Security Kick-Off event

Thomas Ljungberg Kristensen, thomas@welcomesecurity.net

Timeslot	Topic / Agenda
13:00 – 13:30	**Welcome to the “Kick Off” event**
13:30 – 15:00	**What is happing right now and why is it different?!** You open a newspaper and read about a new breach or compromise. Maybe you even got notified that your data has been a breach! But what is going on, and why did we get here?
15:00 – 16:00	**Break / Coffee and Cake / Network**
16:00 – 16:45	**The way in – for it-criminals!** Most attacks start with either a social engineering attack or the exploit of a known software vulnerability, but most people have not seen how easy this is! – Let me show you!
16:45 – 17:00	**Short Break**
17:00 – 17:45	**Where do we go from here?** What can we do to improve security both privately and at OK and how do we improve the security of the software we create?
17:45 – 18:00	**Wrap-up and closing word from OK leadership**
	Dinner and Drinks

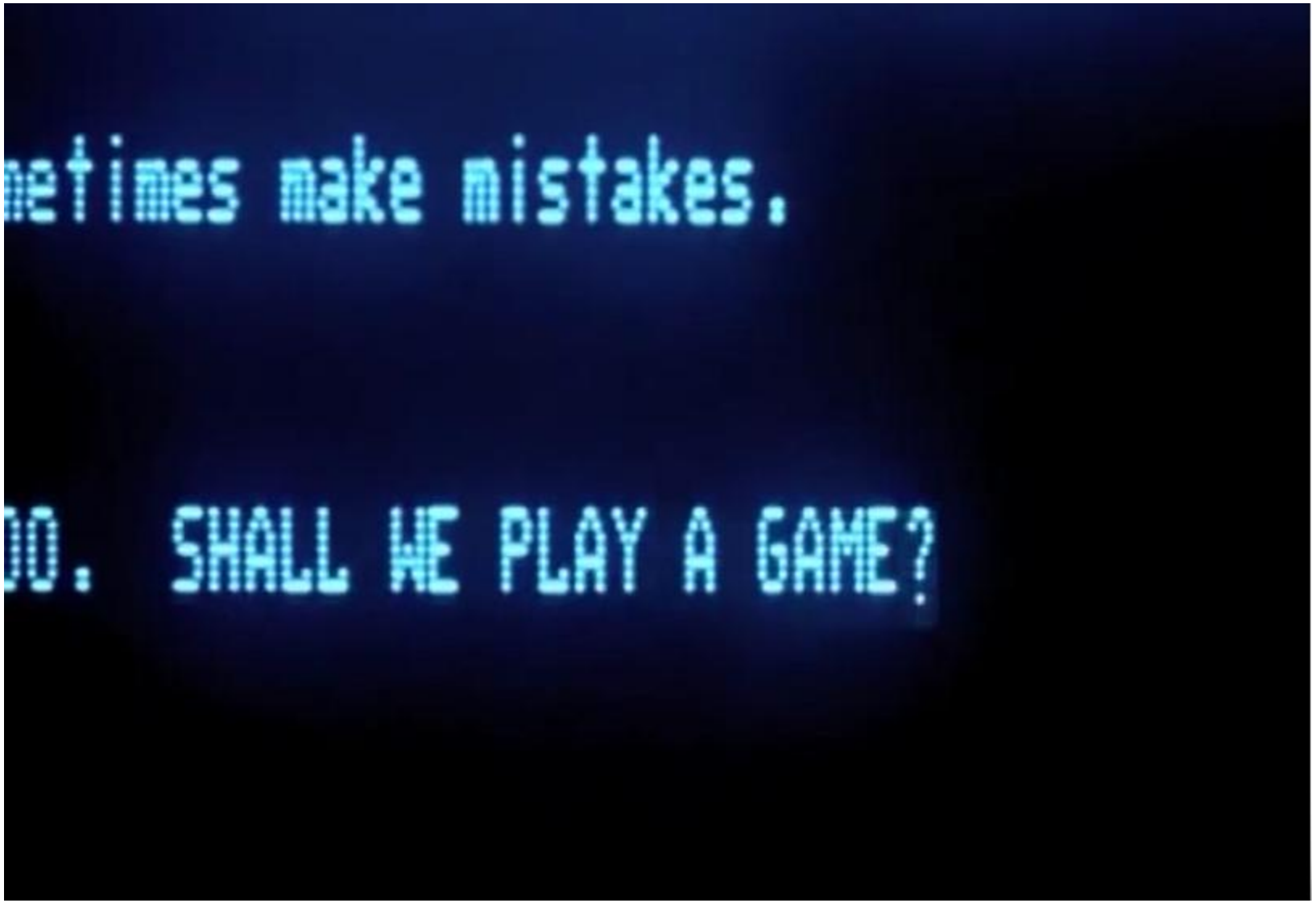
Thomas Ljungberg Kristensen

1996	Aarhus University, Master of Computer Sciences Cryptographical Protocol Theory	
2003	Systematic, Systems Engineer	
2007	Danske Bank, Developer	
2012	Kamstrup, Systems Engineer	
2014	FortConsult (part of NCC group), Senior Security Consultant	
2015 –	***WelcomeSecurity, Security Advisor and Owner***	
2019 –	***OWASP Co-chapter Lead, Aarhus***	
2019	Deloitte, Senior Manager	
2020 – 2021	Norlys, IT Security Architect	
2021 – 2021	Amazon Web Services, Senior Security Consultant	

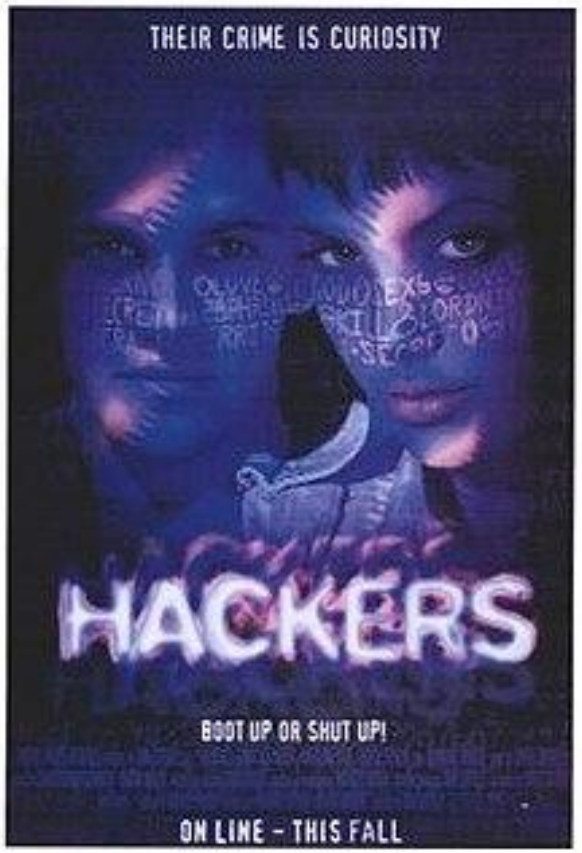
Why are we here and What is changing in the world?

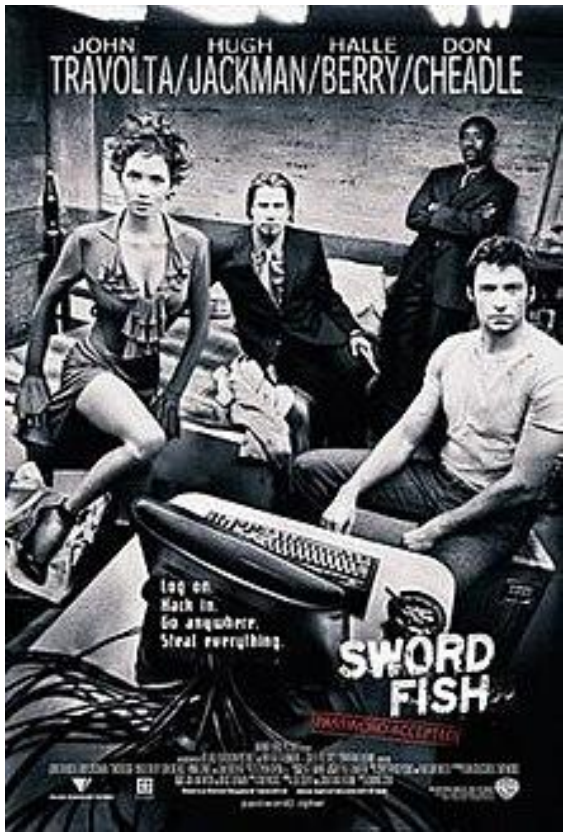
The Past

“Shall we play a game?”

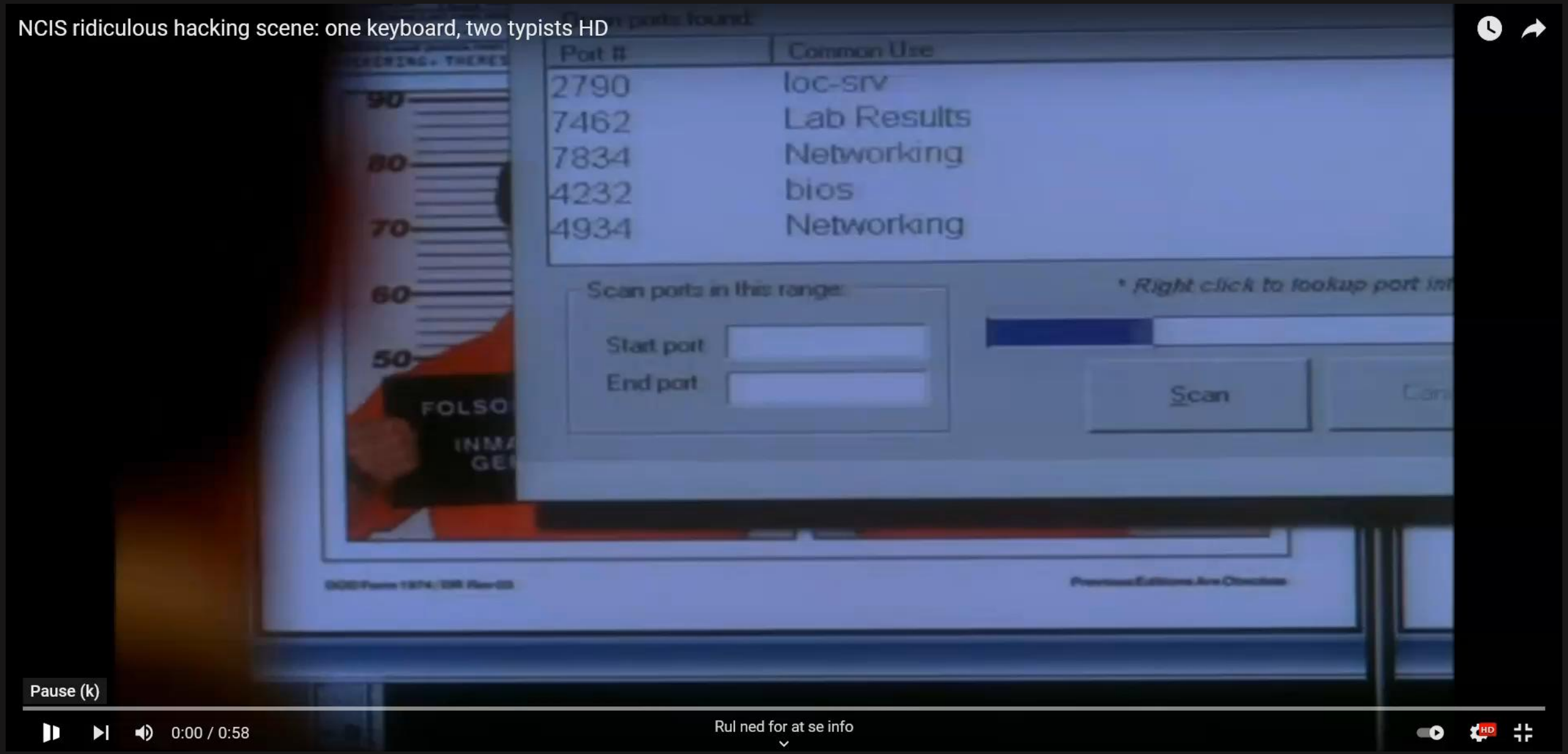


Wargames, 1983, MGM, https://www.mgm.com/#/our-titles/2117/WarGames-(1983)





Wikipedia (https://en.wikipedia.org/wiki/WarGames, https://en.wikipedia.org/wiki/The_Net_(1995_film), https://en.wikipedia.org/wiki/Hackers_(film), and https://en.wikipedia.org/wiki/Swordfish_(film)



https://www.youtube.com/watch?v=kl6rsi7BEtk

Mitnick served five years in prison—four and a half years pre-trial and eight months in solitary confinement—because, according to Mitnick, law enforcement officials convinced a judge that he had the ability to "start a nuclear war by whistling into a pay phone",[23] meaning that law enforcement told the judge that he could somehow dial into the NORAD modem via a payphone from prison and communicate with the modem by whistling to launch nuclear missiles.[24] In addition, a number of media outlets reported on the unavailability of Kosher meals at the prison where he was incarcerated.[25]

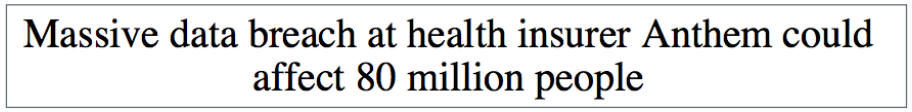
Wikipedia (https://en.wikipedia.org/wiki/Kevin_Mitnick) and https://twitter.com/kevinmitnick

The Present

“We cannot be breached!”

http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html

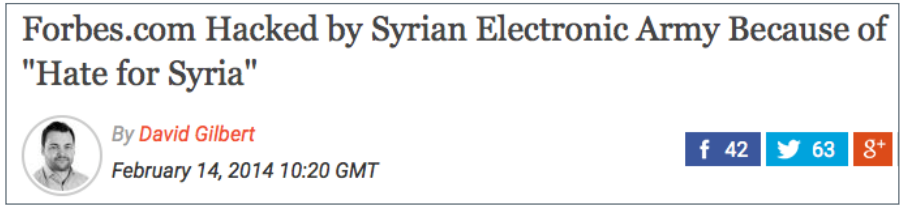
http://www.bbc.com/news/technology-26971363



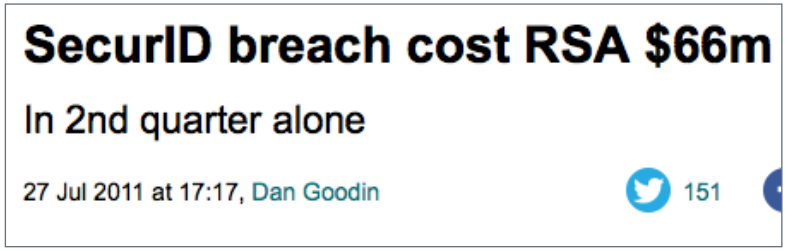
http://theweek.com/5things/537729/massive-data-breach-health-insurer-anthem-could-affect-80-million-people

http://www.huffingtonpost.com/2011/06/08/sony-hack-problems_n_873443.html

http://www.cnet.com/news/lenovo-hit-by-lawsuit-over-superfish-adware/

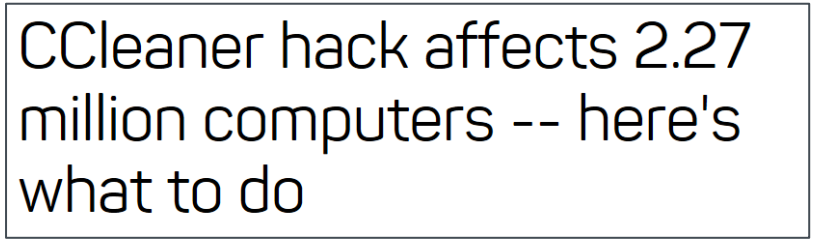


http://www.ibtimes.co.uk/forbes-com-hacked-by-syrian-electronic-army-because-hate-syria-1436415

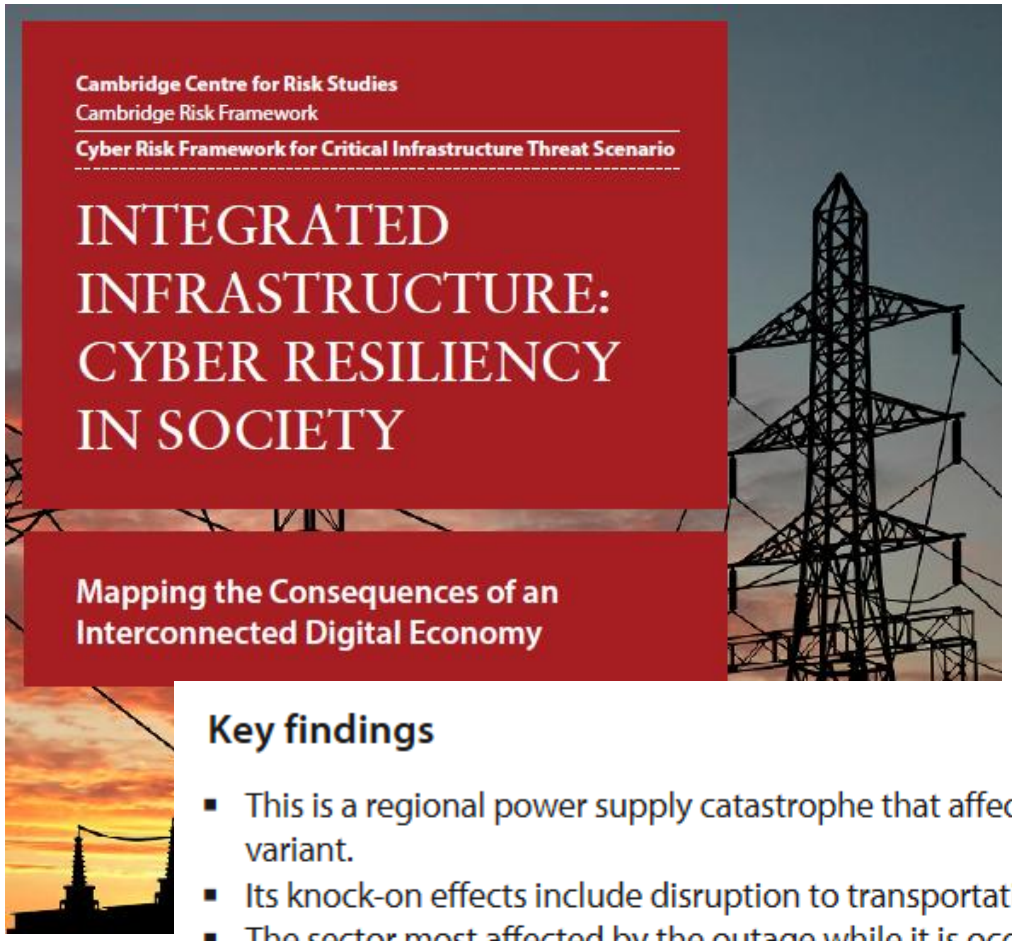


http://www.theregister.co.uk/2011/07/27/rsa_security_breach/

http://www.usatoday.com/story/tech/2014/10/02/jp-morgan-security-breach/16590689/



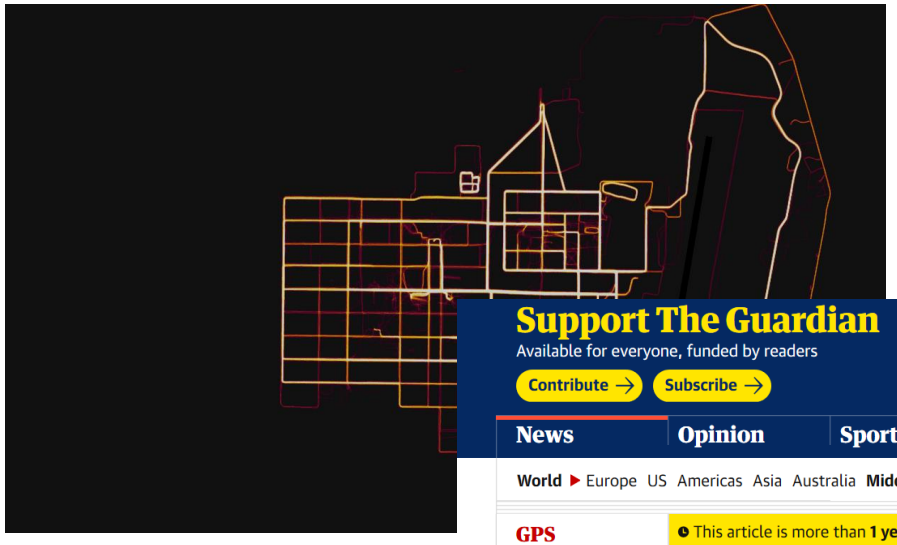
https://www.cnet.com/how-to/ccleaner-was-hacked-heres-what-to-do-next/



Key findings

- This is a regional power supply catastrophe that affects between 9 million and 13 million electricity customers depending on the scenario variant.
- Its knock-on effects include disruption to transportation, digital communications, and water services for 8 to 13 million people.
- The sector most affected by the outage while it is occurring is Financial Services, which loses an estimated £1.3 billion during the period of the outage, in the baseline scenario.
- The secondary economic impacts remain for some time after the initial disaster as confidence continues to wane, perishable products are no longer fit for sale, businesses suffer, international relations are damaged and supply chains take considerable time to recover.
- The economic losses to sectors are in the range of £11.6 billion to £85.5 billion in the different variants of the scenario.
- The overall GDP impact of the attack amounts to a loss between £49 billion to £442 billion across the entire UK economy in the five years following the outage, when compared against baseline estimates for economic growth.

Source: https://www.jbs.cam.ac.uk/faculty-research/centres/centre-for-risk-studies/publications/space-and-technology/integrated-infrastructure-cyber-resiliency-in-society/



Support The Guardian
Available for everyone, funded by readers
Contribute
Subscribe
Search jobs
Sign in
News
Opinion
Sport
Culture
Lifestyle
World
Europe
US
Americas
Asia
Australia
Middle East
Africa
Inequality
Cities
Global development
GPS
This article is more than 1 year old

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

Latest: Strava suggests military users 'opt out' of heatmap as row deepens

Source: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Security Notes from All Over: Coca-Cola and the NSA

Coca-Cola has a new contest. Hidden inside 100 cans of Coke there's a SIM card, GPS transmitter, and a microphone. The winners activate the Coke can by pressing a button, which will call a central monitoring facility. Then Coke tracks the winners down using the GPS transmitter and surprises them with their prize.

NSA engineers drink Coke. Lots and lots of Coke. The possibility that an active microphone in a Coke can could be in one of the NSA's highly secure facilities is worth considering. A reasonable threat analysis might look like this: "You know, the chances that one of these 100 cans out of hundreds of millions of cans ends up in our building is extremely small -- somewhere around 1 in 100,000 -- so it's not worth worrying about."

But the NSA's Information Staff Security Office) decreed differently: "It is important that ALL cans of Coca-Cola within our spaces be inspected. This includes cans already in our buildings and those being delivered on a daily basis. If you discover one of these cans, DO NOT activate it. Instead, you should alert your ISSO immediately and report the incident."

Source: https://www.schneier.com/crypto-gram/archives/2004/0715.html#8

CYBERSECURITY

Chinese spy chips are found in hardware used by Apple, Amazon, Bloomberg says; Apple, AWS say no way

PUBLISHED THU, OCT 4 2018 • 6:15 AM EDT | UPDATED FRI, OCT 5 2018 • 7:36 PM EDT

Kate Fazzini
@KATEFAZZINI

Source: https://www.cnbc.com/2018/10/04/chinese-spy-chips-are-said-to-be-found-in-hardware-used-by-apple-amazon-apple-denies-the-bloomberg-businessweek-report.html

WIRED

NSA HACKER CHIEF EXPLAINS HOW TO KEEP HIM OUT OF YOUR

Share

SHARE

TWEET

COMMENT

EMAIL

KIM ZETTER

IT WAS THE talk most anticipated
Usenix Enigma security conferen
that even the other speakers wer

How the NSA Gets You

In the world of advanced persistent threat actors (APT) like the NSA, credentials are king for gaining access to systems. Not the login credentials of your organization's VIPs, but the credentials of network administrators and others with high levels of network access and privileges that can open the kingdom to intruders. Per the words of a recently leaked NSA document, the NSA hunts sysadmins.

The NSA is also keen to find any hardcoded passwords in software or passwords that are transmitted in the clear—especially by old, legacy protocols—that can help them move laterally through a network once inside.

https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/

INTERNATIONALT

FE-chefen: Rusland vil hacke vores forvaltning og Kina vores virksomheder

Source: https://www.berlingske.dk/internationalt/fe-chefen-rusland-vil-hacke-vores-forvaltning-og-kina-vores-virksomheder

27.10.20 (55 minutter)

TØR VI BRUGE VORES CYBERKAPACITETER?

Lyt med | Podcastside

Beskrivelse

I sidste uge blev seks navngivne russiske militære efterretningsagenter tiltalt i USA for at have begået omfattende hacking og angrebet virksomheder, internationale organisationer, valgkampagner og partier, fremmede regeringer og de olympiske vinterlege i Sydkorea. Men er det kun vores fjender, der laver dristige offensive cyberoperationer? Skal vi i Danmark bruge vores offensive kapacitet? Og hvordan integrerer man cybervåben i konventionelle styrker? Frontlinjen tager debatten med Jeppe Teglskov Jacobsen, adjunkt ved Forsvarsakademiet og forsker i offensive cyberoperationer, John Foley, der var med til at opbygge Center for Cybersikkerhed under Forsvarets Efterretningstjeneste, og Naser Khader (K), formand for Forsvarsudvalget. Undervejs kommer der indspark fra hærchefen Michael Lollesgaard og de cyberværnepligtige på Ryes Kaserne i Fredericia.

Kopier link | Del på facebook | Del på twitter

Naser Khader (K), formand for Forsvarsudvalget
"Vi kan meget mere end vi bør gøre. For eksempelvis så kan vi gå ind og slukke for el og vand i Moskva i et døgn..."

Peter Ernstved Rasmusen (Værten)
"Kan vi det?..."

Naser Khadar
"Nu er jeg ikke ekspert, men jeg tror at vi er i stand til at gøre det..."

https://www.radio4.dk/program/frontlinjen/?id=tr-vi-bruge-vores-cyberkapaciteter_ep_27_10_20 (cirka 10:25 min inde) og https://www.ft.dk/medlemmer/mf/n/naser-khader

Erhverv

Mine nyheder

FINANS

Søg

Hackernes cybertogt kan få flere virksomheder til at gå konkurs

Store økonomiske konsekvenser er en af virksomhedernes største frygt ved hackerangreb.

