IDaaS
AVATIER, okta, Centrify, onelogin, IBM, idaptive, ilantus, Ping, welcome, RSA, Microsoft, THALES, ORACLE

Privileged Management
BeyondTrust, ManageEngine, Centrify, MICRO FOCUS, CYBERARK, ONE IDENTITY, FUDO SECURITY, Remediant, HITACHI, SECURELINK, IBM, thycotic

Identity Governance
AXIOMATICS, Deep Identity, helpsystems, SailPoint, SAVIYNT, simeio

Consumer Identity
Akamai, Auth0, FORGEROCK, IDExperts, ID.me, JUMIO, loginradius, Microsoft, Ping, PIREAN, salesforce, SAP, SECUREKEY, Trulioo, vchain, verato, VERIFF

Security Ops & Incident Response

SIEM
AT&T Cybersecurity, BLACKSTRATUS, CORRELOG, CYGILANT, DEVO, DNIF, EventTracker, exabeam, FORTINET, HanSight, Huntsman, IBM, IGLOO SECURITY, logentries, LOGPOINT, LogRhythm, logz.io, McAfee, MICRO FOCUS, Palantir, RSA, SAWMILL, SECURONIX, solarwinds, splunk, sumo logic, TIBCO, Trustwave

Security Incident Response
arctos networks, atarlabs, ayehu, CYBERBIT, CYBERSPONSE, CYBER TRIAGE, D3 SECURITY, DARKLIGHT, DEMISTO, DFLABS, encode, FIREEYE, Microsoft, paloalto, radar, RAPID7, Resilient, Raytheon, SecBI, servicenow, SIEMPLIFY, SIFT SECURITY, splunk, SWIMLANE, SYNCURITY, THREATCONNECT, THREATQUOTIENT, UPLEVEL, VERINT

Security Analytics
AWAKE, Bay Dynamics, DARKTRACE, dtex, empow, exabeam, Fluency, FORTINET, HanSight, haystax, IMVISION, IronNet, MICRO FOCUS, mistnet, observe it, paloalto, patternex, Reservoir Labs, RSA, SecBI, SECURONIX, sumo logic, TERAMIND, THETARAY, THRESHING FLOOR, TripleCyber, VECTRA, Veriato, vmware

Momentum CYBER

Threat Intelligence
4iQ, ANOMALI, Blueliv, BlueVoyant, CENTRIPETAL NETWORKS, cisco, Cyberint, digital shadows, DOMAINTOOLS, EclecticIQ, FORSIGHT SECURITY, FLASHPOINT, GROUP-IB, HanSight, HYAS, INTEL 471, INTSIGHTS, KELA, LOOKINGGLASS, Malware Patrol, NUCLEON, Recorded Future, RiskBased Security, RISKIQ, SenseCy, Sixgill, SpyCloud, SURFWATCH, THREATCONNECT, ThreatMetrix, THREATQUOTIENT, ThreatSTOP, TRUSTAR, WEBROOT

IoT

IoT Devices
APOLLOSHIELD, ARMIS, Bastille, CENTRI, Convexum, CYBEATS, MBX, CYLUS, dellfer, ICON LABS, IMBRIT, ordr, KEYFACTOR, LEVL, MagicCube, MEDIGATE, MOCANA, Regulus, riscure, Rubicon, SECURITHINGS, SEPIO, SENRIO, ZingBox

Automotive
BlackBerry, c2a security, Continental, CYCURO, CYMOTIVE, ENIGMATOS, foretellix, GuardKnox, HARMAN, Karamba Security, NNG, otonomo, SAFERIDE, Trillium, Upstream

Connected Home
Bitdefender, CUJO, F-Secure, FORTRESS, RUBICA, SAM, Symantec

Messaging Security
AGARI, AREA 1, AstraID, BAE SYSTEMS, Barracuda, cisco, clearswift, CYBONET, CYREN, FIREEYE, FORCEPOINT, FORTINET, GoSecure, GreatHorn, GWAVA, inky, IRONSCALES, mailguard, McAfee, Microsoft, mimecast, PHISHLABS, proofpoint, Sasa Software, SONICWALL, SOPHOS, SPAMINA, Symantec, TREND MICRO, Trustwave, VadeSecure, VALIMAIL, VOTIRO, WEBROOT, wickr, ZERO SPAM, zix

Digital Risk Management
crisp, CYBERSPRINT, digital shadows, DigitalStakeout, EXPANSE, LOOKINGGLASS, NAMOGOO, PHISHLABS, RISKIQ, SafeGuard Cyber, source defense, ZEROFOX

Security Consulting & Services
accenture, ADAPTURE, A-LIGN, appsec consulting, BISHOP FOX, Booz Allen Hamilton, BT, CORVID, Deloitte, DENIM GROUP, EY, FIREEYE, fishtech, GreyCastle, GuidePoint, IBM, IOActive, Komodo Consulting, KPMG, KUDELSKI SECURITY, leidos, MindPoint Group, nccgroup, NEC, NEW CONTEXT, NISOS, NTT, OPTIV, pwc, RENDITION INFOSEC, REVEALRISK, Revolutionary Security, SecurityCompass, SERABRYNN, SPECTER OPS, STROZ FRIEDBERG, SYGNIA, VERSPRITE, wipro

Blockchain
BLOCK ARMOUR, Chain, edge, guardtime, IDEE, Manifold, NuID, remme, ShoCard, vchain, xage, VALID

Fraud & Transaction Security
AU10TIX, BIOCATCH, BLOCK FRAUD, Brighterion, CARDINAL COMMERCE, DATAVISOR, EARLY WARNING, emailage, ethoca, EverCompliant, feedzai, FICO, First Data, FORTER, GROUP-IB, Guardian Analytics, IdentityMind, IdenTrust, Kount, MagicCube, MAXMIND, NetGuardians, NS8, NuData Security, Pondera, riskified, Shift Technology, sift, SIGNIFYD, simility, SOCURE, ThreatMetrix, TokenID, TransUnion, UNIKEN

Cloud Security

Container
anchore, aqua, CAPSULE8, deepfence, NeuVector, POLYVERSE, portshift, Qualys, StackRox, Sysdig, Twistlock

Infrastructure
alcide, aporeto, ARMOR, BetterCloud, BRACKET, cavirin, Check Point, CLEARDATA, Cloud Conformity, CloudPassage, CYBERARK, EDGEWISE, Guardicore, HYTRUST, illumio, LACEWORK, paloalto, portshift, SHIELDX, sonrai, threat stack, varmour

CASB
AVANAN, bitglass, CipherCloud, cisco, CORONET, Managed Methods, McAfee, Microsoft, netskope, ORACLE, proofpoint, SKYFORMATION, StratoKey, Symantec