ERHVERV | 17.07.2017 KL. 06:17

55 pct. af de adspurgte virksomheder mener, at økonomiske omkostninger vil være det største problem ved et hackerangreb, og hver anden svarer samtidig, at et hackerangreb kan betyde, at virksomheden går konkurs.

https://finans.dk/erhverv/ECE9722058/hackernes-cybertogt-kan-faa-flere-virksomheder-til-at-gaa-konkurs/

ING/VERSION2

NYHEDER BLOGS DEBAT JOB SEKTIONER MERE IT-TALENT INFOSECURITY TIP

Danmarks største nyhedsbureau lagt ned af hackerangreb

https://www.version2.dk/artikel/danmarks-stoerste-nyhedsbureau-lagt-ned-hackerangreb-1091672

PENGE

ISS ramt af hackerangreb: Formålet var afpresning

Hackergruppe angreb servicegiganten ISS for at få løsepenge. Alt tyder på russiske bagmænd, vurderer ekspert.

https://www.dr.dk/nyheder/penge/iss-ramt-af-hackerangreb-formaalet-var-afpresning

DR Nyheder TV Radio Privatlivspolitik KONTAKT DR SØG PÅ DR.DK

SENESTE NYT INDLAND UDLAND PENGE POLITIK REGIONALT VEJRET

PENGE

Hackerangreb koster dansk virksomhed over en halv milliard

Hackerangrebet betød, at høreapparatvirksomheden Demant ikke kunne distribuere produkter, og det har kostet salg.

https://www.dr.dk/nyheder/penge/hackerangreb-koster-dansk-virksomhed-over-en-halv-milliard

NYHEDER DR

TEMA HACKERANGREB 37 ARTIKLER

Hackerangreb koster Mærsk milliardbeløb

Mærsk anslår, at hackerangrebet fra juni og juli vil koste selskabet 1,3 til 1,9 milliarder kroner.

https://www.dr.dk/nyheder/penge/hackerangreb-koster-maersk-milliardbeloeb

VERSION 2 IT-NYHEDER BLOGS DEBAT IT-JOB SEKTIONER MERE

Norsk Hydro ramt af stort hackerangreb: Anlæg står stille - forbud mod brug af netværk og pc'er

(Illustration: Aleksandr Kalugin/Bigstock)

Det store norske aluminiumsselskab er udsat for et omfattende hackerangreb- selskabets side er nede.

Caroline Rutter og Henning Mølsted @Henningcph Tirsdag, 19. marts 2019 - 10:30

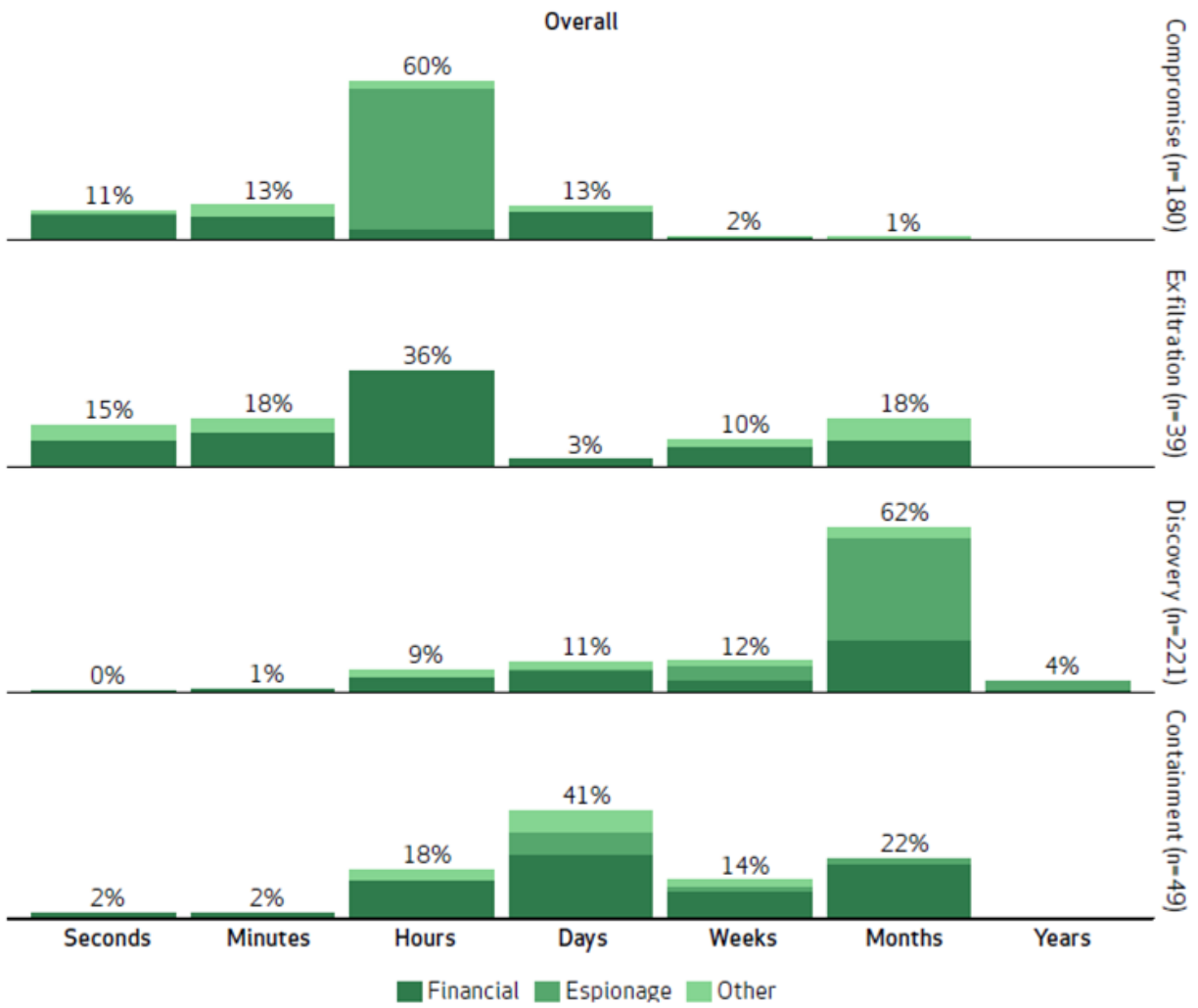
Opdateret kl. 11:51.

Norsk Hydro er udsat for et omfattende cyberangreb, som påvirker selskabets drift på flere parametre. Det skriver selskabet i en børsmeddelelse.

https://www.version2.dk/artikel/norsk-hydro-ramt-stort-hackerangreb-anlaeg-staar-stille-forbud-mod-brug-netvaerk-pcer

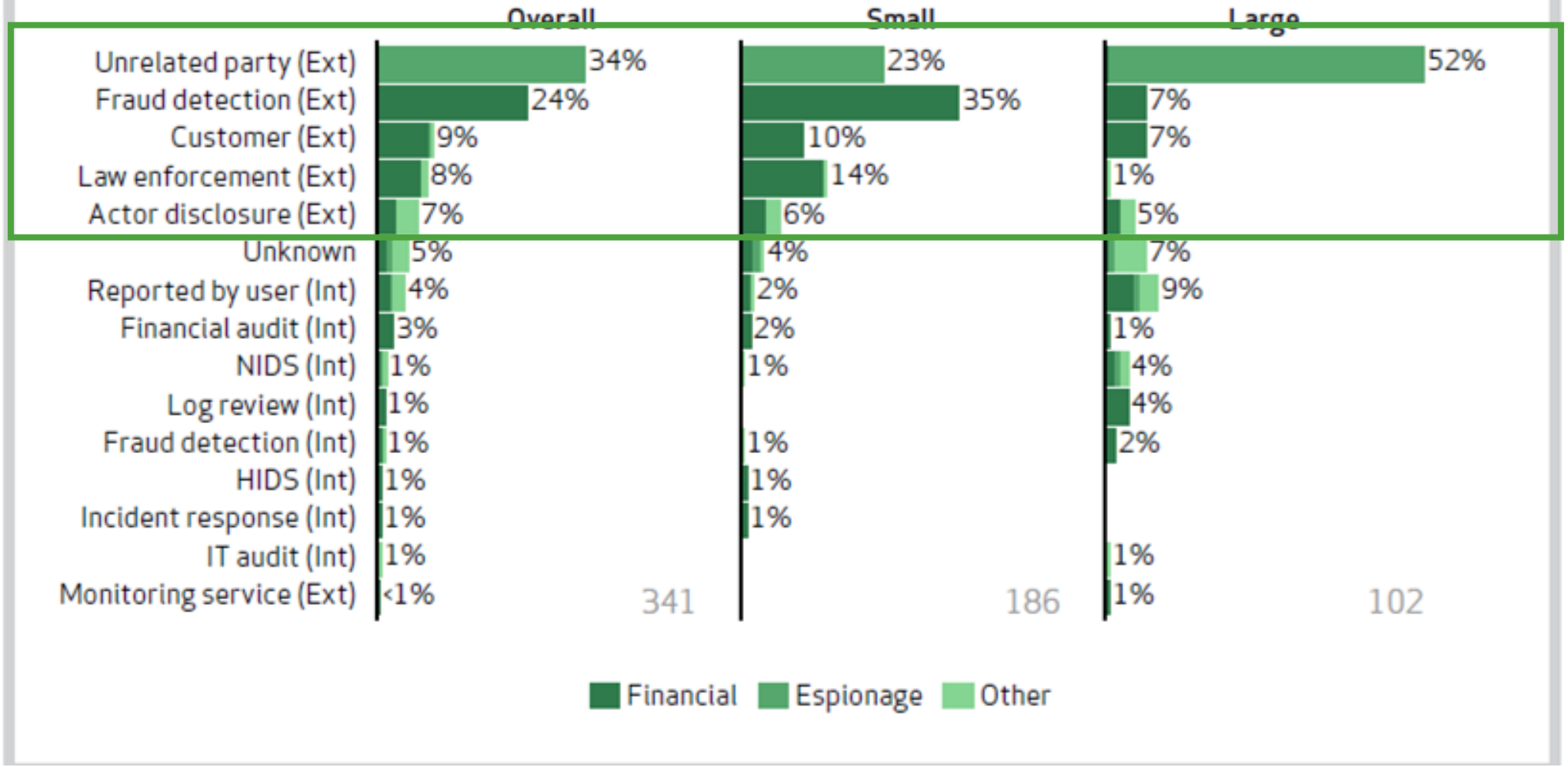
Compromise
Exfiltration
Discovery
Containment

Figure 41: Timespan of events

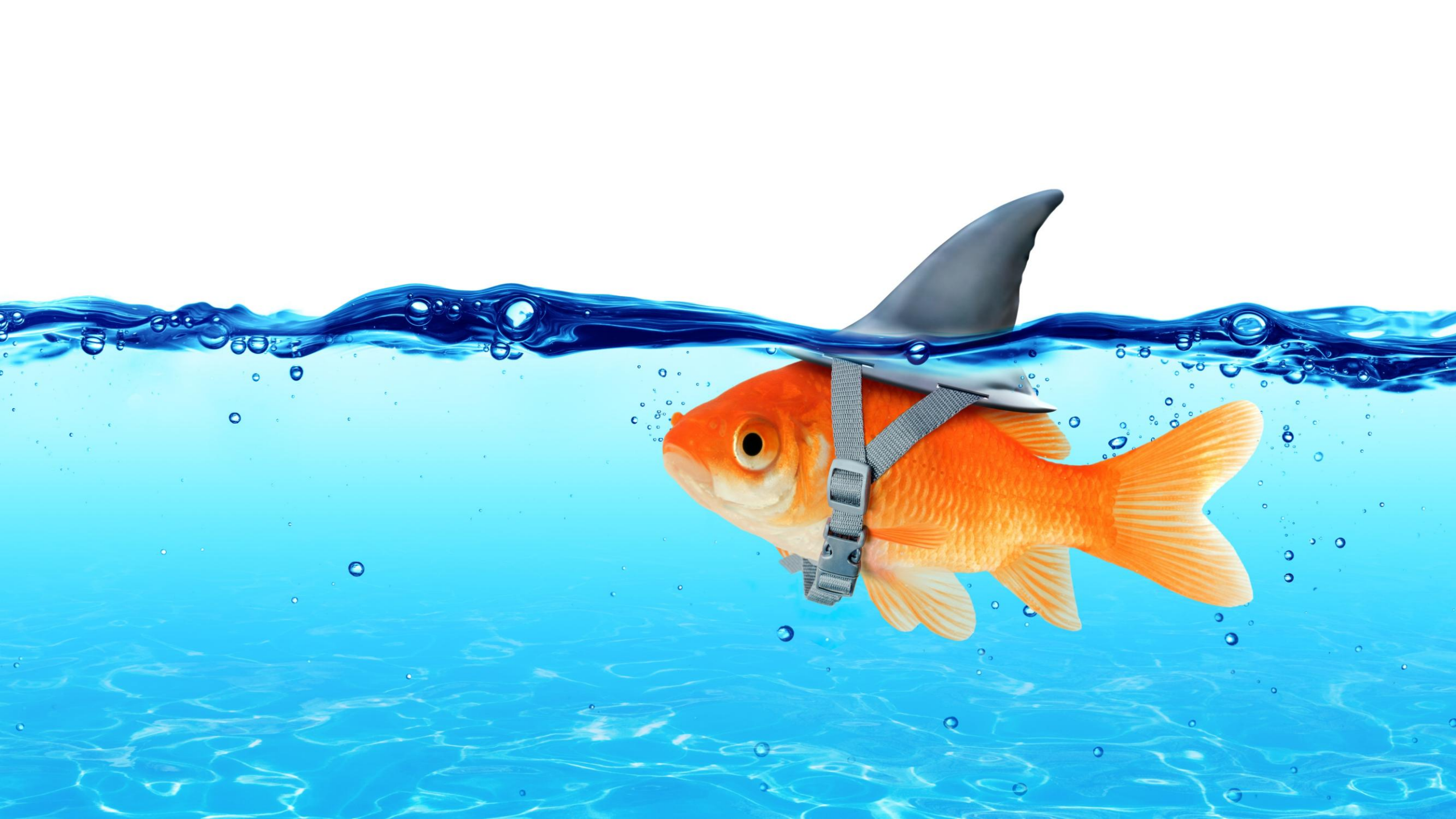


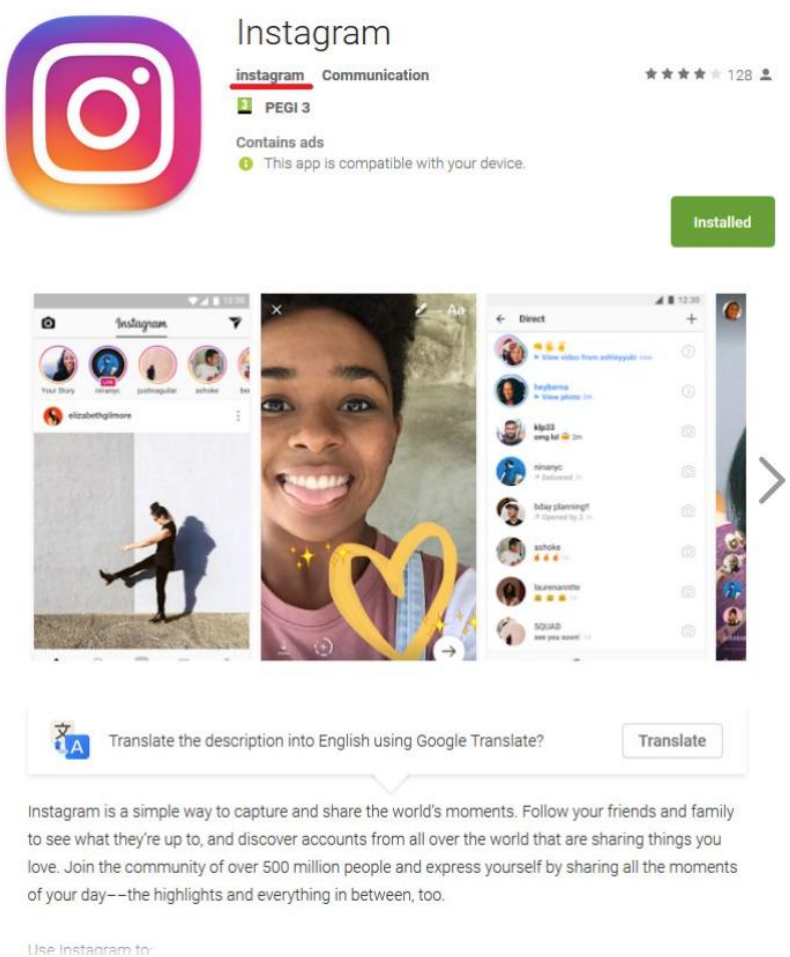
Sources: Verizon, 2013 Data Breach Investigations Report

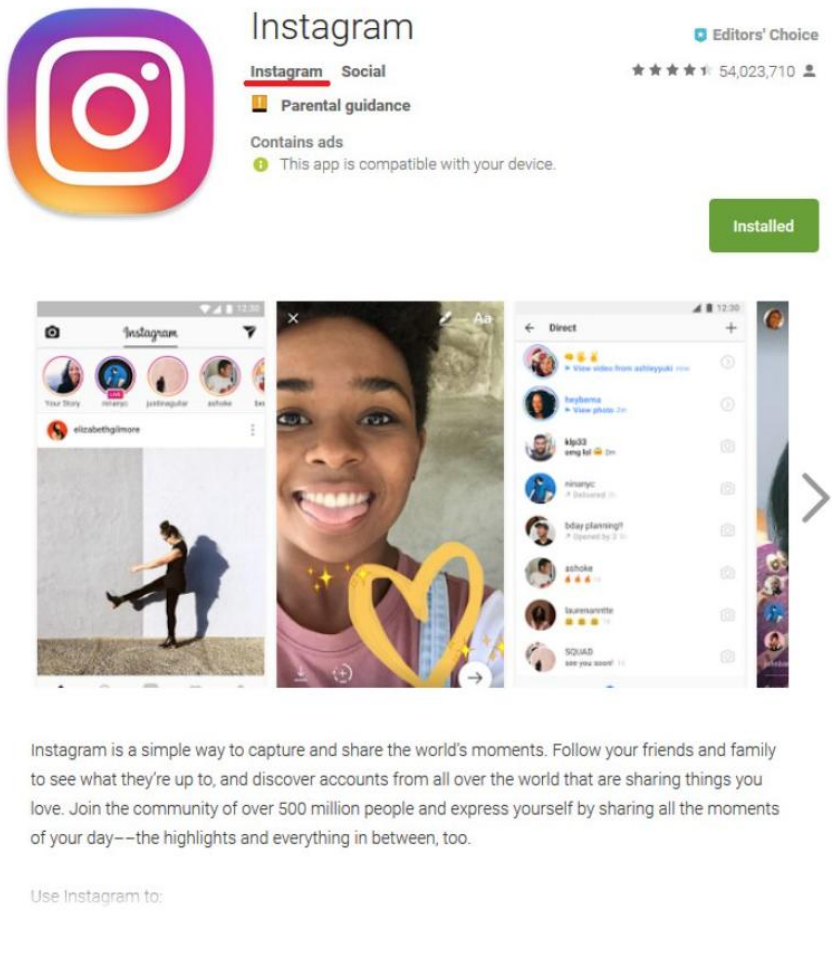
Figure 44: Discovery methods



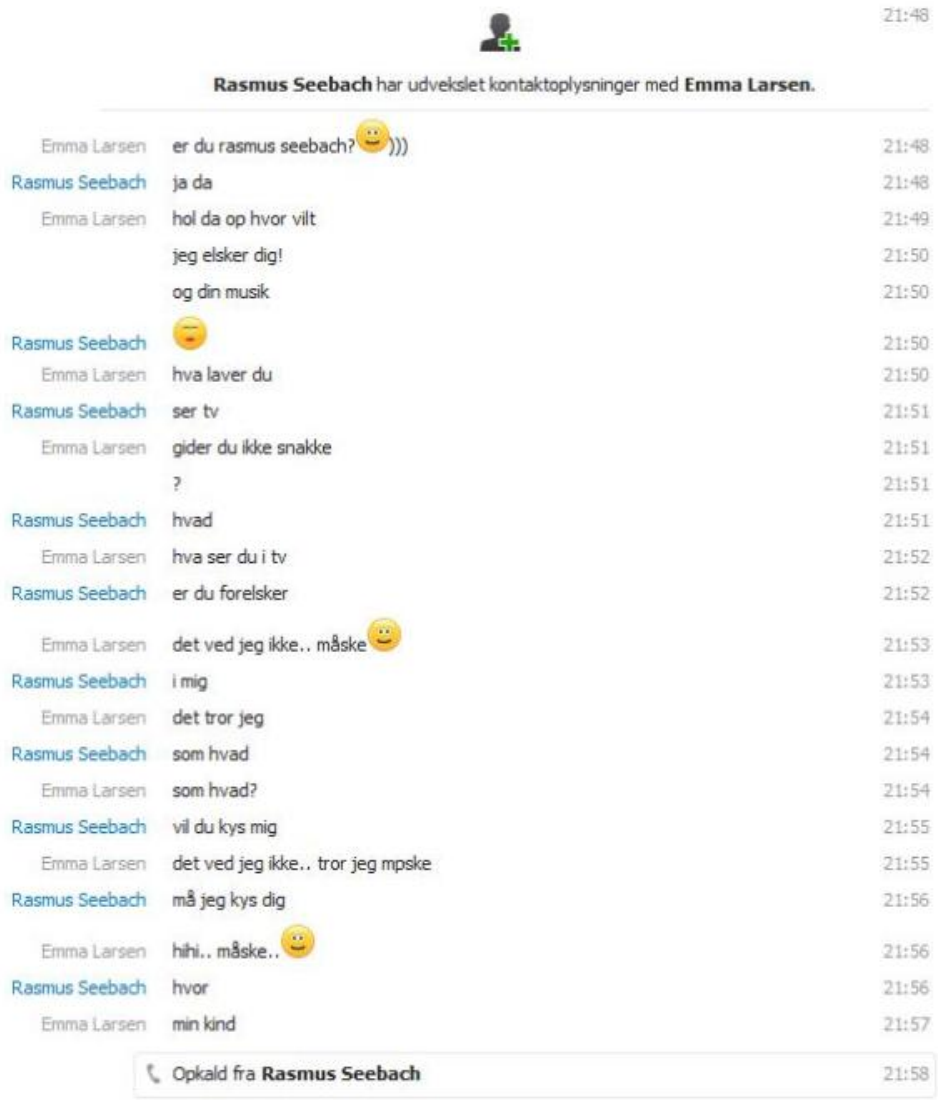
Sources: Verizon, 2013 Data Breach Investigations Report







Sources: https://twitter.com/LukasStefanko/status/909753129478082565



https://www.mx.dk/nyheder/danmark/story/13307249

Rasmus Seebach

36 years old

ASSOCIATED WITH: Ditte Marie Lund , Ida Marie Steensborg , Flemming Daniel Frederiksen , Ulla Rostgaard Poulsen , Frederik Lassen Hesseldahl , Nina Maglehøj Skjødt , Steffen Rise Andersen , Mette Hestehave Hansen , Jette Güldner Knudsen , Kamilla Juel Sørensen , 6 more »

Rasmus Seebach, rasmus.seebach, rasmus.seebach.9 - Svenstrup & ...
facebook.com/people/_/546092605
Personal Web Profile - Facebook

Rasmus Seebach, 36 years old
en.wikipedia.org/wiki/Rasmus_Seebach
The Free Encyclopedia - Wikipedia

Rasmus Seebach, Kristian Klinge (krillerone)
flickr.com/people/37901254@N02
Online Photo Album - Flickr

facebook.com/people/_/100003858655822
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.75
facebook.com/people/_/100003157308966
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.7
facebook.com/people/_/100003795579810
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.1238
facebook.com/people/_/100003522528600
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.12
facebook.com/people/_/100001115043646
Personal Web Profile - Facebook

Rasmus Seebach, rasmus.seebach.750
facebook.com/people/_/100004124554813
Personal Web Profile - Facebook

Rasmus Seebach Seebach
facebook.com/people/_/100000640895528
Personal Web Profile - Facebook

Fra: Info Nets <noreply@nets.com>
Dato: 8. marts 2017 kl. 10.07.57 CET
Til:
Emne: Adgang Til Dine Konto

Kære kunder Nets,

Det ser ud til, at en anden bruger din konto.

For din sikkerhed, har vi blokeret din konto
Vi har brug for nogle oplysninger for at løse dette problem

> Klik her https://www.nets.eu/dk-da/l%C3%B8sninger/dankort/022136

© Nets i Danmark (HQ)-kontoteamet

POST

Du har uforløste pakken

Vi har modtaget din pakke **CT5389919582DK** på **2015/09/21**. Courier var ude af stand til at levere denne pakke til dig

Få og udskrive forsendelsesetiketten, og vise det på det nærmeste posthus for at få din pakke.

Få en adresselapp

Hvis pakken ikke er modtaget inden 20 arbejdsdage PostNord AB vil være berettiget til at kræve kompensation fra dig - 55 kroner for hver dag i at holde. Du kan finde oplysninger om fremgangsmåden ved og betingelserne af pakken holde i det nærmeste kontor.

Dette er en automatisk genereret meddelelse. Klik her for at afmelde

Fra: **Skat.dk** <skat@skat.dk>
Dato: 1. okt. 2013 12.00
Emne: ID:38933 - tilbagebetaling af skat - DKK 6940,00
Til: XXX

SKAT

Bemærk: Tilbagebetaling af skat for året 2012

Kære skatteyder,

Vores registreringer viser, at du er kvalificeret til en tilbagebetaling af skat af:
DKK 6940,00

For at få adgang til din skat tilbagebetaling, klik venligst her.

Udfyld venligst formularen indtil d. **02-10-2013.**
Den hurtigste og nemmeste måde at modtage din tilbagebetaling på er ved direkte inc
check/opsparingskonto.

Vores hovedkontor adresse kan findes på vores hjemmeside på
http://www.skat.dk

http://www.it-blogger.dk/post-nord-virus-rammer-danmark/, http://skat.dk/SKAT.aspx?oId=68747 og https://www.nets.eu/dk-da/digital-sikkerhed/Pages/Phishing.aspx

DU ER EN SKYDESKIVE

Brugernavn og passwords

Hvis du er blevet hacket, kan IT-kriminelle installere programmer på din computer, der opfanger alt, hvad du taster inklusiv dine brugernavne og passwords. Den information bruges til at logge på dine online-konti så som:

- *Dine bankkonti, hvorfra de kan stjæle eller overføre dine penge.*
- *Din iCloud, Google Drev eller Dropbox konto hvilket kan give adgang til dine følsomme data.*
- *Dine konti til online indkøb, så kan de handle i dit navn og for dine penge.*

Høste informationer fra din e-mail

Hvis du er blevet hacket, har IT-kriminelle adgang til din e-mail og kan finde information de kan sælge. Det kan eksempelvis være:

- *Alle navne, e-mailadresser og telefonnumre fra din kontaktliste/telefonbog.*
- *Alle dine personlige e-mails og arbejds e-mail.*

Virtuelle varer

Hvis du er blevet hacket, kan IT-kriminelle kopiere og stjæle alle dine virtuelle varer og sælge dem til andre. Det drejer sig om:

- *Dine karakterer, varer og valuta i online spil.*
- *Alle licenser til software, operativsystemer og spil.*

Botnet

Hvis du er blevet hacket, kan din computer blive forbundet til et netværk af hackede computere, der bliver kontrolleret af den IT-kriminelle. Dette netværk kaldes et Botnet og kan blive brugt til at:

- *Sende spam til millioner personer.*
- *Overbelaste andres systemer og få dem til at gå ned.*

Du ved det måske ikke, men du er et mål for IT-kriminelle. Din computer, dine mobile enheder, dine (online) konti og dine informationer har en meget høj værdi. Denne plakat sætter fokus på, hvordan IT-kriminelle kan tjene penge på at hacke dig. Heldigvis kan du beskytte dig og din familie ved at følge nogle simple råd. Hvis du vil vide mere kan du abonnere på det månedlige nyhedsbrev om IT-sikkerhed fra OUCH!

www.securingthehuman.org/ouch

Identitetstyveri

Hvis du er blevet hacket, kan IT-kriminelle benytte din online profil til at begå svindel eller sælge din identitet til tredjepart. Det kan være:

- *Din Facebook, Twitter eller LinkedIn konto.*
- *Din e-mail konto.*
- *Din Skype konto.*

Web Server

Hvis du er blevet hacket, kan IT-kriminelle benytte din computer som server til:

- *At forsøge at stjæle andres brugernavne og passwords.*
- *Programmer, der hacker andre computere.*
- *Distribution af børneporno, piratkopier af film og stjålet musik.*

Økonomisk

Hvis du er blevet hacket, kan IT-kriminelle lede efter værdifuld information i dit system så som:

- *Information om dine kreditkort.*
- *Dine skatteoplysninger.*
- *Dine investeringer og pension.*

Afpresning

Hvis du er blevet hacket, kan IT-kriminelle overtage din computer og kræve penge. Dette kan de gøre ved at:

- *Tage billede med dit indbyggede kamera og kræve penge for at destruere det eller for ikke at offentliggøre det.*
- *Kryptere al data på din computer og kræve penge for at dekryptere det.*
- *True med at offentliggøre hvilke hjemmesider du har besøgt.*

Denne plakat er baseret på arbejde udført af Brian Krebs. Du kan lære mere om IT-kriminalitet ved at følge hans blog http://krebsonsecurity.com

Source: http://securingthehuman.sans.org/media/resources/STH-Poster-YouAreATarget-Danish.zip

Statistics from Denmark (and in Danish)

1 Cyber-angreb er den største risiko for virksomheder i Europa og medfører store økonomiske tab og potentielt konkurser

44% af de danske borgere har være udsat for: Infektion med skadelig software, misbrug af fortrolige oplysninger, økonomisk tab og tab af data

73% af danske virksomheder er blevet angrebet – eller forsøgt angrebet!

20 nye sårbarheder bliver offentliggjort om dagen

1/4 million angreb fra internettet hver dag!

2 minutter tager det, før en ny enhed på Internettet bliver ramt

https://www.danskerhverv.dk/siteassets/mediafolder/downloads/analysenotater-2017/66-cybersikkerhed.pdf,
https://digst.dk/media/18755/danskernes_informationssikkerhed_december_2018_191218.pdf,
https://www.weforum.org/reports/regional-risks-for-doing-business,
https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

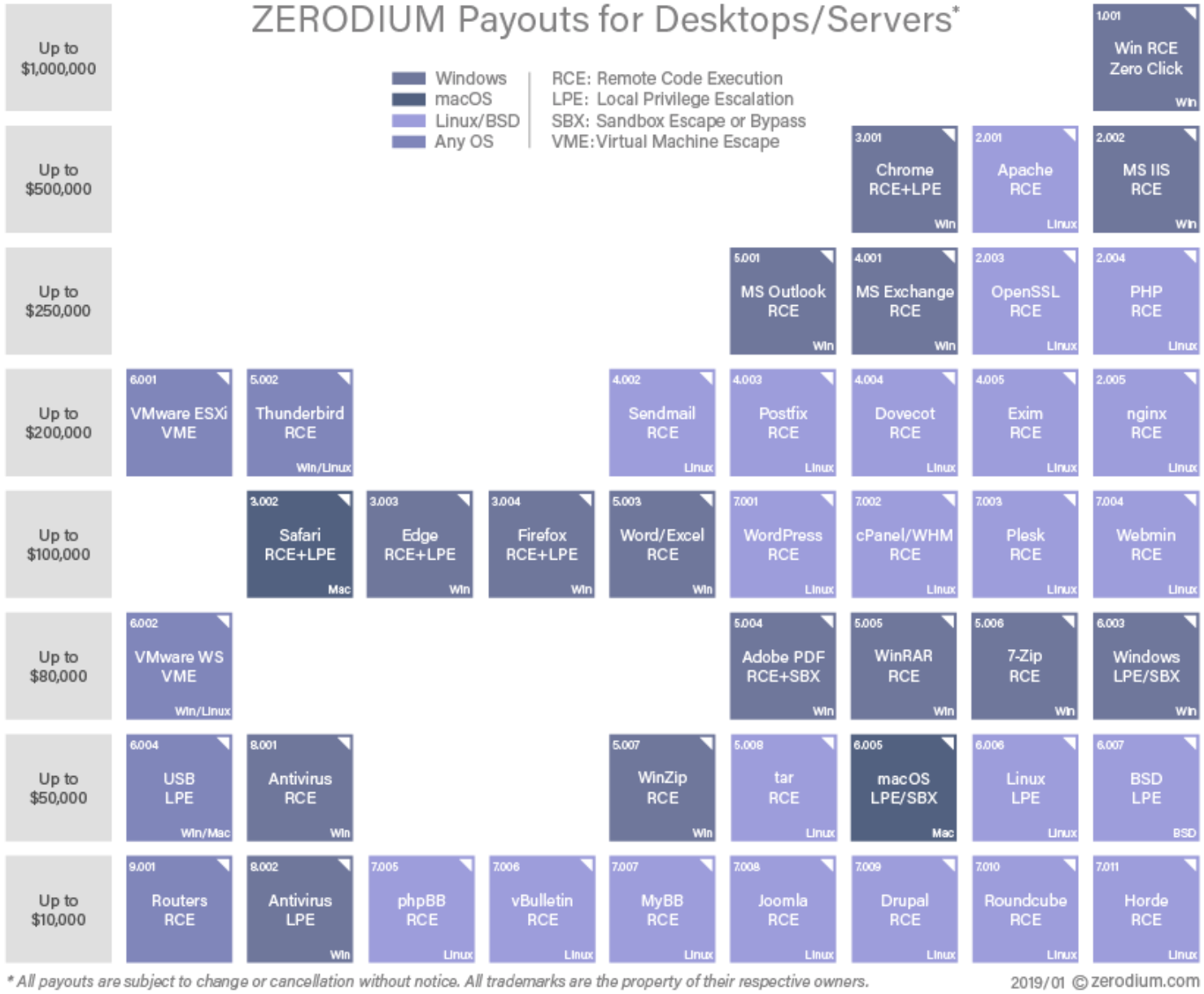
An attack is low risk and high ROI

Dedicated server (powerful servers)	0.50 – 1 (10 – 20)
1000 downloads in EU	80
Programming Services	? (100 – 250)
1 day DDoS	30 – 70
Cheap email spamming	10 per 1,000,000 emails
Email spamming, custom database	50 – 500 per 50,000 to 1,000,000 emails
SMS spamming	3 – 150 per 100 – 10,000 SMS
1 hour call flooding	2 – 5
Bots	200 for 2,000 bots
Copy of scanned EU passport	5
Windows 7 Ultimate license	7
Fake website	5 – 20
Credit card details	2 – 90 (add 190 for physical card)
Bank Credentials (with guaranty)	80 – 700
Purchase and forward of products	30 – 300

Fake web site	$20
1,000,000 spam emails	$10
5 Servers to host site	$70
	$100

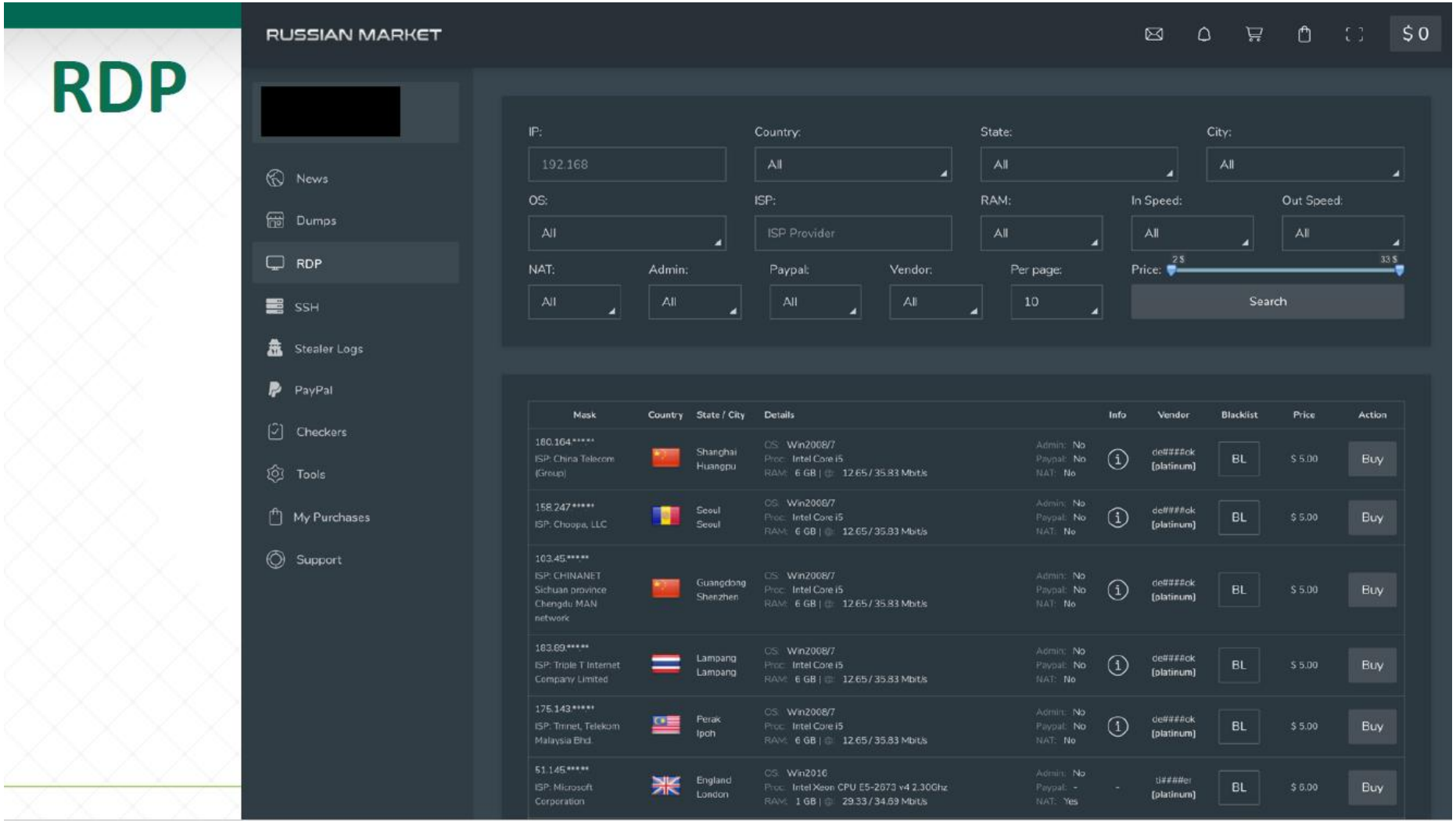
Break-even at 0.005% (or 50) people entering credit card details

"Russian Underground 101" by Trend Micro and "The Cyber-crime black market uncovered" by Panda Security



https://zerodium.com/program.html

RDP



The Industrialization of Cybercrime and Evolution of Cybercrime Syndicates - https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=446997

Annual license: $ 1500
Half-year license: $ 1000
3-month license: $ 700

Update cryptor $ 50
Changing domain $ 20 multidomain $ 200 to license.
During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): $ 200
2 weeks (14 full days): $ 300
3 weeks (21 full day): $ 400
4 weeks (31 full day): $ 500
24-hour test: $ 50

- There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

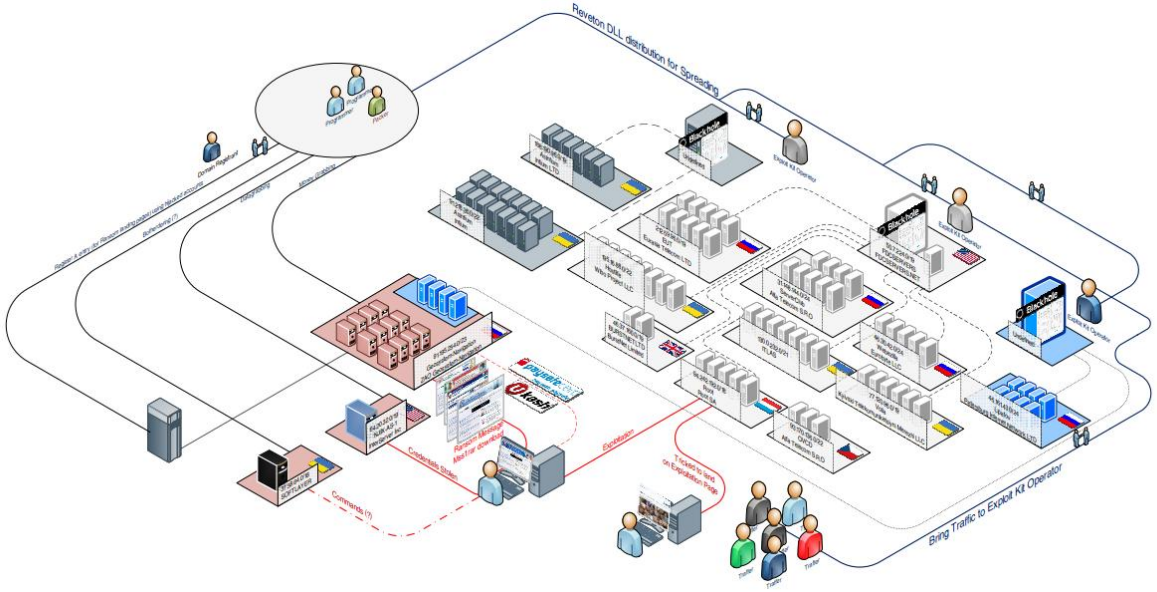
Providing our proper domain included. The subsequent change of the domain: $ 35
No longer any hidden fees, rental includes full support for the duration of the contract.

Sources: http://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-3/

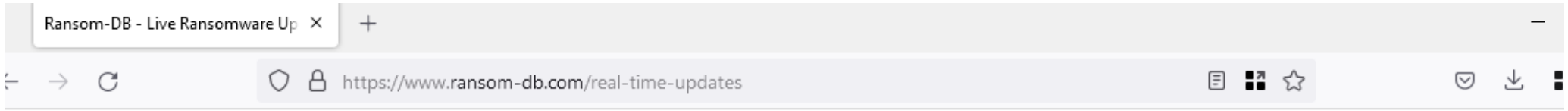
The most common 'positions' or specializations according to the FBI are:

1. **Programmers**. Who develop the exploits and malware used to commit cyber-crimes.
2. **Distributors**. Who trade and sell stolen data and act as vouchers for the goods provided by other specialists.
3. **Tech experts**. Who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases, and the like.
4. **Hackers**. Who search for and exploit applications, systems and network vulnerabilities.
5. **Fraudsters**. Who create and deploy various social engineering schemes, such as phishing and spam.
6. **Hosted systems providers**. Who offer safe hosting of illicit content servers and sites.
7. **Cashiers**. Who control drop accounts and provide names and accounts to other criminals for a fee.
8. **Money mules**. Who complete wire transfers between bank accounts. The money mules may use student and work visas to travel to the U.S. to open bank accounts.
9. **Tellers**. Who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.
10. **Organization Leaders**. Often "people persons" without technical skills. The leaders assemble the team and choose the targets.

Sources: "The Cyber-crime black market uncovered" by Panda Security



Sources: http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/



Live Ransomware Updates

Last 15 Ransomware Incidents \ Updates

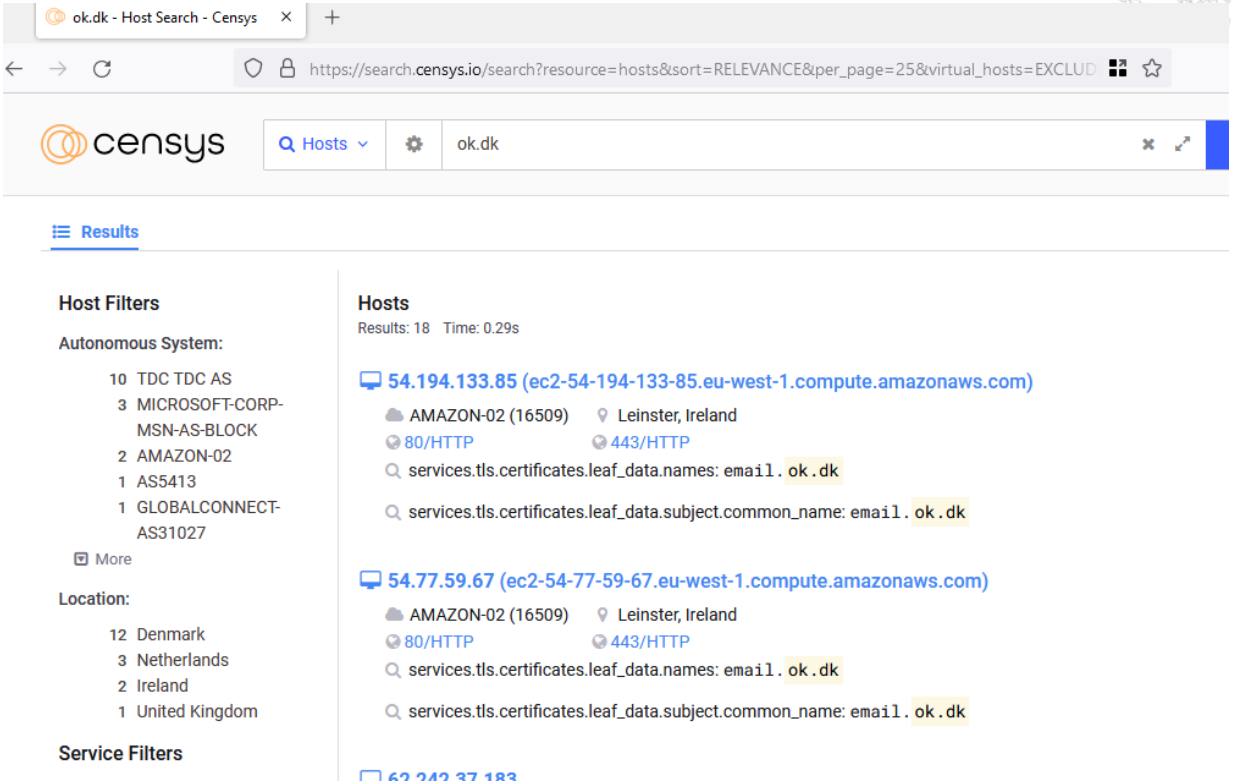
Ransom-DB Provides you with real-time ransomware tracking of ransomware groups and their victims

No.	Victim Name	Additional Info	Dates	Ransomware Group\Name	Icon
1	Veritas Solicitors	N\A	2022-10-04	BianLian	
2	Early, Lucarelli, Sweeney & Meisenkothen	N\A	2022-10-04	BianLian	
3	Dorsey metrology	N\A	2022-10-04	BianLian	

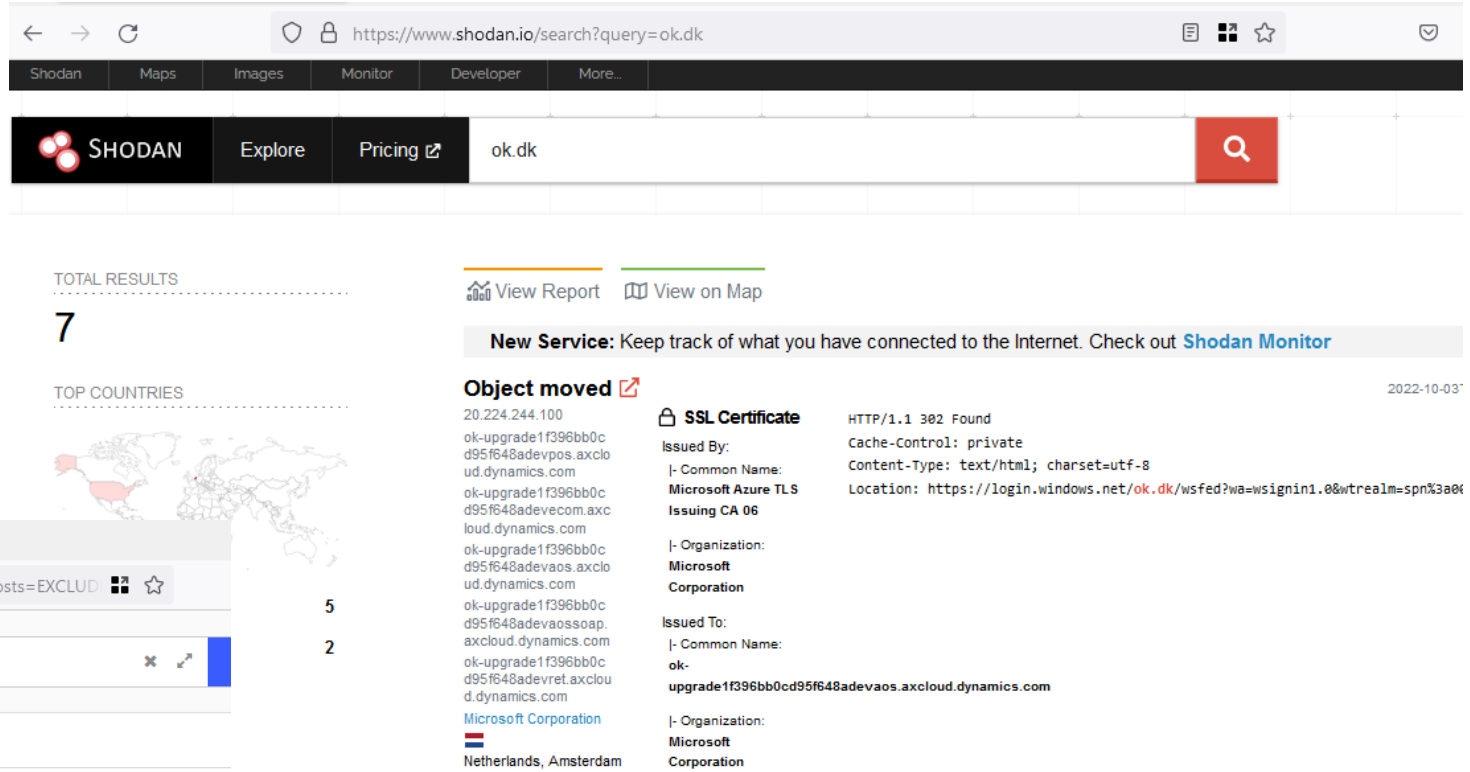
https://www.ransom-db.com/real-time-updates

…an emerging trend with traditional organized crime syndicates and criminally minded technology professionals working together and pooling their resources and expertise…

Sources: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime



https://search.censys.io



https://www.shodan.io/search?query=ok.dk

Bring a company offline?

Source: https://www.youtube.com/watch?v=vn-lU3Zu3dw

The Future

"Assume Breach – Detect Compromise"

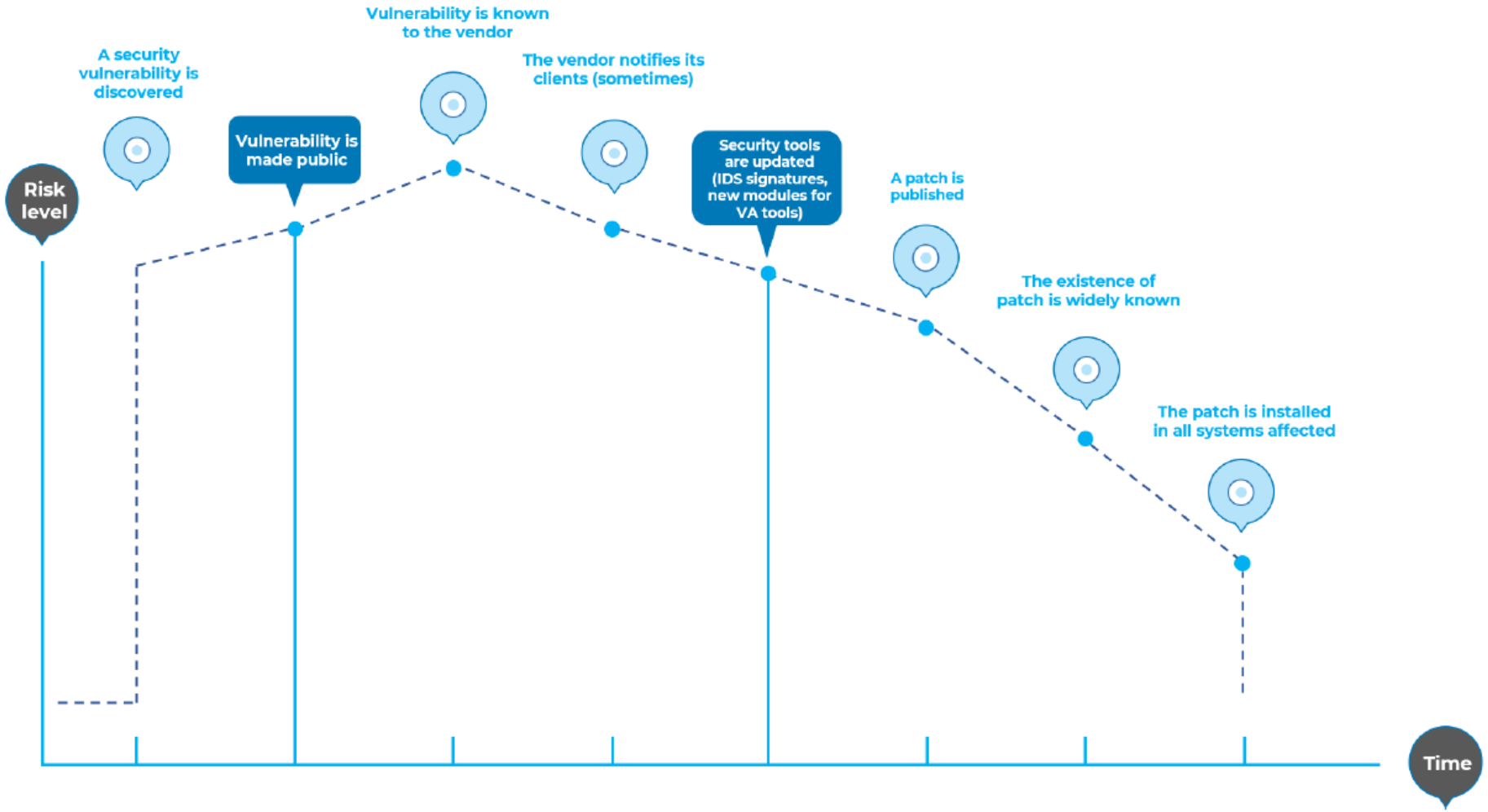
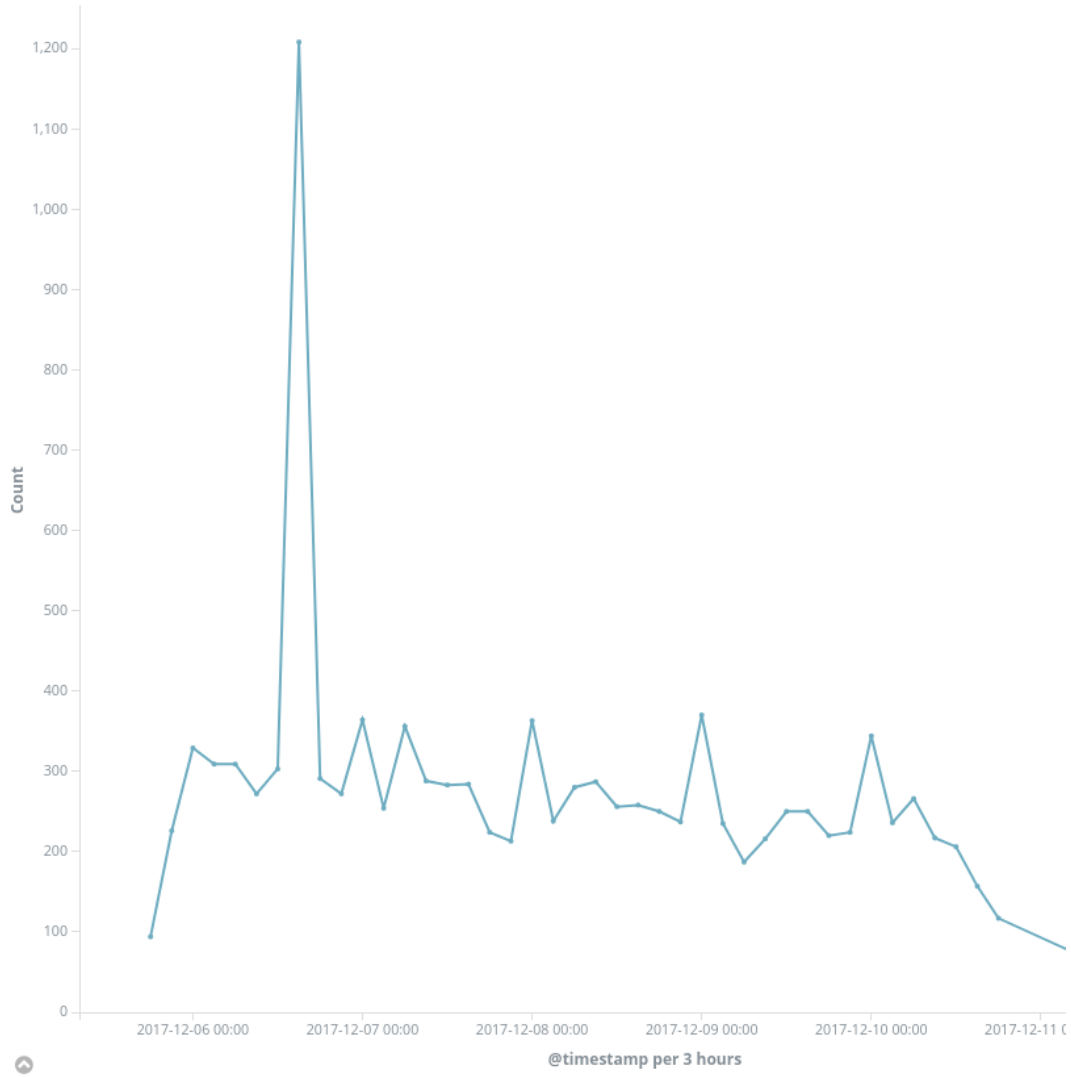
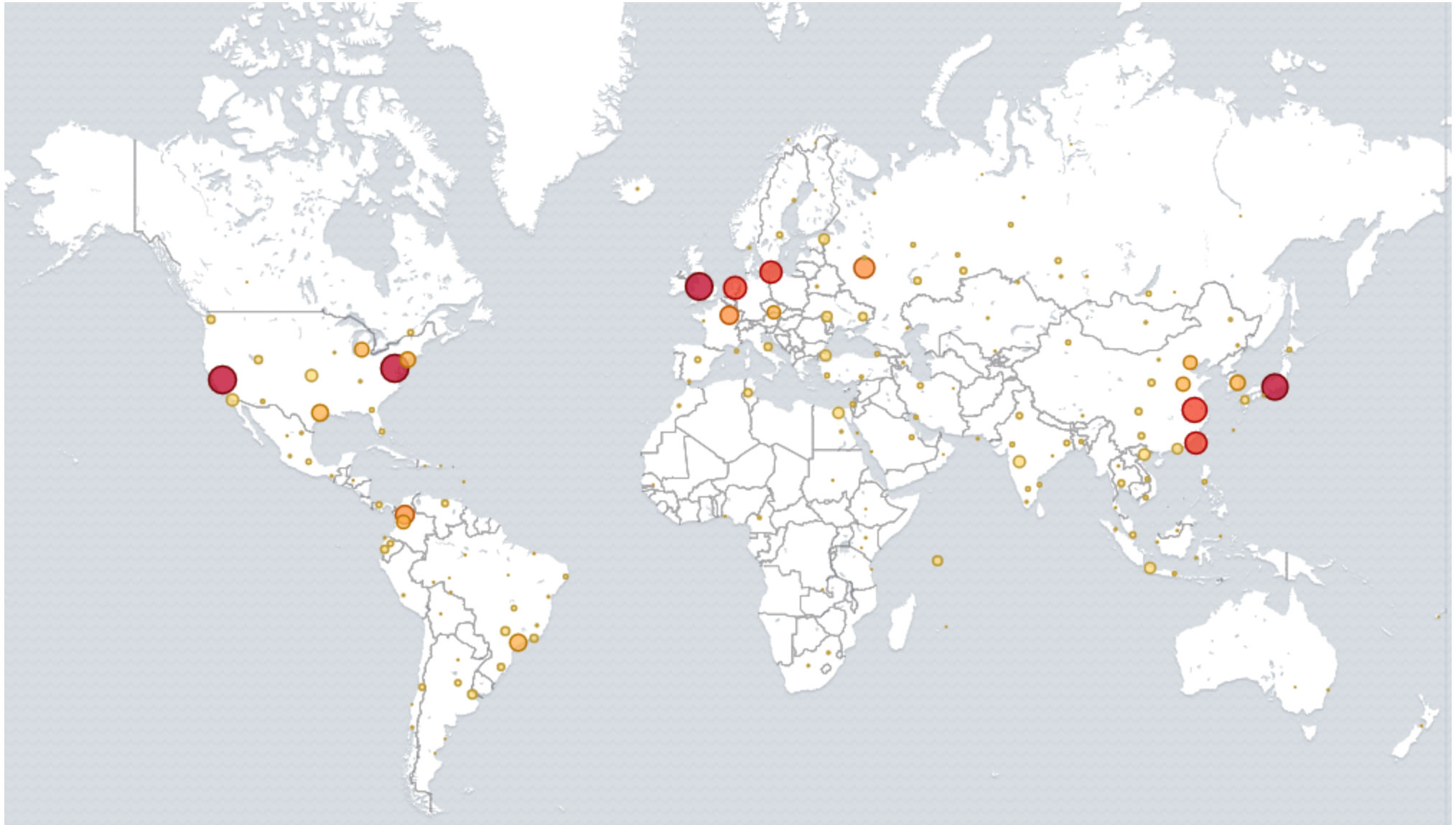


Figure 2-2: Window of Vulnerability

https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf


1,200
1,100
1,000
900
800
700
600
500
400
300
200
100
0
Count
2017-12-06 00:00
2017-12-07 00:00
2017-12-08 00:00
2017-12-09 00:00
2017-12-10 00:00
@timestamp per 3 hours

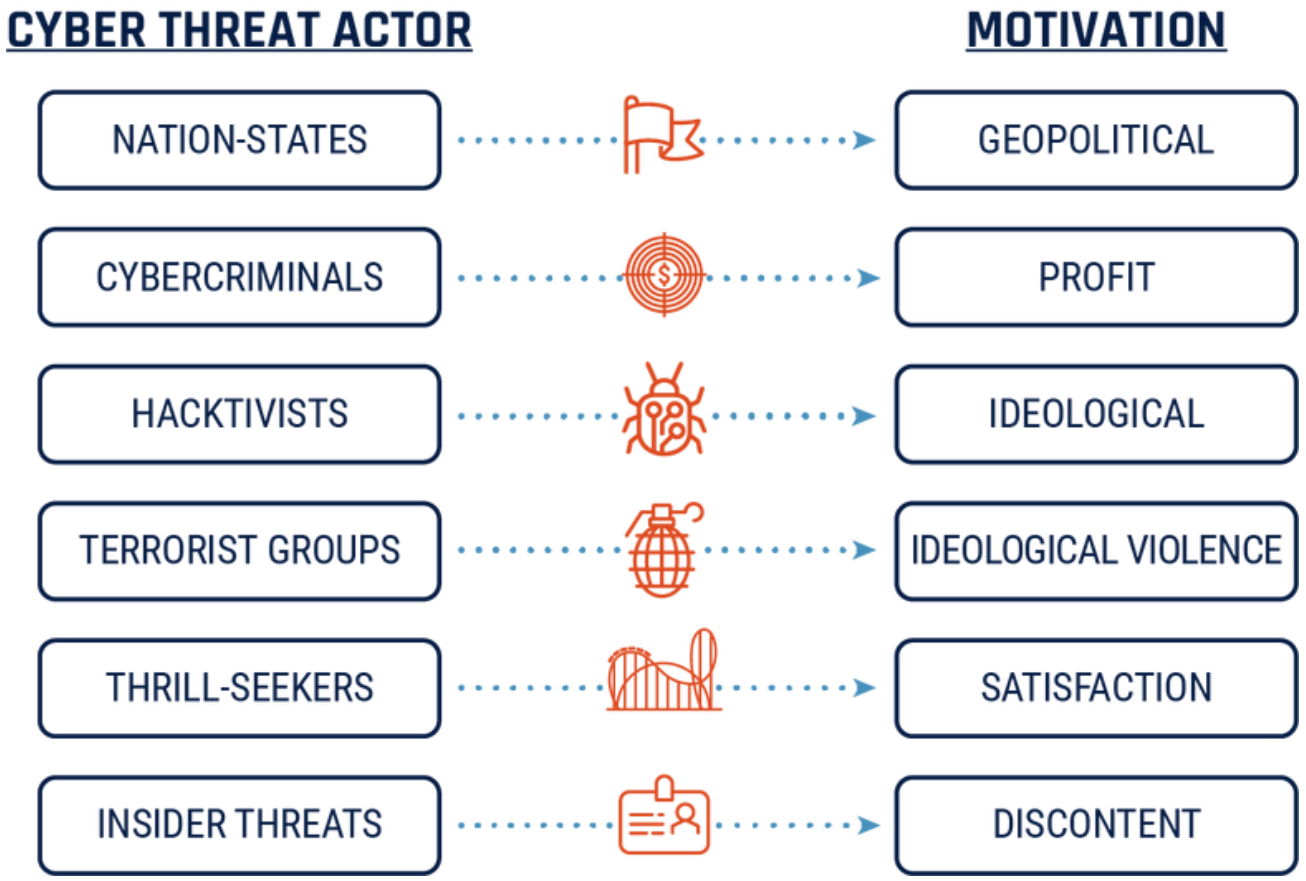


“There are only two types of companies: Those that have been hacked, and those that will be.”

Former FBI Director, Rubert Muller

“There are only two types of companies: Those that have been hacked, and those who don’t know they have been hacked.”

Former CEO at Cisco, John T. Chamber



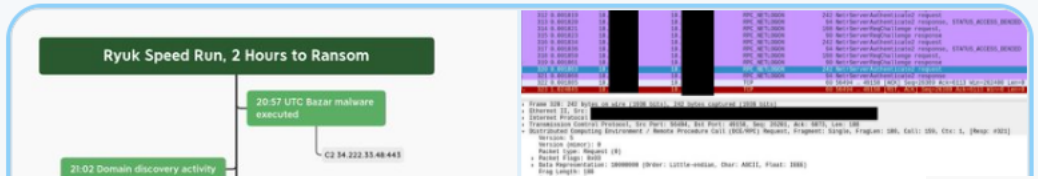
https://vividcomm.com/2019/04/15/threat-actors/

The DFIR Report @TheDFIRReport · Nov 5

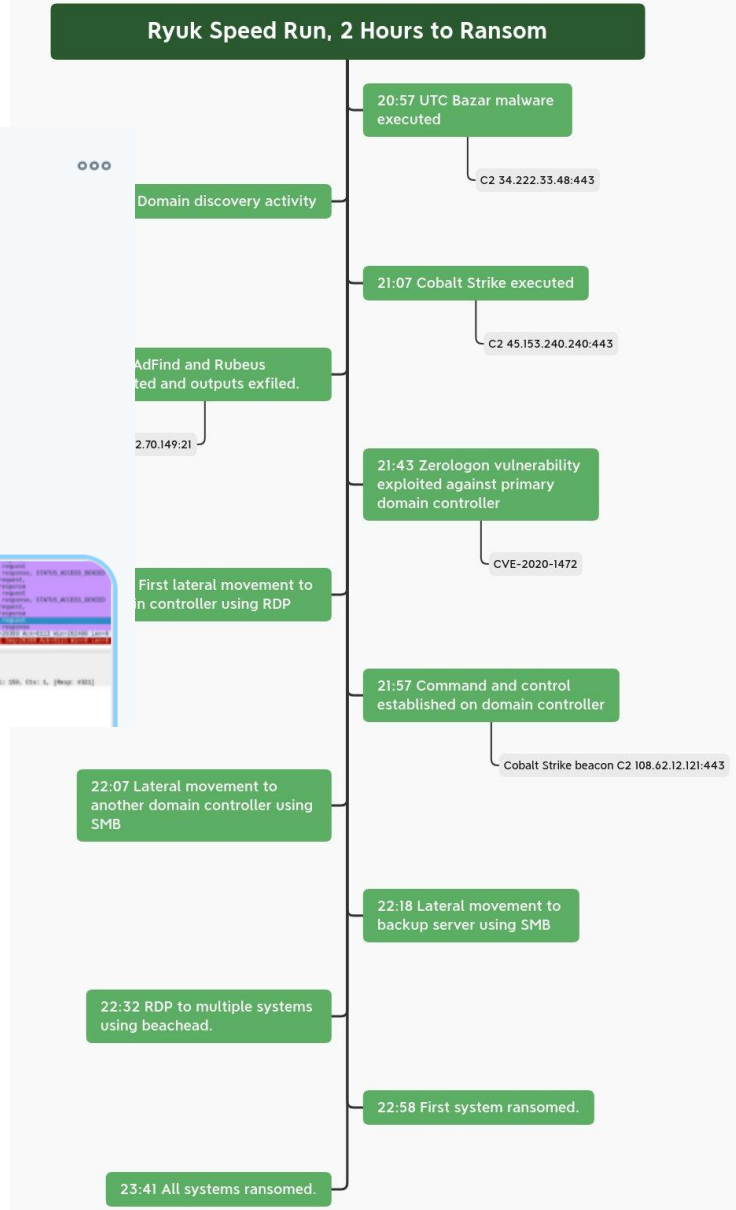
Ryuk Speed Run, 2 Hours to Ransom

- Discovery using Net, NItest, and AdFind
- Cobalt Strike and Bazar for C2
- Zerologon for Privilege Escalation
- Credential Access via Rubeus
- Lateral Movement via SMB

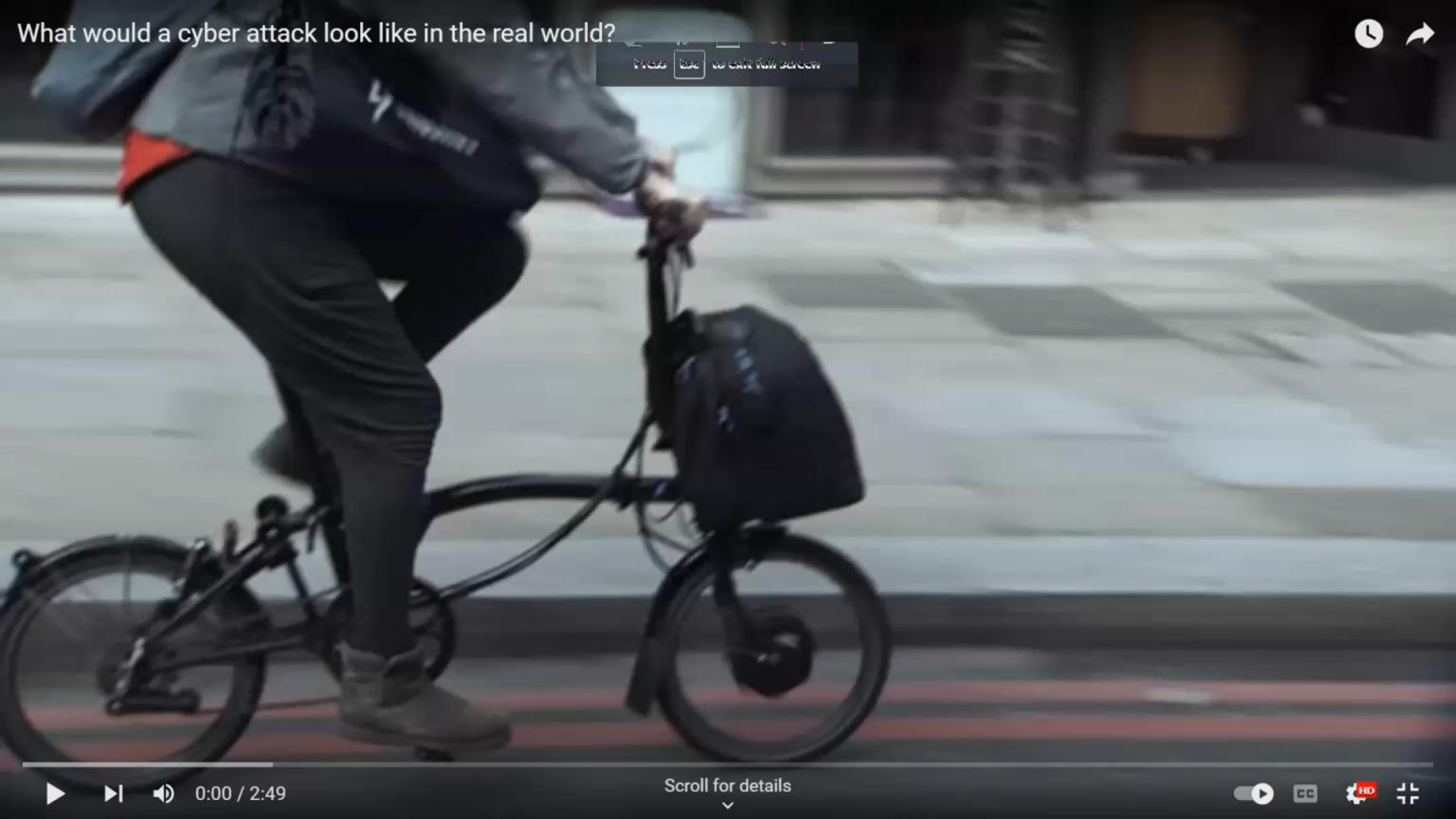
thedfirreport.com/2020/11/05/ryu...



https://twitter.com/TheDFIRReport/status/1324408962318557184/

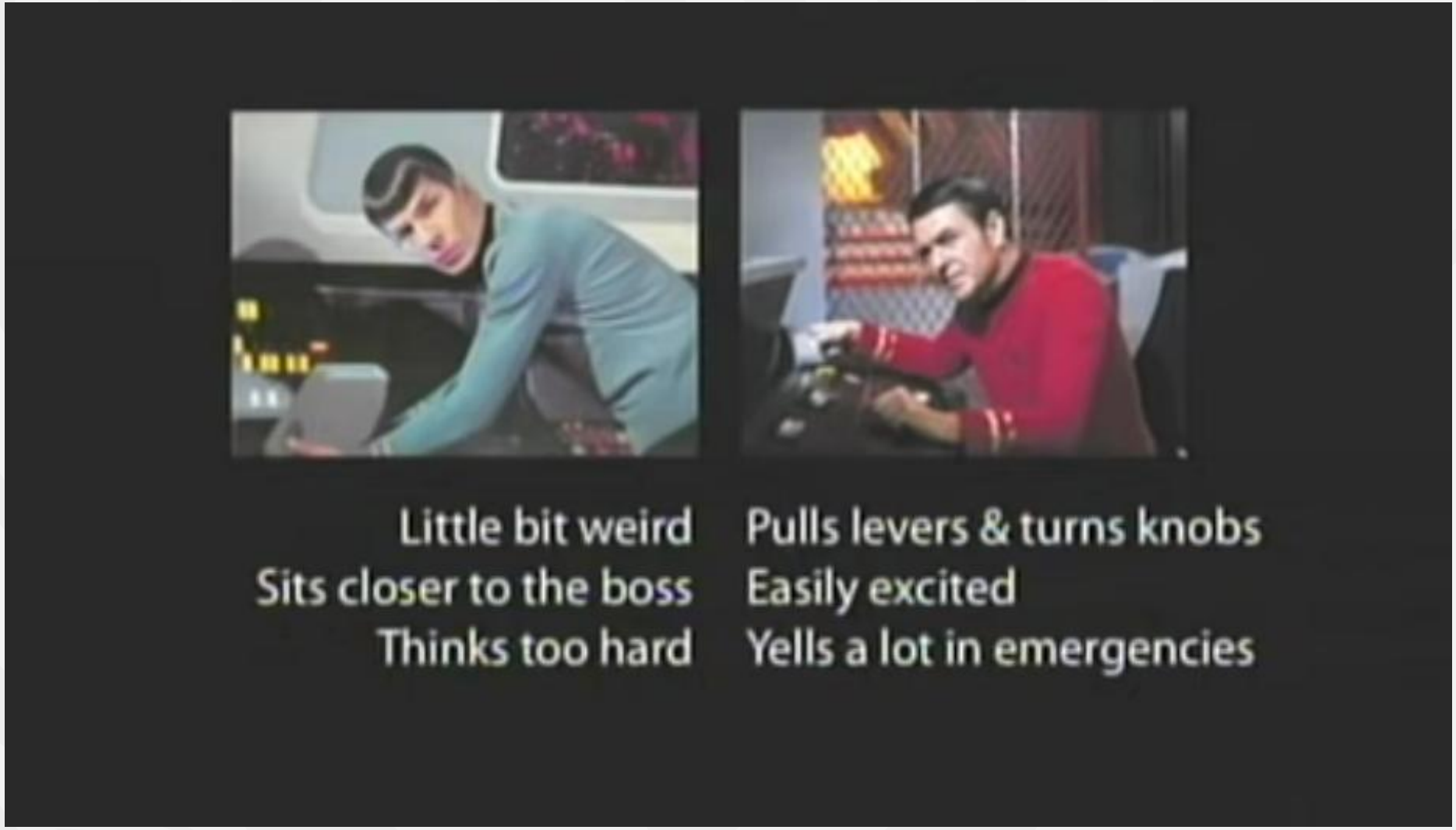


https://twitter.com/TheDFIRReport/status/1324408962318557184/photo/1


What would a cyber attack look like in the real world?
0:00 / 2:49
Scroll for details

Developer

"But we are not a part of the problem, right?"


Little bit weird
Sits closer to the boss
Thinks too hard
Pulls levers & turns knobs
Easily excited
Yells a lot in emergencies

Windows 95 Launch

5.525.158 visninger...

98.353 KAN IKKE LIDE DEL GEM

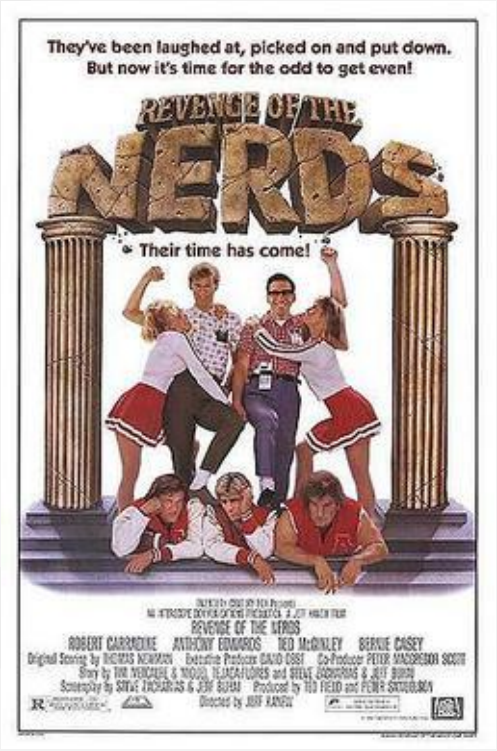
Windows 95 Launch - https://www.youtube.com/watch?v=lAkuJXGldrM

Windows 95 Launch

0:00 / 0:24

Scroll for details

Rolling Stones “Start me up”



Windows 95 Launch

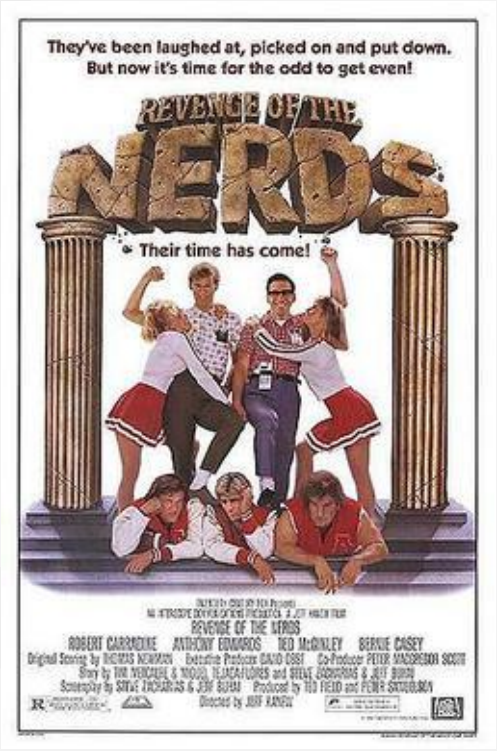
5.525.158 visninger...

98.353 KAN IKKE LIDE DEL GEM ...

Windows 95 Launch - https://www.youtube.com/watch?v=lAkuJXGldrM

Rolling Stones “Start me up”

“You make a grown man cry”



Windows 95 Launch

5.525.158 visninger...

98.353 KAN IKKE LIDE DEL GEM ...

Windows 95 Launch - https://www.youtube.com/watch?v=lAkuJXGldrM

2019 - Steve Ballmer Developers, Developers, Developers - https://www.youtube.com/watch?v=SaVTHG-Ev4k


Steve Ballmer Developers, Developers, Developers
Press Esc to exit full screen
Microsoft
0:00 / 0:19
Scroll for details

Building Blocks and Abstraction

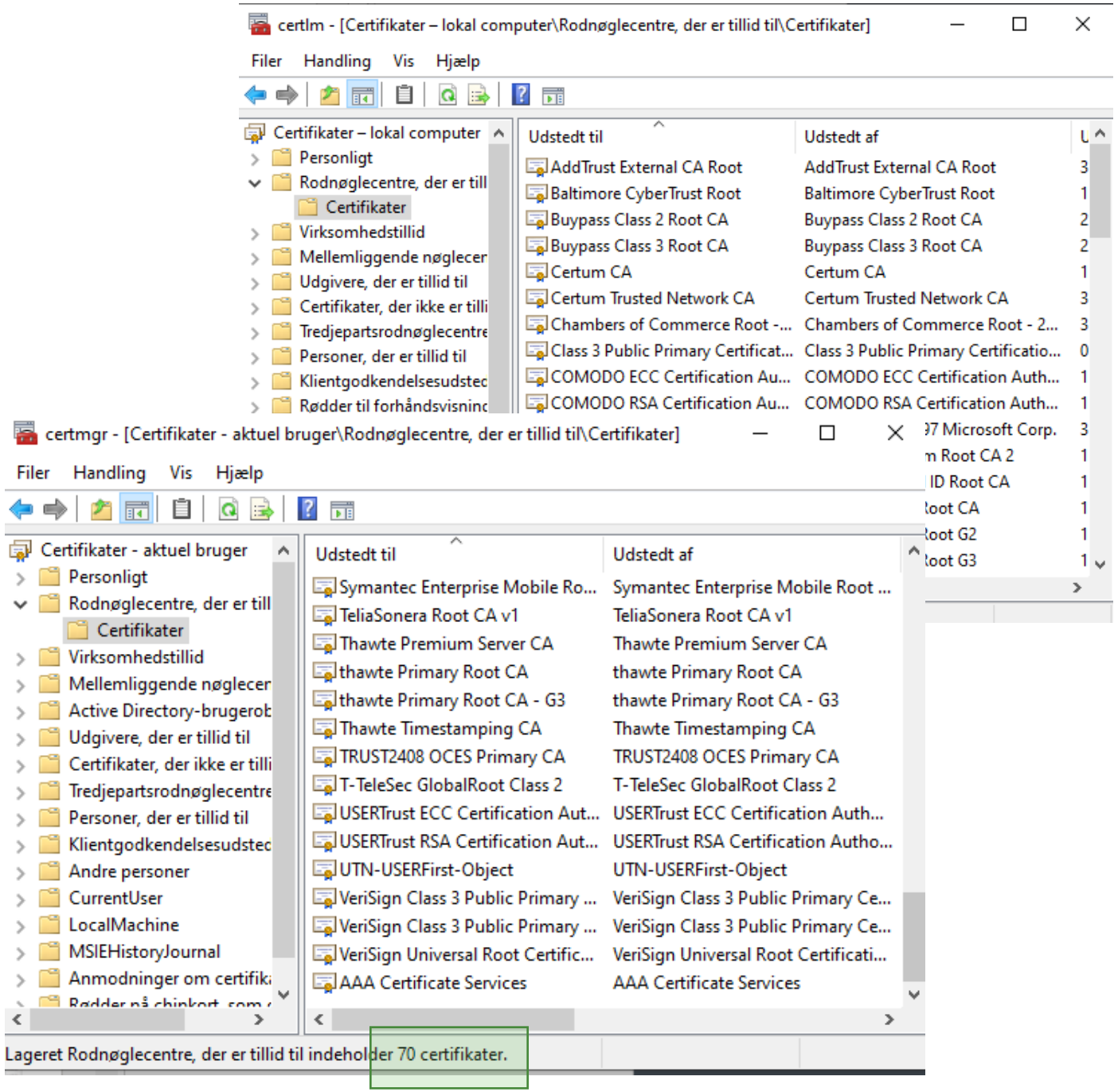
https://www.lego.com/en-dk/product/hogwarts-castle-71043

https://en.wikipedia.org/wiki/Turtles_all_the_way_down

Whom do we trust to impersonate everyone else!?

Certificate Manager – Local and Personal

Note, some systems/platforms/frameworks maintain their own!



cloud native wiki
by aqua

Enter search term

- Containerized Architecture
- DevSecOps
- Cloud Native Applications
- Kubernetes in Production
- Serverless Architecture
- Container Platforms
- Docker Container
  - Container Monitoring

Docker CIS Benchmark: Best Practices in Brief

Get the gist of the Docker CIS Benchmark recommendations for host configuration, Docke
Daemon configuration and more, and learn to automate security testin

What is Docker CIS Benchmark?

https://www.aquasec.com/cloud-native-academy/docker-container/docker-cis-benchmark/

```
root@123bb443a4f6: /
Ident   CCE-
Result  notapplicable

Title   Set SSH Idle Timeout Interval
Rule    xccdf_org.ssgproject.content_rule_sshd_set_idle_timeout
Ident   CCE-
Result  notapplicable

Title   Set SSH Client Alive Count
Rule    xccdf_org.ssgproject.content_rule_sshd_set_keepalive
Ident   CCE-
Result  notapplicable

Title   Disable SSH Root Login
Rule    xccdf_org.ssgproject.content_rule_sshd_disable_root_login
Ident   CCE-
Result  notapplicable

Title   Disable SSH Access via Empty Passwords
Rule    xccdf_org.ssgproject.content_rule_sshd_disable_empty_passwords
Ident   CCE-
Result  notapplicable
```

```
tlk@development: ~/Desktop/source_code/docker-bench-security
[INFO] 2.7 - Ensure TLS authentication for Docker daemon is configured (Scored)
[INFO]      * Docker daemon not listening on TCP
[INFO] 2.8 - Ensure the default ulimit is configured appropriately (Manual)
[INFO]      * Default ulimit doesn't appear to be set
[WARN] 2.9 - Enable user namespace support (Scored)
[PASS] 2.10 - Ensure the default cgroup usage has been confirmed (Scored)
[PASS] 2.11 - Ensure base device size is not changed until needed (Scored)
[WARN] 2.12 - Ensure that authorization for Docker client commands is enabled (S
cored)
[WARN] 2.13 - Ensure centralized and remote logging is configured (Scored)
[WARN] 2.14 - Ensure containers are restricted from acquiring new privileges (Sc
ored)
[WARN] 2.15 - Ensure live restore is enabled (Scored)
[WARN] 2.16 - Ensure Userland Proxy is Disabled (Scored)
[PASS] 2.17 - Ensure that a daemon-wide custom seccomp profile is applied if app
ropriate (Manual)
[IN
ed)
```

OpenSCAP Security Guide

Profile: CIS Ubuntu 20.04 Level 1 Server Benchmark

select a profile to display its guide and a command line snippet needed to use it

Guide to the Secure Configuration of Ubuntu 20.04

with profile CIS Ubuntu 20.04 Level 1 Server Benchmark

— This baseline aligns to the Center for Internet Security
Ubuntu 20.04 LTS Benchmark, v1.0.0, released 07-21-2020.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide

This guide presents a catalog of security-relevant configuration settings for Ubuntu 20.04. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

http://static.open-scap.org/ssg-guides/ssg-ubuntu2004-guide-index.html

```
tlk@development:~/Desktop/source_code$ sudo grype ubuntu:latest
 ✔ Vulnerability DB        [no update available]
 ✔ Loaded image
 ✔ Parsed image
 ✔ Cataloged packages      [101 packages]
 ✔ Scanned image           [20 vulnerabilities]
NAME          INSTALLED              FIXED-IN                TYPE  VULNERABILITY   SEVERITY
coreutils     8.32-4.1ubuntu1                                deb   CVE-2016-2781   Low
dpkg          1.21.1ubuntu2          1.21.1ubuntu2.1         deb   CVE-2022-1664   Medium
e2fsprogs     1.46.5-2ubuntu1                                deb   CVE-2022-1304   Medium
libcom-err2   1.46.5-2ubuntu1                                deb   CVE-2022-1304   Medium
libext2fs2    1.46.5-2ubuntu1                                deb   CVE-2022-1304   Medium
libgmp10      2:6.2.1+dfsg-3ubuntu1                          deb   CVE-2021-43618  Low
libpcre2-8-0  10.39-3build1                                  deb   CVE-2022-1587   Low
libpcre2-8-0  10.39-3build1                                  deb   CVE-2022-1586   Low
libpcre3      2:8.39-13build5                                deb   CVE-2017-11164  Negligible
libpcre3      2:8.39-13build5        2:8.39-13ubuntu0.22.04.1 deb  CVE-2019-20838  Low
libss2        1.46.5-2ubuntu1                                deb   CVE-2022-1304   Medium
libssl3       3.0.2-0ubuntu1         3.0.2-0ubuntu1.1        deb   CVE-2022-1292   Medium
libssl3       3.0.2-0ubuntu1         3.0
```

```
tlk@development:~/Desktop/source_code$ sudo grype alpine:latest
 ✔ Vulnerability DB        [no update available]
 ✔ Loaded image
 ✔ Parsed image
 ✔ Cataloged packages      [14 packages]
 ✔ Scanned image           [0 vulnerabilities]
No vulnerabilities found
tlk@development:~/Desktop/source_code$
```

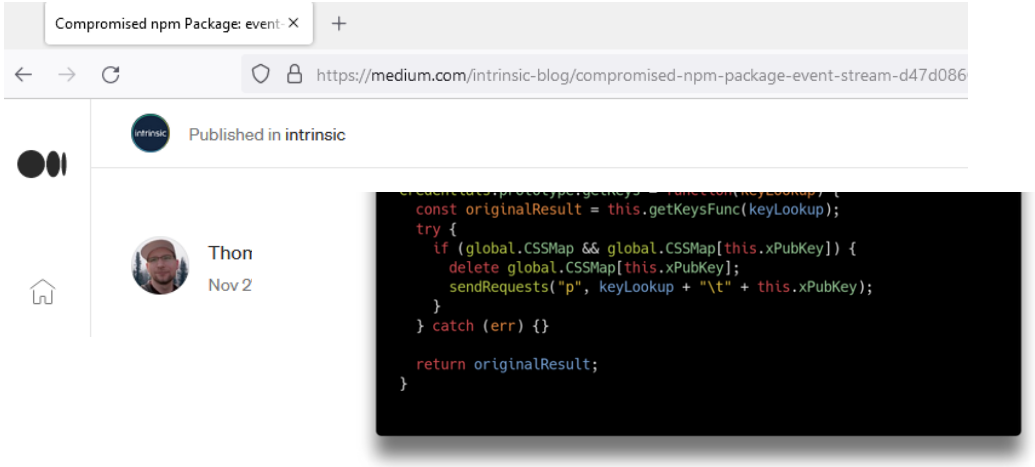
Grype - https://github.com/anchore/grype

https://www.version2.dk/artikel/javascript-bibliotek-overskriver-russiske-filer-med-hjertesymboler?utm_source=nyhedsbrev&utm_medium=email&utm_campaign=v2_daglig

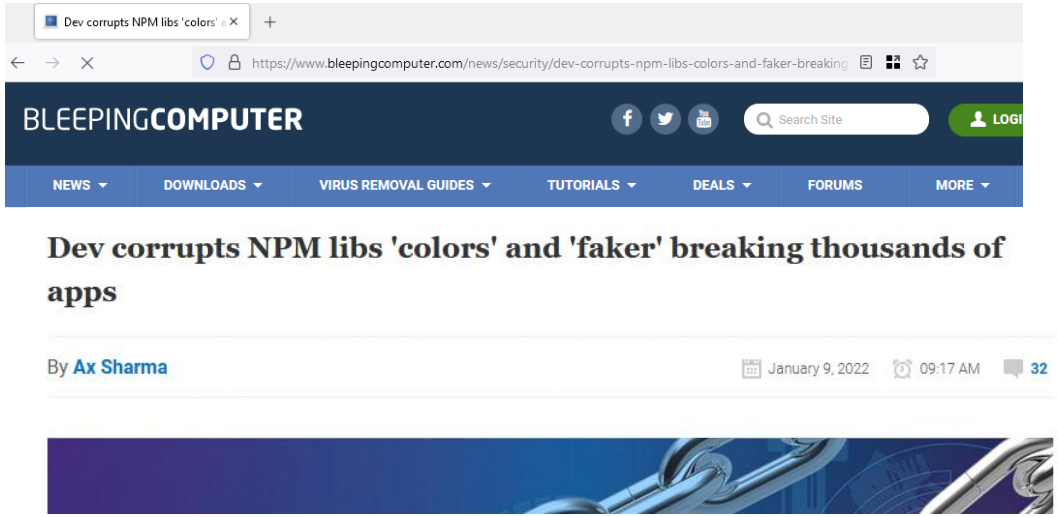
https://www.version2.dk/artikel/microsoft-ansatte-laekker-login-oplysninger-til-interne-systemer-paa-github

https://snyk.io/blog/peacenotwar-malicious-npm-node-ipc-package-vulnerability/

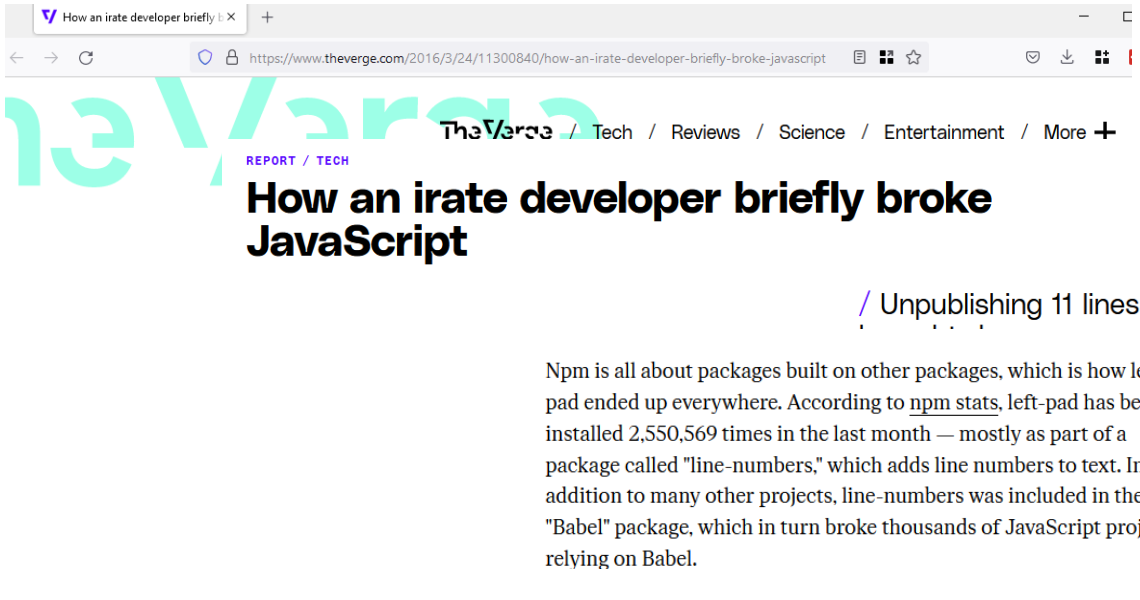
https://www.theregister.com/2016/03/23/npm_left_pad_chaos/



https://medium.com/intrinsic-blog/compromised-npm-package-event-stream-d47d08605502



https://www.bleepingcomputer.com/news/security/dev-corrupts-npm-libs-colors-and-faker-breaking-thousands-of-apps/



https://www.theverge.com/2016/3/24/11300840/how-an-irate-developer-briefly-broke-javascript

https://www.zdnet.com/article/more-than-75-of-all-vulnerabilities-reside-in-indirect-dependencies/

ZDNET

tomorrow
belongs to those who embrace it
today

trending innovation home & office business finance education security

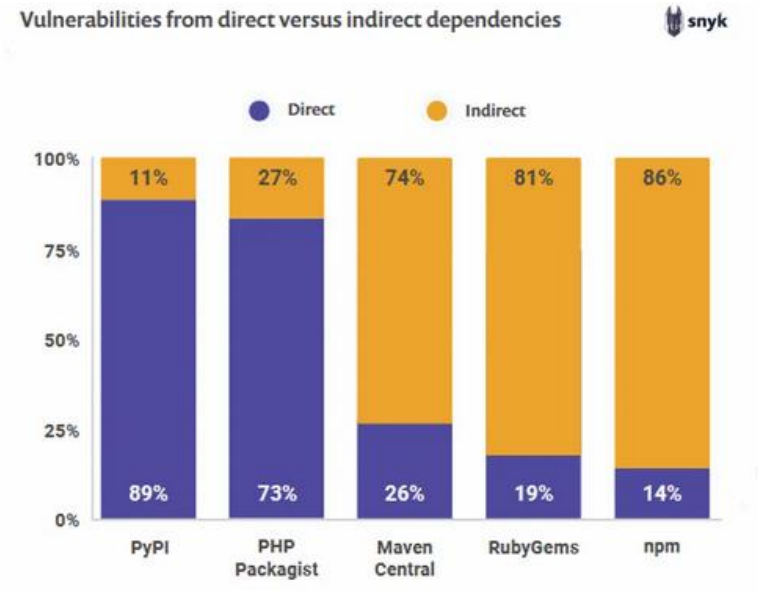
/ innovation

Home / Innovation / Security

More than 75% of all vulnerabilities reside in indirect dependencies

JavaScript, Ruby, and Java are the ecosystems with most bugs in indirect dependencies.

Written by **Catalin Cimpanu**, Contributor on June 26, 2020



"Ask any Node developer, and they probably have a story of waiting for long periods to open a project while npm is trying to pull all the necessary dependencies," Miller added. "One of our favorite examples is an 80 line Java application that specifies 7 dependencies. When you walk the entire dependency tree, however, you find 59 sub-dependencies, and suddenly, the 80 lines of code turns into 740,000 lines.

But the Snyk team also pointed to another quirck in their report, namely that "malicious packages" ranked as the second most common type of security issue they found in projects last year.

This refers to open-source libraries that have either been created to be malicious on purpose, or libraries where the developer account was hacked and the code poisoned.

https://www.zdnet.com/article/more-than-75-of-all-vulnerabilities-reside-in-indirect-dependencies/

http://ars.userfriendly.org/cartoons/?id=20061029

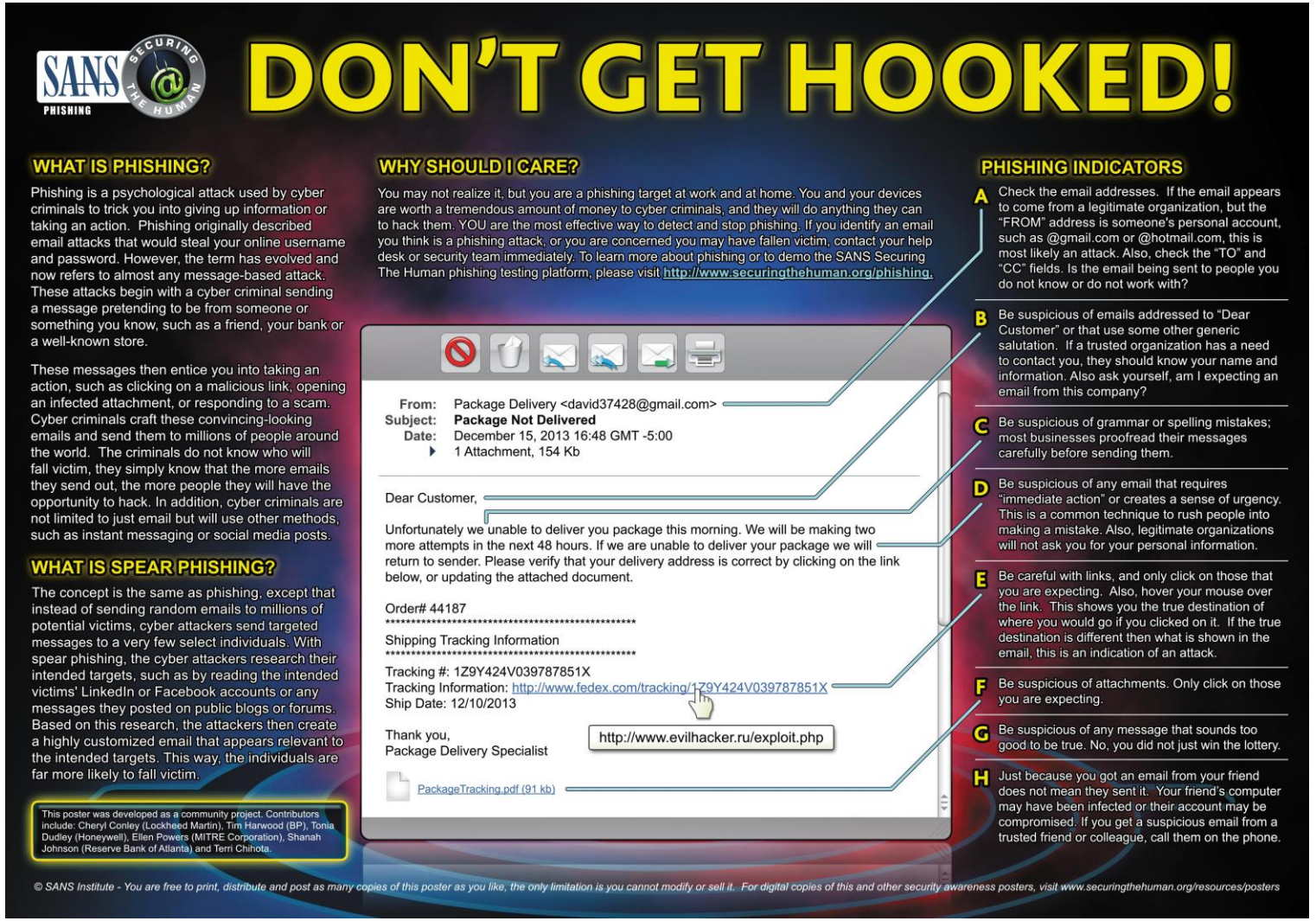
Ten Immutable Laws Of Security (Version 2.0)

Law #1	If a bad guy can persuade you to run his program on your computer, it's not solely your computer anymore
Law #2	If a bad guy can alter the operating system on your computer, it's not your computer anymore.
Law #3	If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
Law #4	If you allow a bad guy to run active content in your website, it's not your website anymore.
Law #5	Weak passwords trump strong security.
Law #6	A computer is only as secure as the administrator is trustworthy.
Law #7	Encrypted data is only as secure as its decryption key.
Law #8	An out-of-date antimalware scanner is only marginally better than no scanner at all.
Law #9	Absolute anonymity isn't practically achievable, online or offline.
Law #10	Technology is not a panacea.

https://docs.microsoft.com/da-dk/archive/blogs/rhalbheer/ten-immutable-laws-of-security-version-2-0

Demo

Phishing



https://www.sans.org/blog/new-security-awareness-poster-dont-get-hooked/

Fra: Info Nets <noreply@nets.com>
Dato: 8. marts 2017 kl. 10.07.57 CET
Til:
Emne: Adgang Til Dine Konto

Kære kunder Nets,

Det ser ud til, at en anden bruger din konto.

For din sikkerhed, har vi blokeret din konto
Vi har brug for nogle oplysninger for at løse dette problem

> Klik her https://www.nets.eu/dk-da/I%C3%B8sninger/dankort/022136(

© Nets i Danmark (HQ)-kontoteamet

POST

Du har uforløste pakken

Vi har modtaget din pakke **CT5389919582DK** på **2015/09/21**. Courier var ude af stand til at levere denne pakke til dig

Få og udskrive forsendelsesetiketten, og vise det på det nærmeste posthus for at få din pakke.

Få en adresselapp

Hvis pakken ikke er modtaget inden 20 arbejdsdage PostNord AB vil være berettiget til at kræve kompensation fra dig - 55 kroner for hver dag i at holde. Du kan finde oplysninger om fremgangsmåden ved og betingelserne af pakken holde i det nærmeste kontor.

Dette er en automatisk genereret meddelelse. Klik her for at afmelde

Fra: **Skat.dk** <skat@skat.dk>
Dato: 1. okt. 2013 12.00
Emne: ID:38933 - tilbagebetaling af skat - DKK 6940,00
Til: XXX

SKAT

Bemærk: Tilbagebetaling af skat for året 2012

Kære skatteyder,

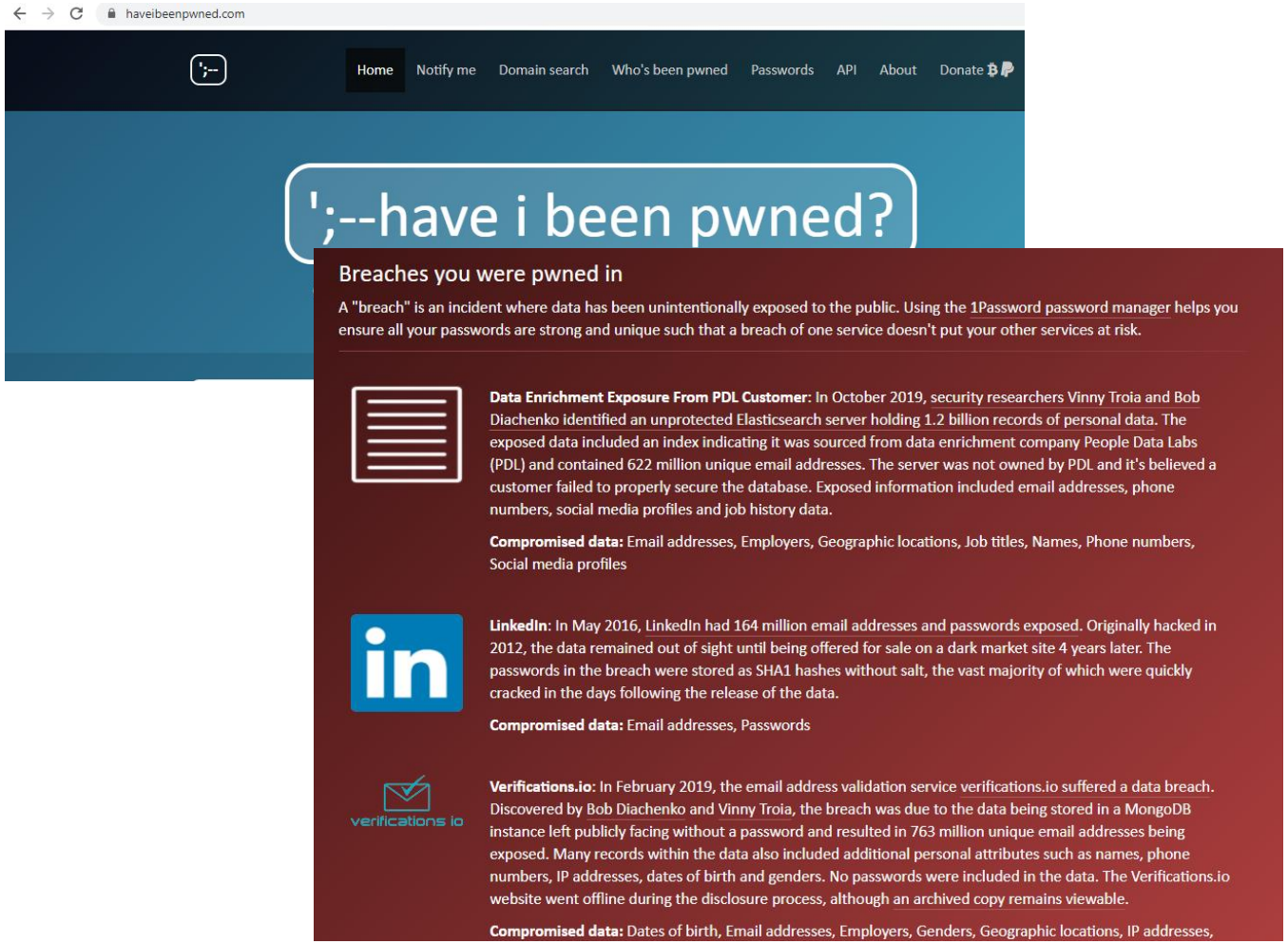
Vores registreringer viser, at du er kvalificeret til en tilbagebetaling af skat af:
DKK 6940,00

For at få adgang til din skat tilbagebetaling, klik venligst her.

Udfyld venligst formularen indtil d. **02-10-2013.**
Den hurtigste og nemmeste måde at modtage din tilbagebetaling på er ved direkte inc
check/opsparingskonto.

Vores hovedkontor adresse kan findes på vores hjemmeside på
http://www.skat.dk

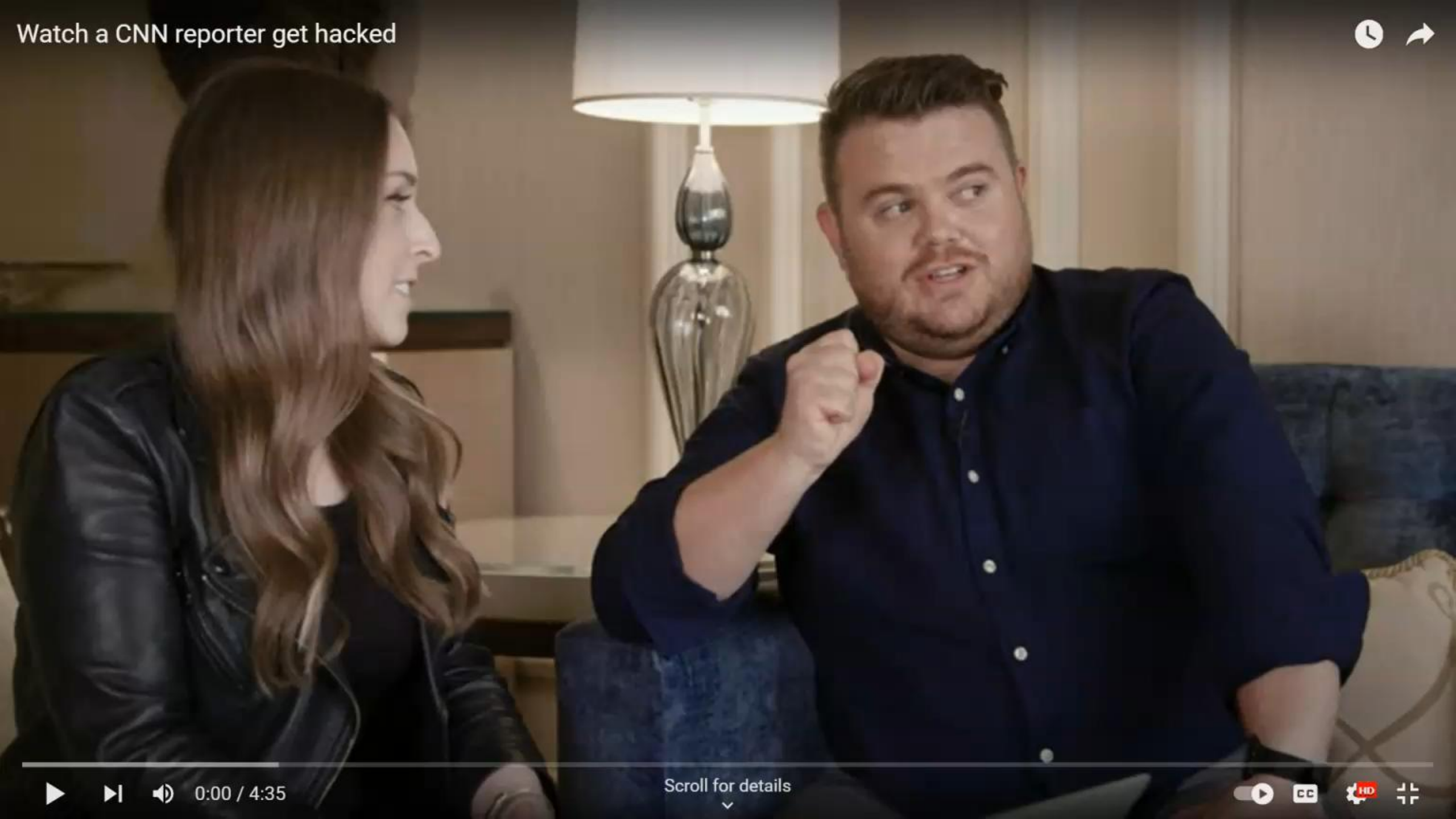
http://www.it-blogger.dk/post-nord-virus-rammer-danmark/, http://skat.dk/SKAT.aspx?oId=68747 and https://www.nets.eu/dk-da/digital-sikkerhed/Pages/Phishing.aspx



https://haveibeenpwned.com/

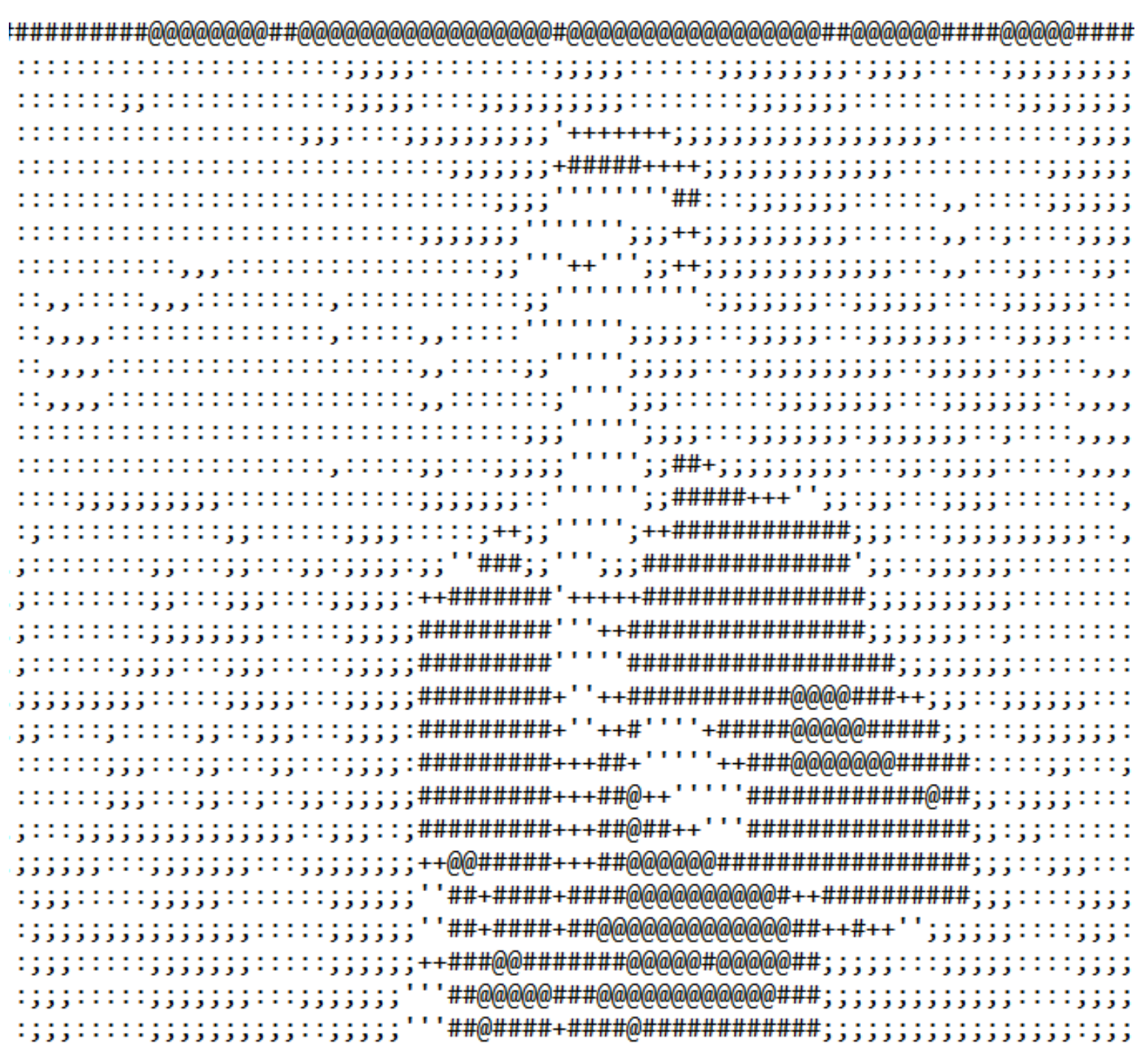
103	sdsda@ok.dk	4
104	spt@ok.dk	16
105	tbr@ok.d	1
106	tbr@ok.dk	5
107	tdr@ok.dk	2
108	teg@ok.dk	1
109	TGU@ok.dk	5
110	Thlj@ok.dk	10
111	THN@ok.dk	4
112	tnr@ok.dk	11
113	**Grand Total**	**823**
114		
115		

Row Labels	Count of password
ok **** ko	55
to **** un	46
al **** 12	46
qa **** 12	25
mr **** dw	23
12 **** 45	21
si **** on	18
so **** ri	18
he **** he	18


Watch a CNN reporter get hacked
0:00 / 4:35
Scroll for details

Demo

I am never going to give you up!



You can have Security without Privacy, but you cannot have Privacy without Security

Out-of-scope

01 For godt til at være sandt!

Hvis tilbuddet eller emailen er for godt til at være sandt…. Så er det nok ikke sandt!

02 Hastende!

Hvis det haster, så du ikke har mulighed for at tænke dig om… Der er meget få ting i livet, som ikke kan vente til imorgen!

03 Hvem er afsender?

Selvom afsender ser rigtig ud, så behøver det ikke være tilfældet. Ring og få det bekræftigt!

04 Klik ikke på links

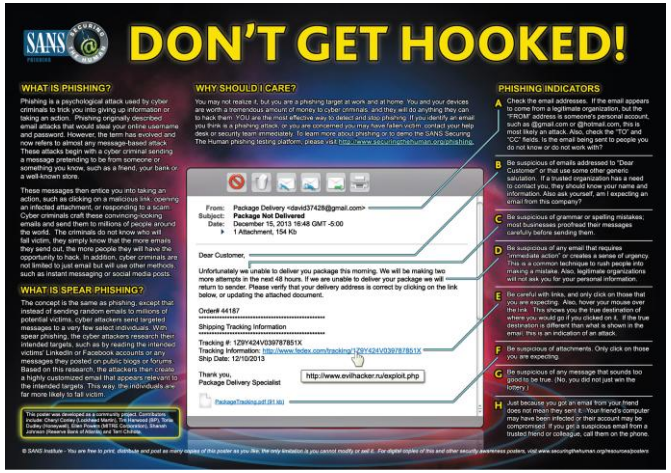
Lad være med at klikke på alle links, du modtager! Overvej evt. at taste dem selv!

05 Åben ikke alle vedhæftede filer

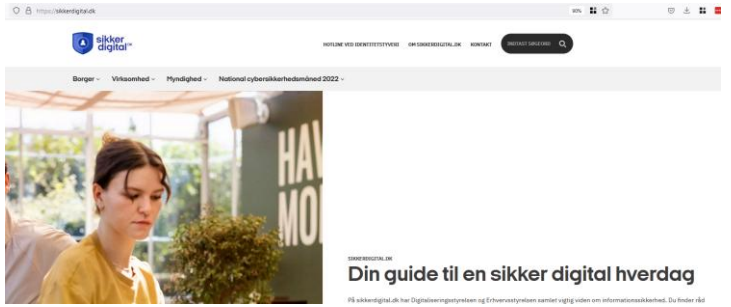
Hvis du ikke forventet at få filen, så lad være med at åbne den. Hvis du er i tvivl, så ring og spørg!

06 Vær skeptisk!

https://securingthehuman.sans.org/media/resources/STH-Poster-CyberSecureHome-Print.pdf

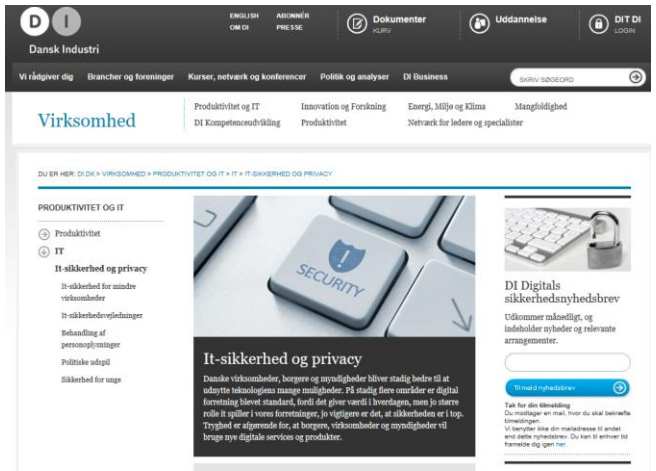


https://securingthehuman.sans.org/resources/posters

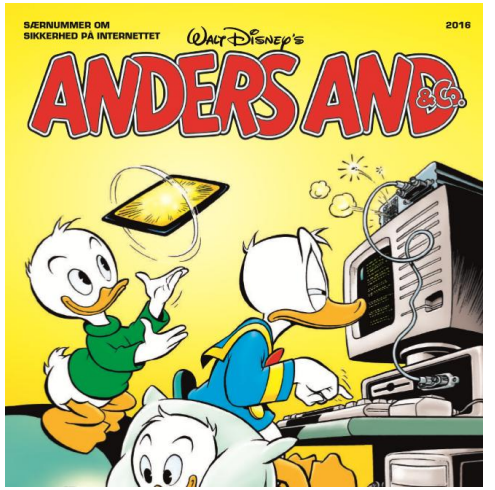


https://sikkerdigital.dk/

https://www.cert.dk/da/vejled

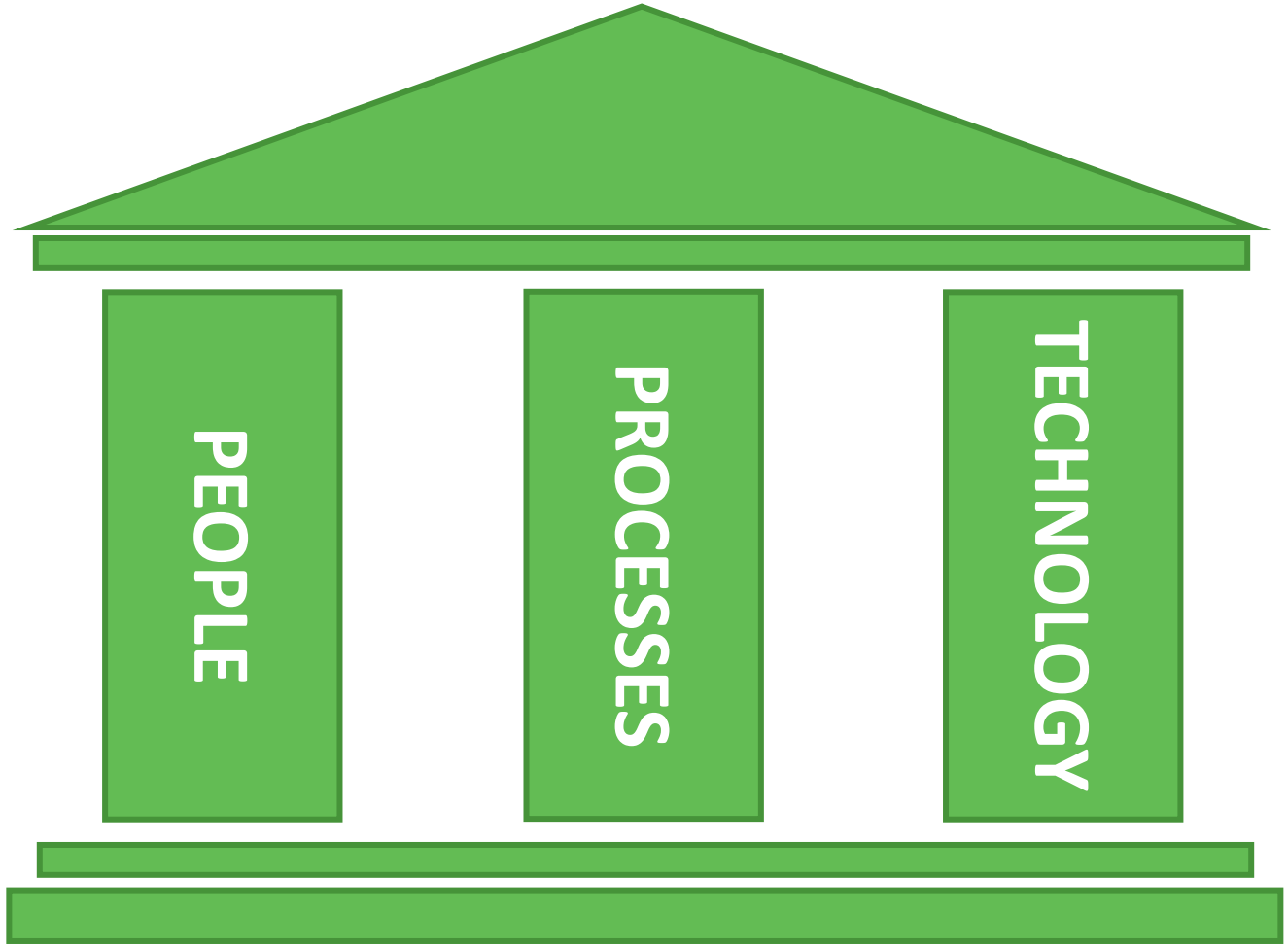


https://di.dk/Virksomhed/Produktion/IT/itsikkerhed/Pages/default.aspx



https://børneulykkesfonden.dk/laeringsmaterialer/hjemmet/tryg-pa-nettet-med-anders-and

The three pillars



The technology must support the processes supporting the people achieving their goals.

What is needed for the secure operation of the solution?

Best-practices:
OWASP Application Security Verification Standard (*OWASP ASVS*)

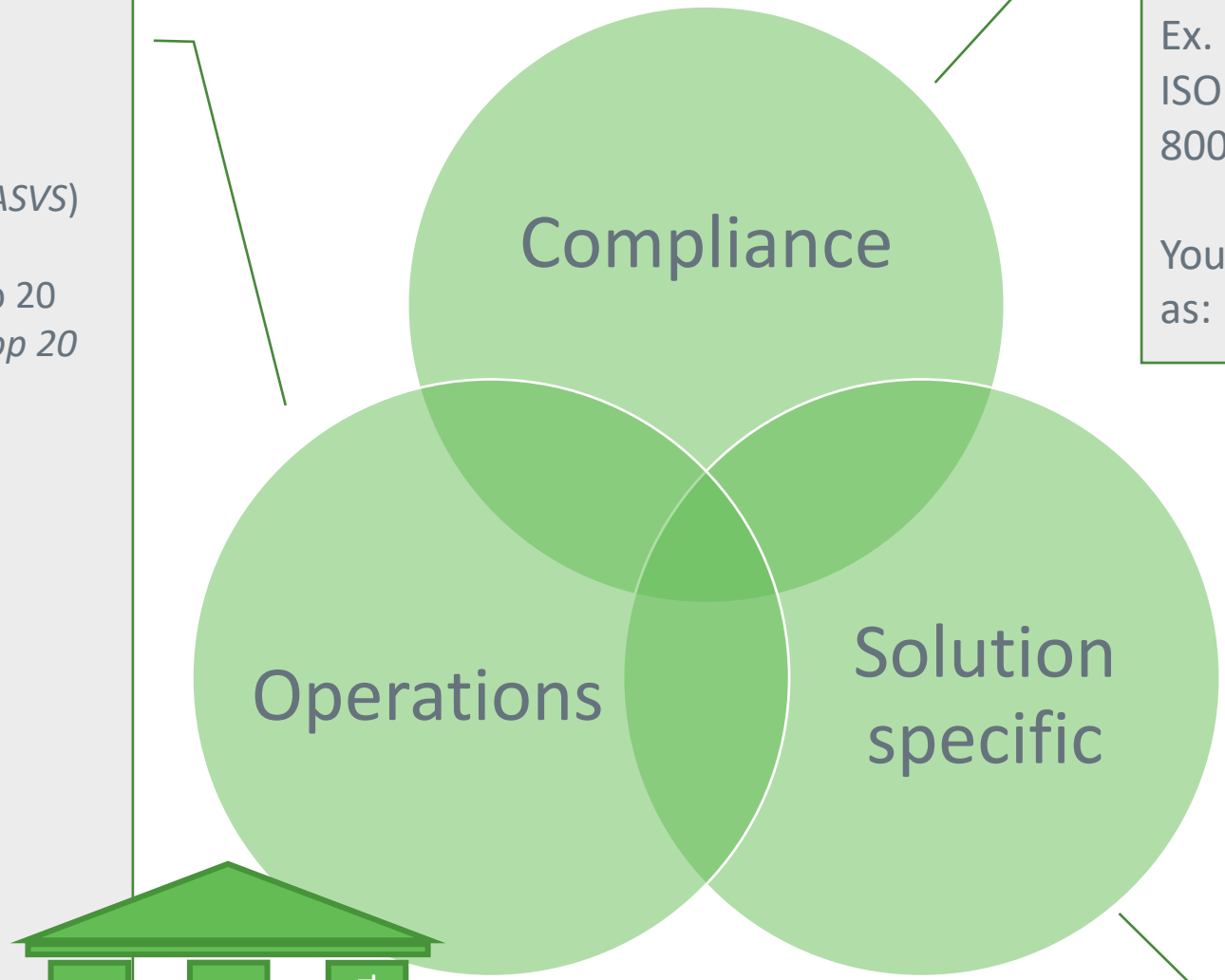
Center for Internet Security Top 20 Critical Security Controls (*CIS Top 20 or CIS Top 18*)

The Cyber KILL Chain

Catalog of Security Controls:
OWASP Proactive Controls
ISO 27002
NIST SP 800-53

Other:
MITRE ATTACK
Misuse/abuse cases

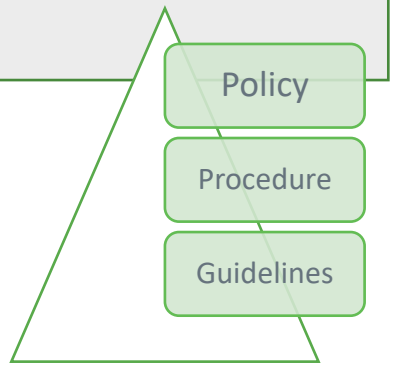
OWASP Software Assurance Maturity Model (SAMM)



Regulatory, Company-wide, etc.

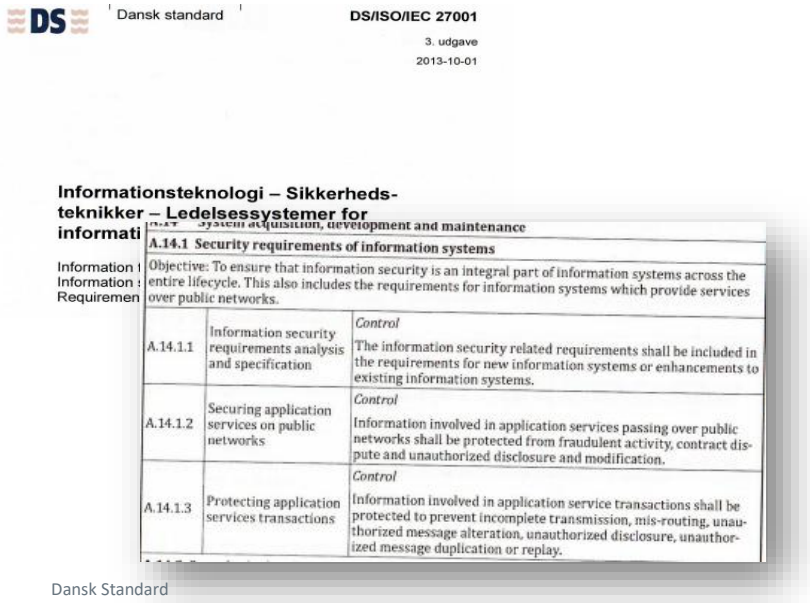
Ex.
ISO 27001, ISAE 3000, NIST SP 800, NIS, NIS2, GDPR and more

You should have access to these as:



Protection against specific threats and risk mitigating elements

We will come back to this!


Dansk standard DS/ISO/IEC 27001 3. udgave 2013-10-01

Informationsteknologi – Sikkerheds-teknikker – Ledelsessystemer for informati

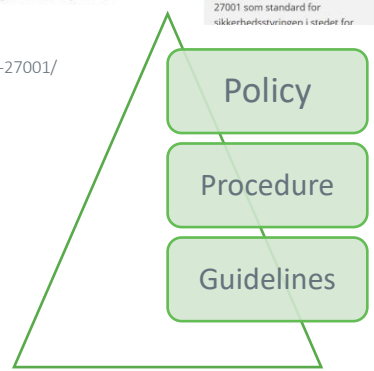
A.14.1 Security requirements of information systems

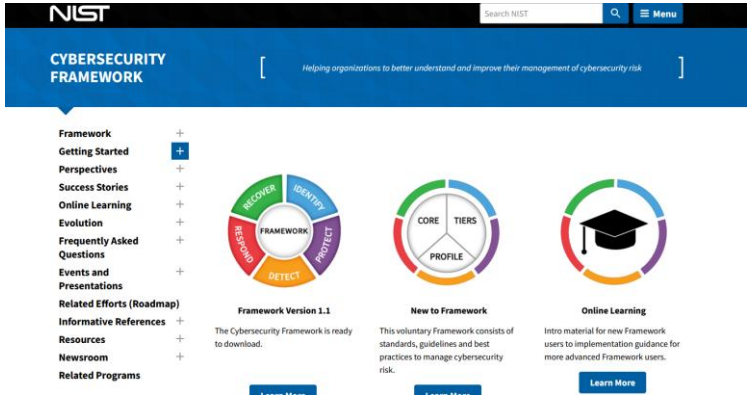
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

A.14.1.1	Information security requirements analysis and specification	Control: The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
A.14.1.2	Securing application services on public networks	Control: Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
A.14.1.3	Protecting application services transactions	Control: Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

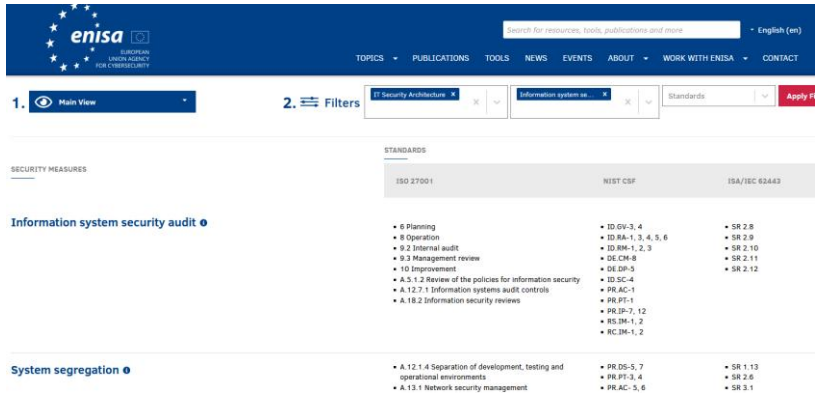
Dansk Standard

https://digst.dk/sikkerhed/iso-27001/hvad-er-iso-27001/

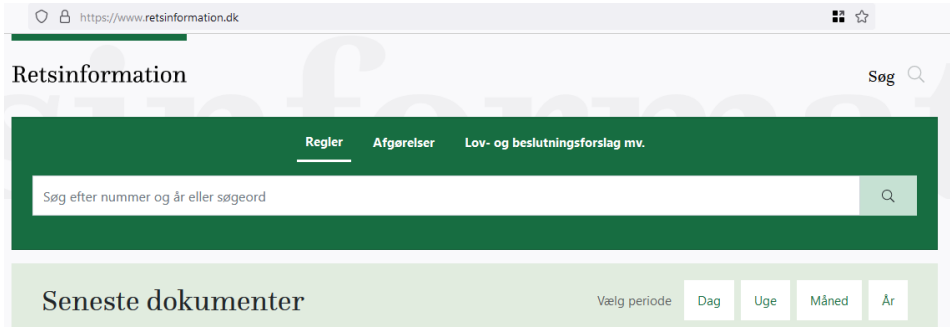




https://www.nist.gov/cyberframework

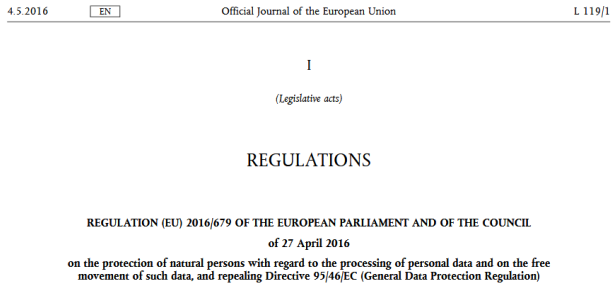


https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services



https://www.retsinformation.dk/

https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf


4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2021)689333

Critical Security Controls

https://www.cisecurity.org/controls/

THE CYBER KILL CHAIN®

The New York Times

Stolen Data Is Tracked to Hacking at Lockheed

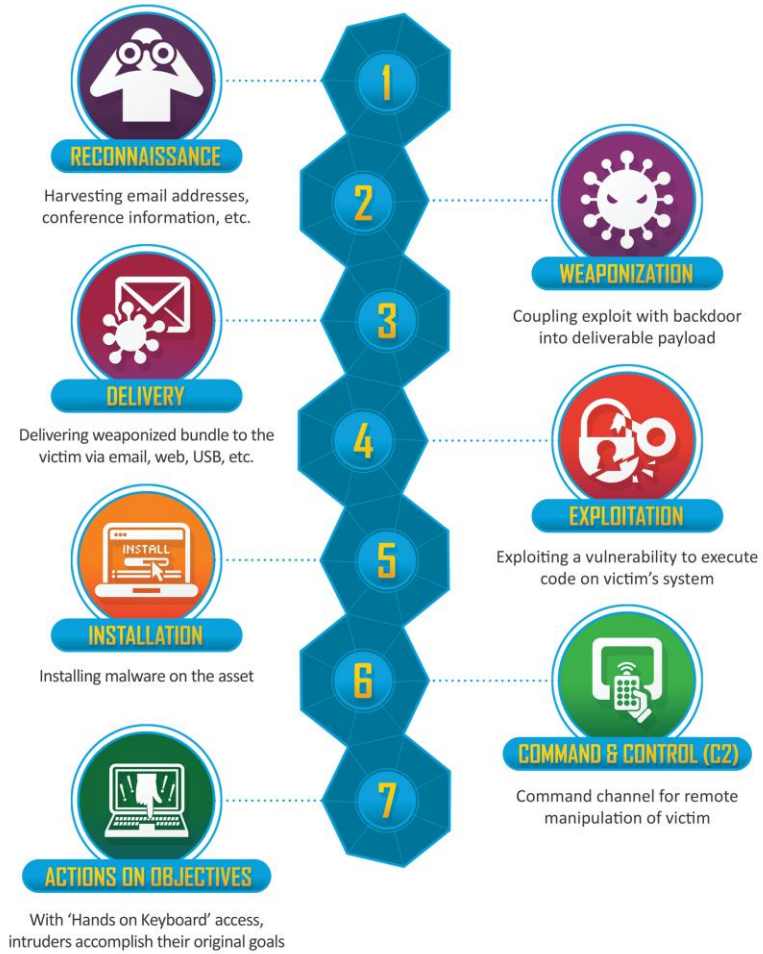
By CHRISTOPHER DREW JUNE 3, 2011

Lockheed Martin said Friday that it had proof that hackers breached its network two weeks ago partly by using data stolen from a vendor that supplies coded security tokens to tens of millions of computer users.

Lockheed's finding confirmed the fears of security experts about the safety of the SecurID tokens and heightened concerns that other companies or government agencies could be vulnerable to hacking attacks.

The tokens, which are used to protect remote access to computer networks, are sold by the RSA Security Division of the EMC Corporation. RSA officials said Friday that they accepted Lockheed's findings and were working with customers to offset the risks through other measures.

https://www.nytimes.com/2011/06/04/technology/04security.html



Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

3.18 SYSTEM AND COMMUNICATIONS PROTECTION

Quick link to System and Communications Protection Summary Table

SC-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] system and communications protection policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: System and communications protection policy and procedures address the controls

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

1 af 492

Standards About us News Taking part Store EN

ICS › 35 › 35.030

ISO/IEC 27002:2013

Information technology — Security techniques — Code of practice for information security controls

BUY THIS STANDARD

FORMAT	LANGUAGE
PDF + COLOR PDF + EPUB	English
PDF + EPUB	English

ABSTRACT PREVIEW

ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s)

https://www.iso.org/standard/54533.html

OWASP PROACTIVE CONTROLS FOR DEVELOPERS 2018 v 3.0

10 Critical Security Areas That Software Developers Mu

PROJECT LEADERS

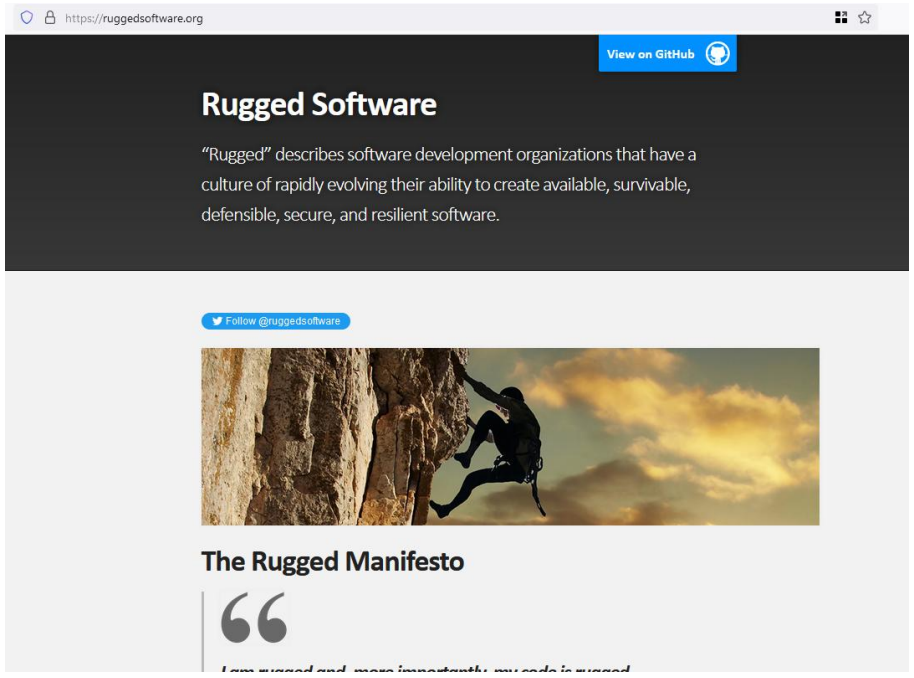
KATY ANTON
JIM MANICO
JIM BIRD

C1: Define Security Requirements
C2: Leverage Security Frameworks and Libraries
C3: Secure Database Access
C4: Encode and Escape Data
C5: Validate All Inputs
C6: Implement Digital Identity
C7: Enforce Access Controls
C8: Protect Data Everywhere
C9: Implement Security Logging and Monitoring
C10: Handle All Errors and Exceptions

https://owasp.org/www-project-proactive-controls/

An Ideal Approach For Success

https://pages.awscloud.com/rs/112-TZM-766/images/How%20to%20use%20Infrastructure%20as%20Code%20for%20automated%20self-service%20AWS%20environments.pdf



https://ruggedsoftware.org/

Conceptually, DevOps is often defined as CALMS.

Culture
Automation
Lean
Measuring
Sharing

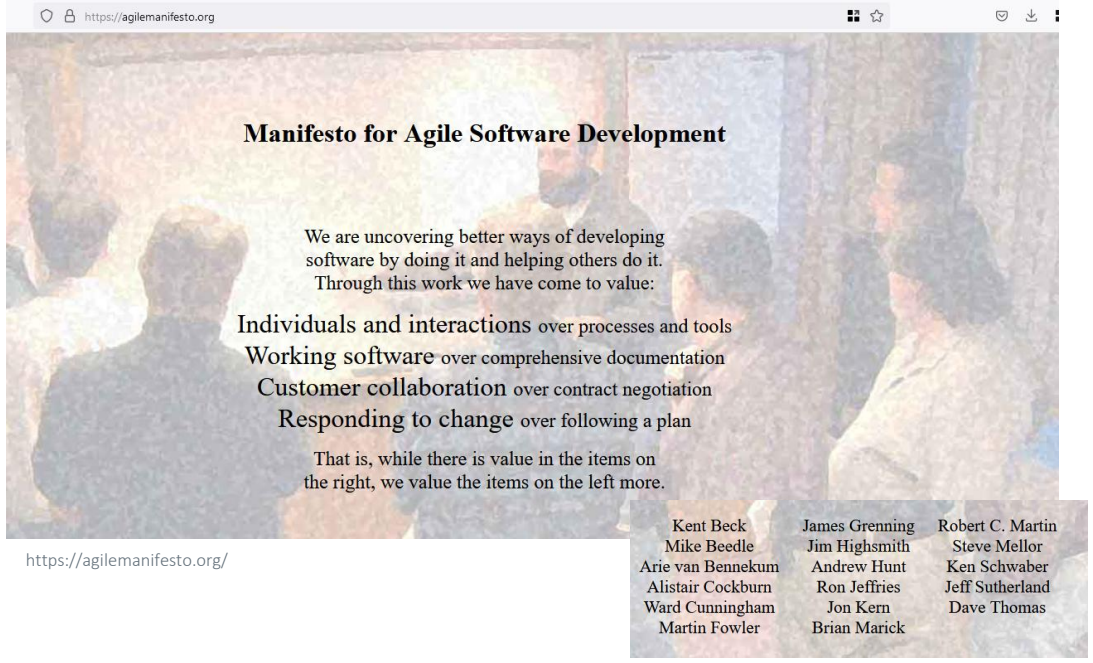
The relation between CALMS and cloud can be mapped compared to traditional IT practices.

DevOps practices	Cloud practices	Traditional IT practices
Culture	Self service for development	Silos, IT department
Automation	Infrastructure as Code (IaC) through cloud APIs	Infrastructure as 'Ticket'
Lean	OpEx - cloud elasticity allows cost to scale with use Managed CI/CD Platforms Managed advanced technology, e.g. ML	CapEx - sunk IT cost. Unused resources are waste On-premise maintenance Static/inflexible technology landscape
Measuring	Infra usage and monitoring, network, cost, etc	No insight Fragmented/heterogeneous insight
Sharing	Infrastructure-as-Code sharable components and platforms Visibility through standardized dashboards, metrics, etc	Peer-to-peer knowledge sharing Low knowledge transfer across organizational boundaries

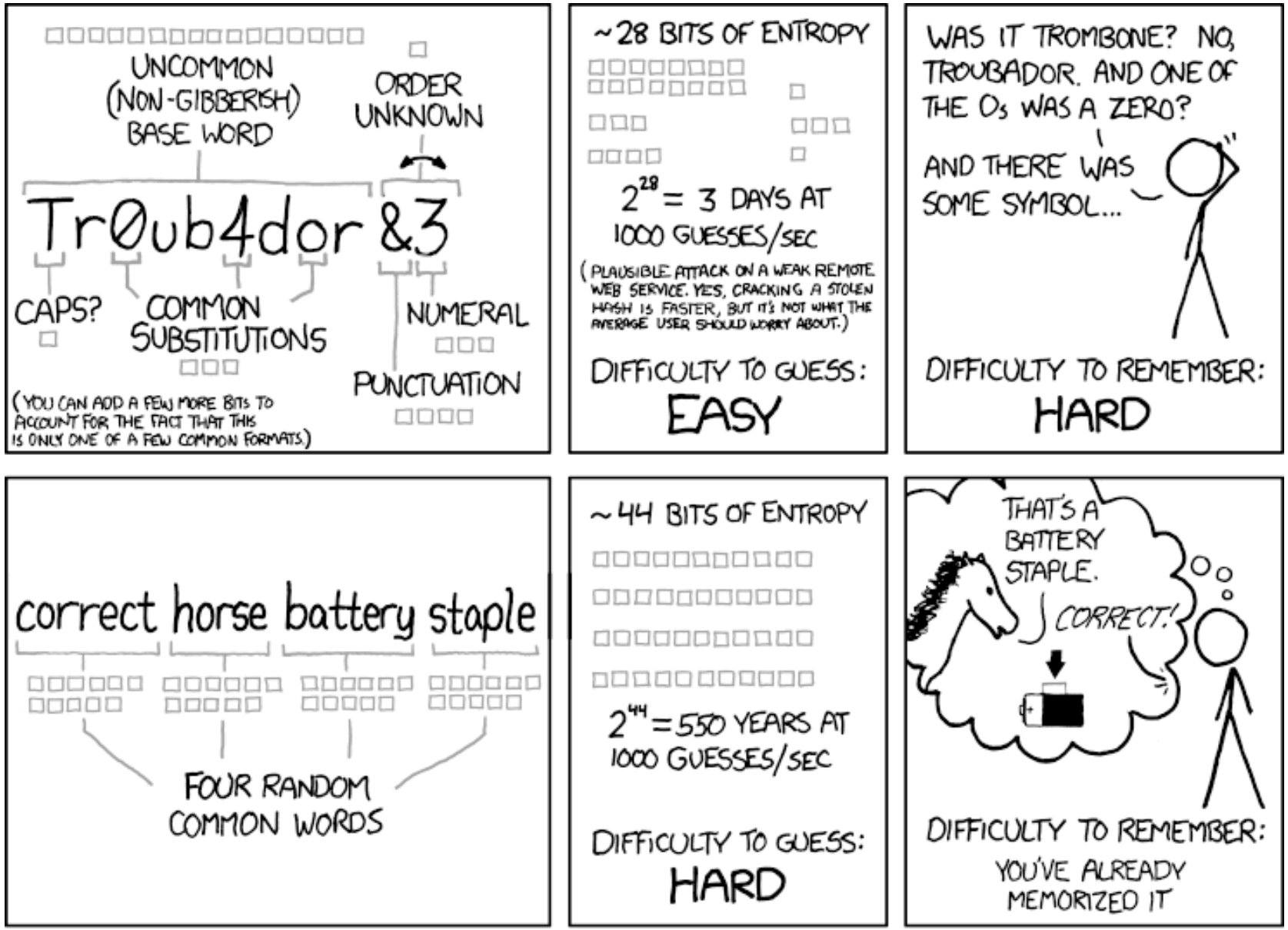
8 - Introduction

eficode

https://www.eficode.com/hubfs/guides/DevOps and cloud guide - Eficode.pdf



https://agilemanifesto.org/



Source:http://xkcd.com/936/

Security is a process not a goal!

You will never be secure against everything.

It is about choosing what to secure against.

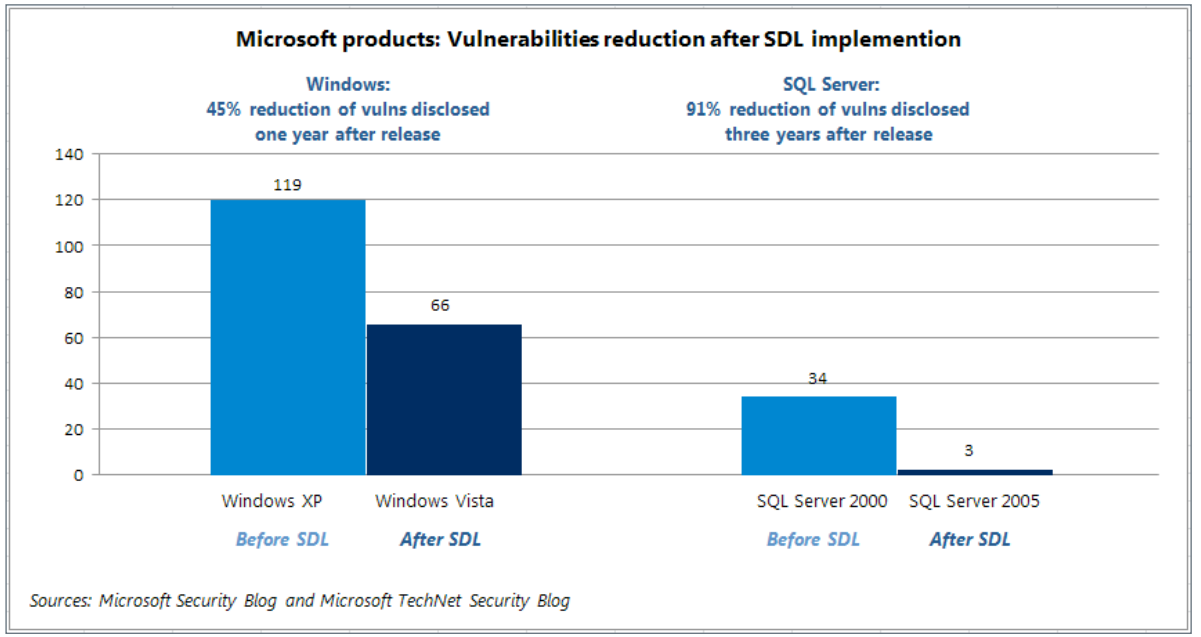
https://www.linkedin.com/posts/ssimonsen_activity-6907746977048870912-wUyn/

Memo from Bill Gates

Posted January 11, 2012 By

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing – or able – to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

Sources: http://news.microsoft.com/2012/01/11/memo-from-bill-gates/



Sources: http://www.microsoft.com/security/sdl/about/benefits.aspx

"...Industry average experience is about 1–25 errors per 1000 lines of code for delivered software..."

"Code Complete", 2nd Edition by Steve McConnell, http://www.microsoft.com/security/sdl/about/benefits.aspx

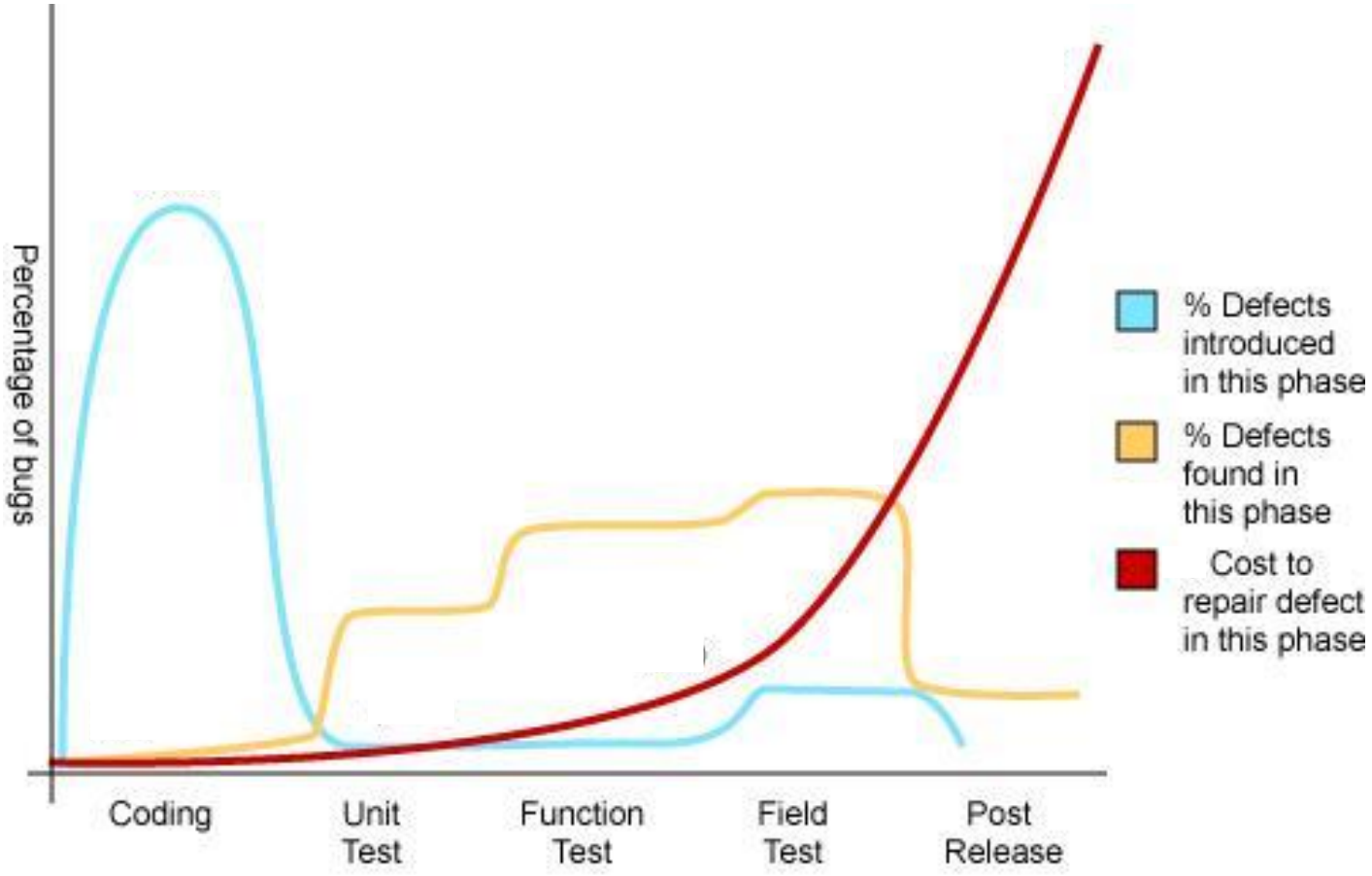
	Millions LOC	Estimated Number of Defects
Simple iOS game	0,01	10 – 250
Win32/Simile virus	0,01	10 – 250
Google Chrome	6,7	6.700 – 167.500
Windows XP	40,00	40.000 – 1.000.000
Windows 7	40,00	40.000 – 1.000.000
Software typical car, 2013	100,00	100.000 – 2.500.000

http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

Higher Cost

"Shift Left"

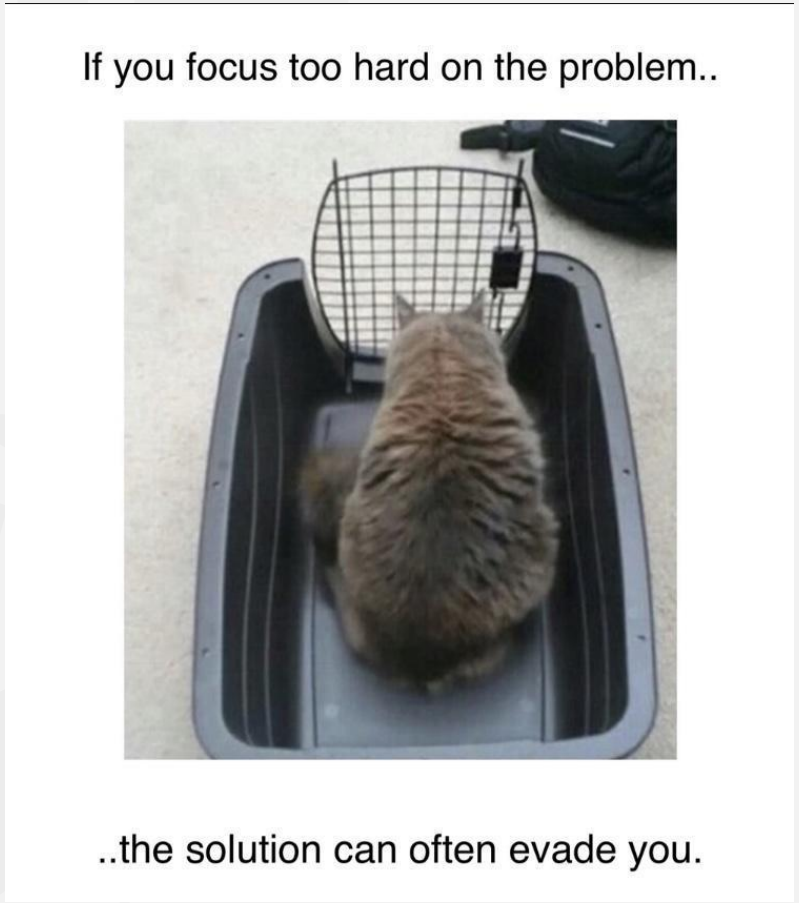
- Higher Monetary Cost,
- Lost Time (rework),
- Lost of Productivity,
- Failure to meet deadline,
- Loss of functional scope,
- Failure to meet time to market,
- Downtime,
- Lost of Customer Trust



Adapted from "Applied Software Measurement, Capers Jonas, 1996

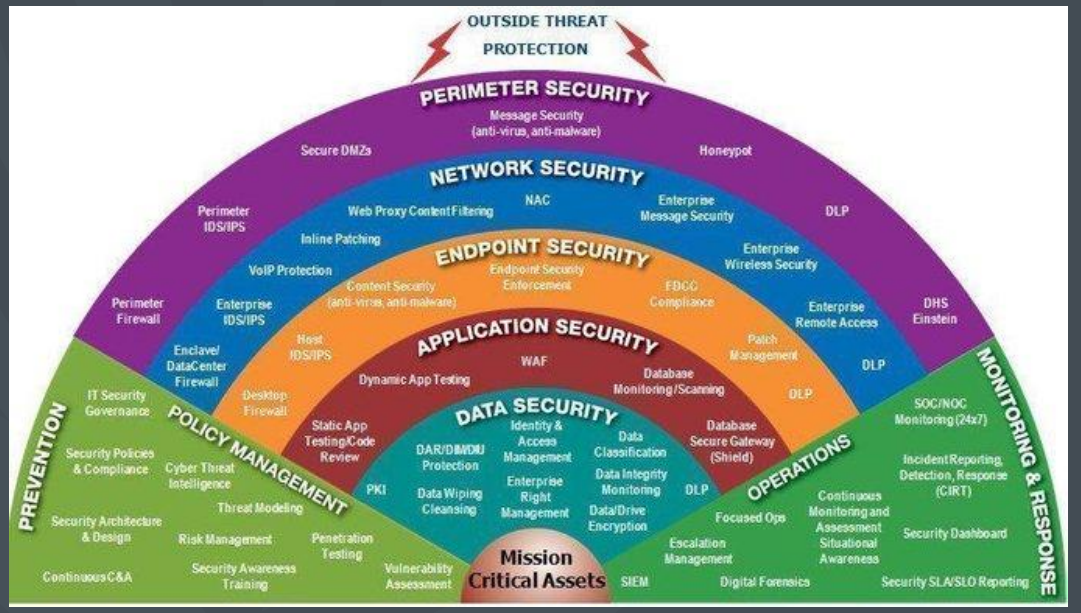
Adapted from https://www.owasp.org/index.php/CISO_AppSec_Guide:_Metrics_For_Managing_Risks_%26_Application_Security_Investments

Establishing Security Requirement



https://www.linkedin.com/posts/the-cyber-security-hub_activity-6751117864536682496-4JWq

– Or what are we building?

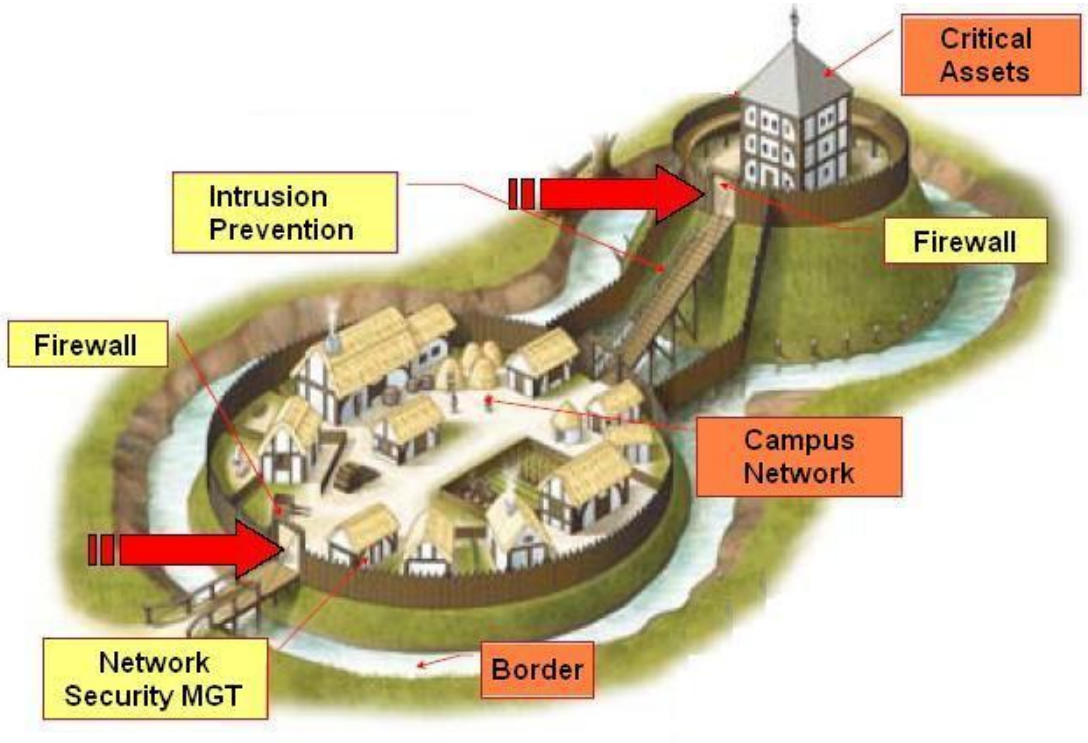


https://twitter.com/Fisher85M/status/1030976170181976064

Defense in Depth

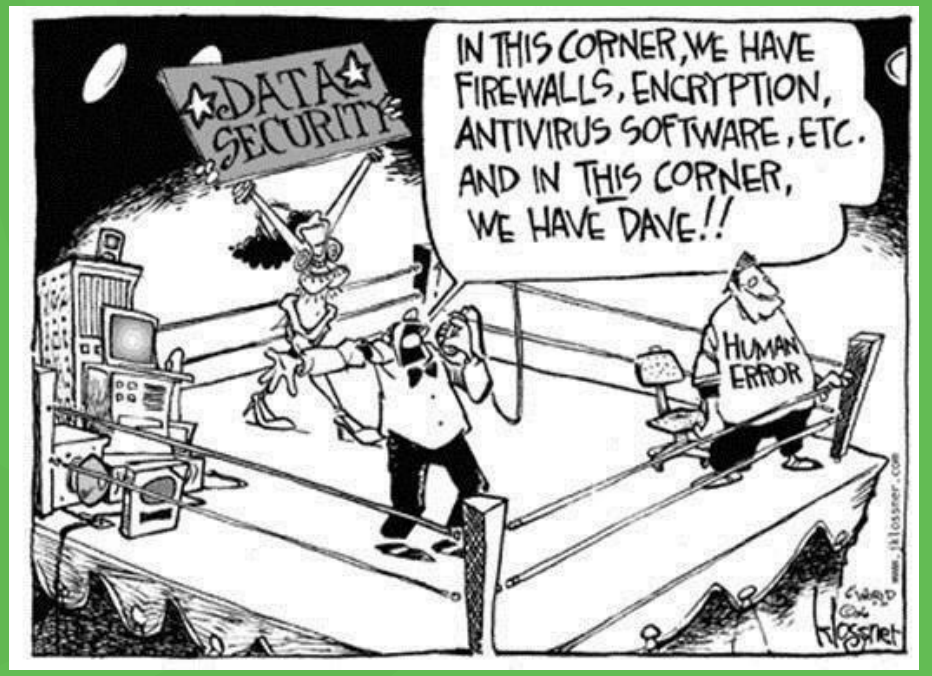
– Overlapping Security Controls

http://commons.wikimedia.org/wiki/File:EU-EE-Tallinn-Kesklinn-Kassisaba.JPG



http://nigesecurityguy.wordpress.com/2013/06/28/architecture-case-study-part-1/

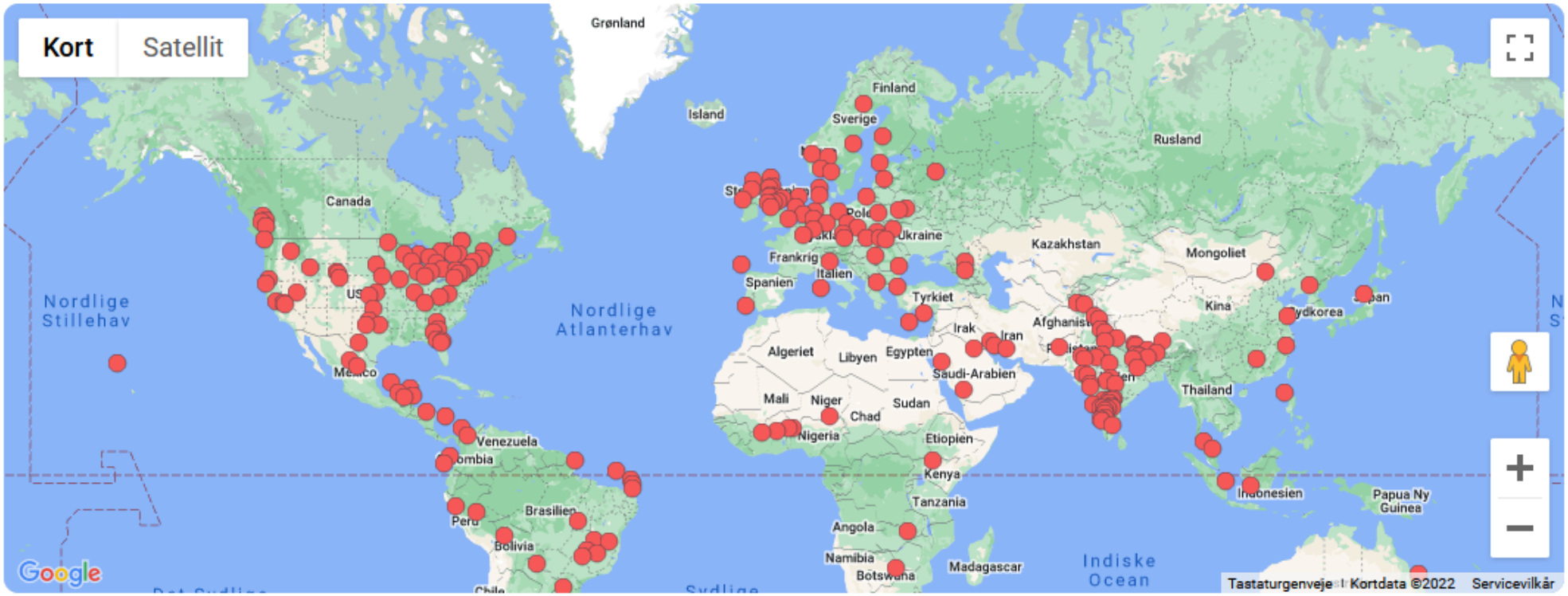
Plan on Failure, Resilient Architecture, Fail Secure, and Defensive Coding



Threat Modelling

Reuse high quality solution to similar problems

OWASP® Foundation World Wide



OWASP® Foundation

Members	Groups	Countries
110,799	248	77

From https://www.meetup.com/pro/owasp May 12th, 2022

Danish Chapters

Aarhus (Jutland) https://owasp.org/www-chapter-aarhus/

Dennis Perto (He/Him) · 1.
Managing ransomware incidents in Denmark | Proactively doing security monitoring based on industry leading Threat Intelligence | OWASP Chapter Leader

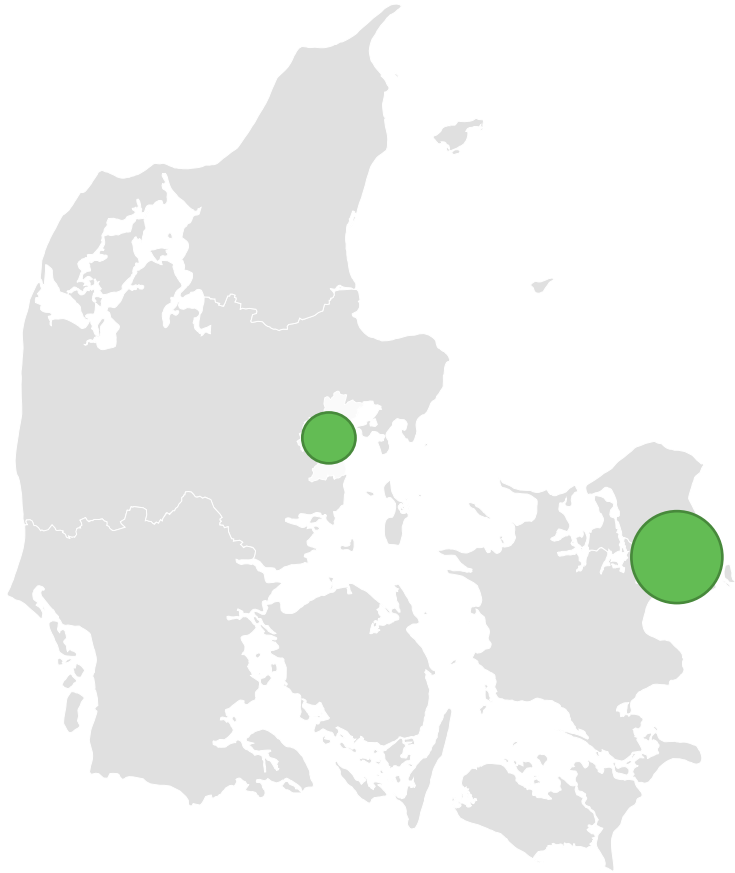
dennis.perto@owasp.org

Mikkel Rømer · 1.
Truesec | Cyber Security Expert | SEC699 | eCCPTv2 | DSO I Malware Dev | DSO 2 Adversary Emulation | Sitecore Platform Associate Developer | SC .NET Developer XP 8.0

mikkel.romer@owasp.org

Thomas Ljungberg Kristensen
Security Advisor at WelcomeSecurity / Co-chapter lead OWASP Aarhus

thomas.kristensen@owasp.org



Copenhagen (Zealand)

https://owasp.org/www-chapter-copenhagen/

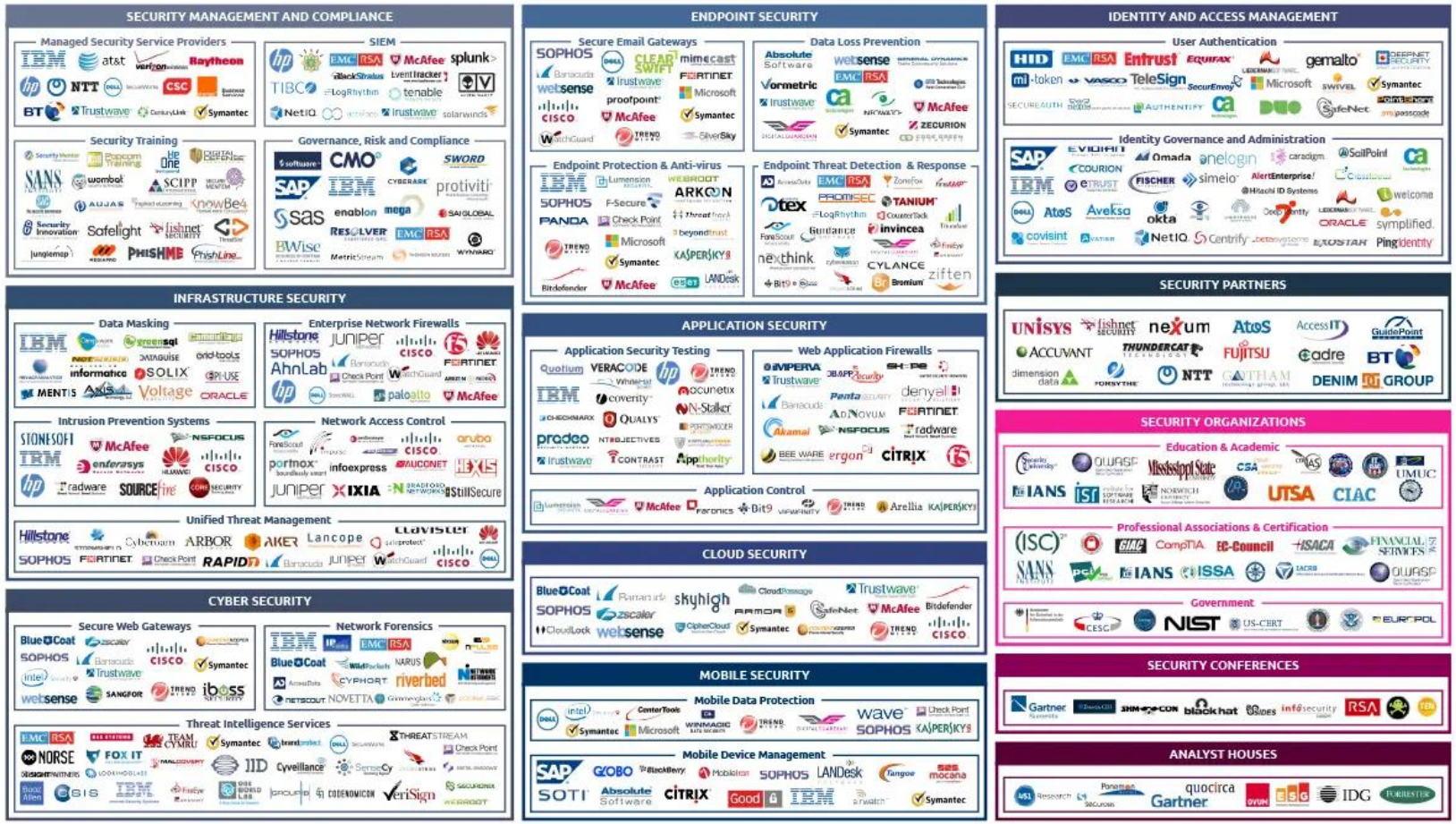
Alessandro Bruni · 1.
Associate Professor at IT-Universitetet i København
København, Hovedstaden, Danmark · Kontaktoplysninger

alessandro.bruni@owasp.org

Andrada Son · 1.
Headhunter/ Nerd/ Happy volunteer in OWASP & BSides Copenhagen/ Friend of the community
København og omegn · Kontaktoplysninger

andrada.son@owasp.org

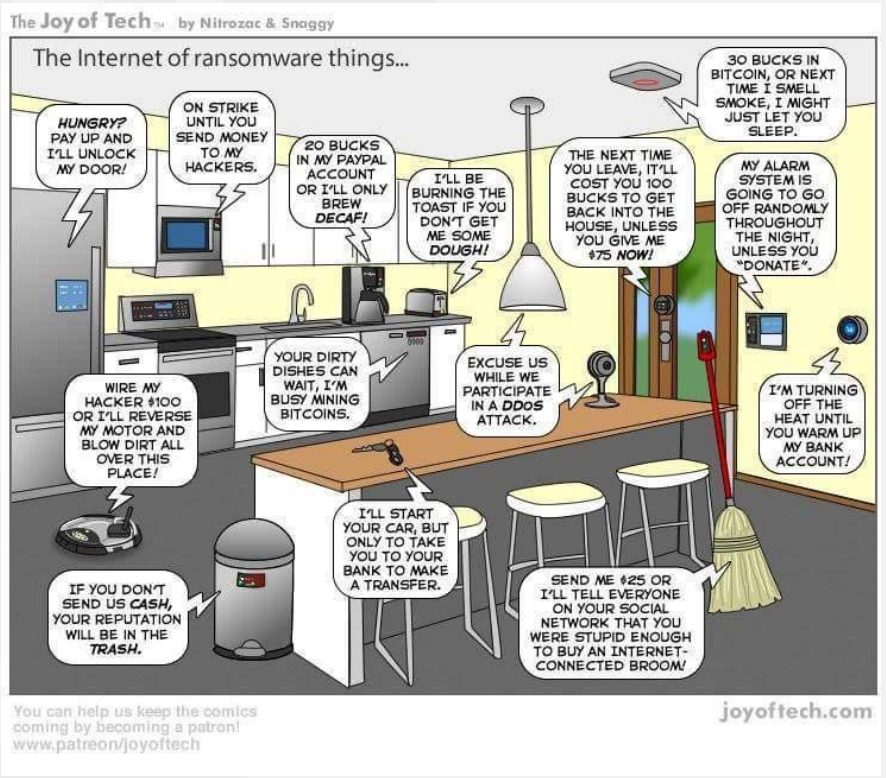
Information Security IndustryScape



Version 1
November 2014

DIGITAL GUARDIAN
Formerly VERDASYS

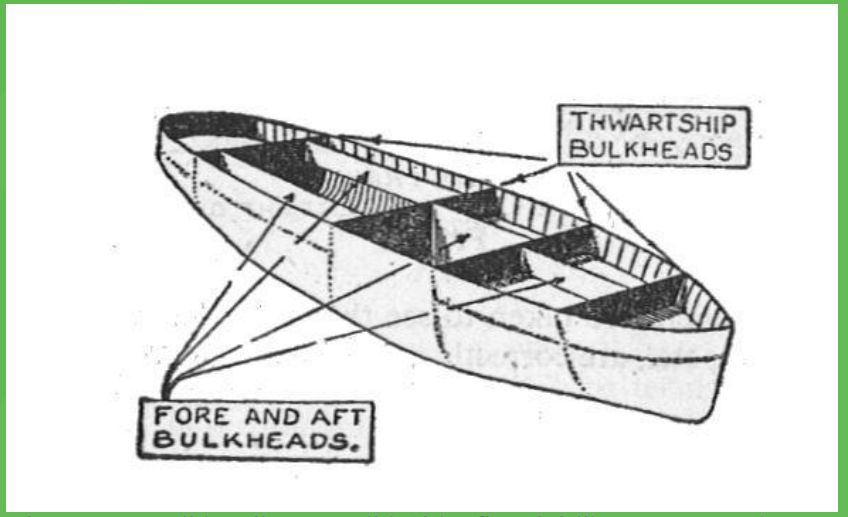
https://digitalguardian.com/blog/information-security-industryscape



Hardening / Attack Surface Mimimzing

– “You aren't gonna need it” (YAGNI) and if you do not need it – kill it”

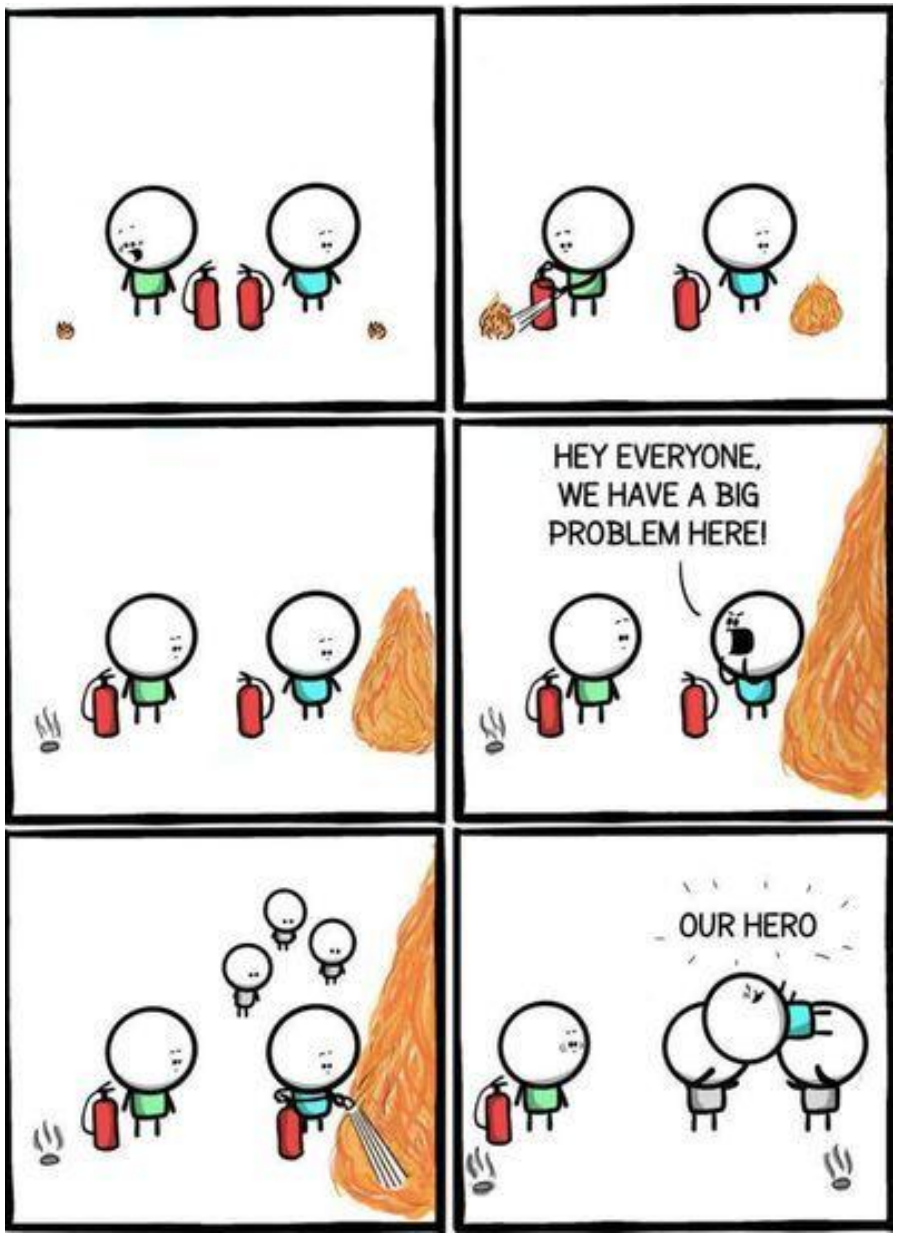
Breach Containment, Breach Detection, or Assume Breach



https://en.wikipedia.org/wiki/Ship_floodability

Supply chain attacks
– 3rd party and CI/CD

One person’s development is another person’s production


HEY EVERYONE, WE HAVE A BIG PROBLEM HERE!
OUR HERO

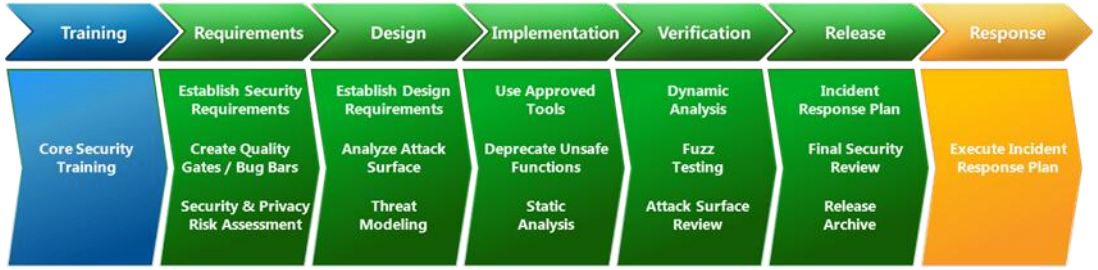
From a security perspective, your problem has been solved before – and better!

But security uses a different language – often more than one!

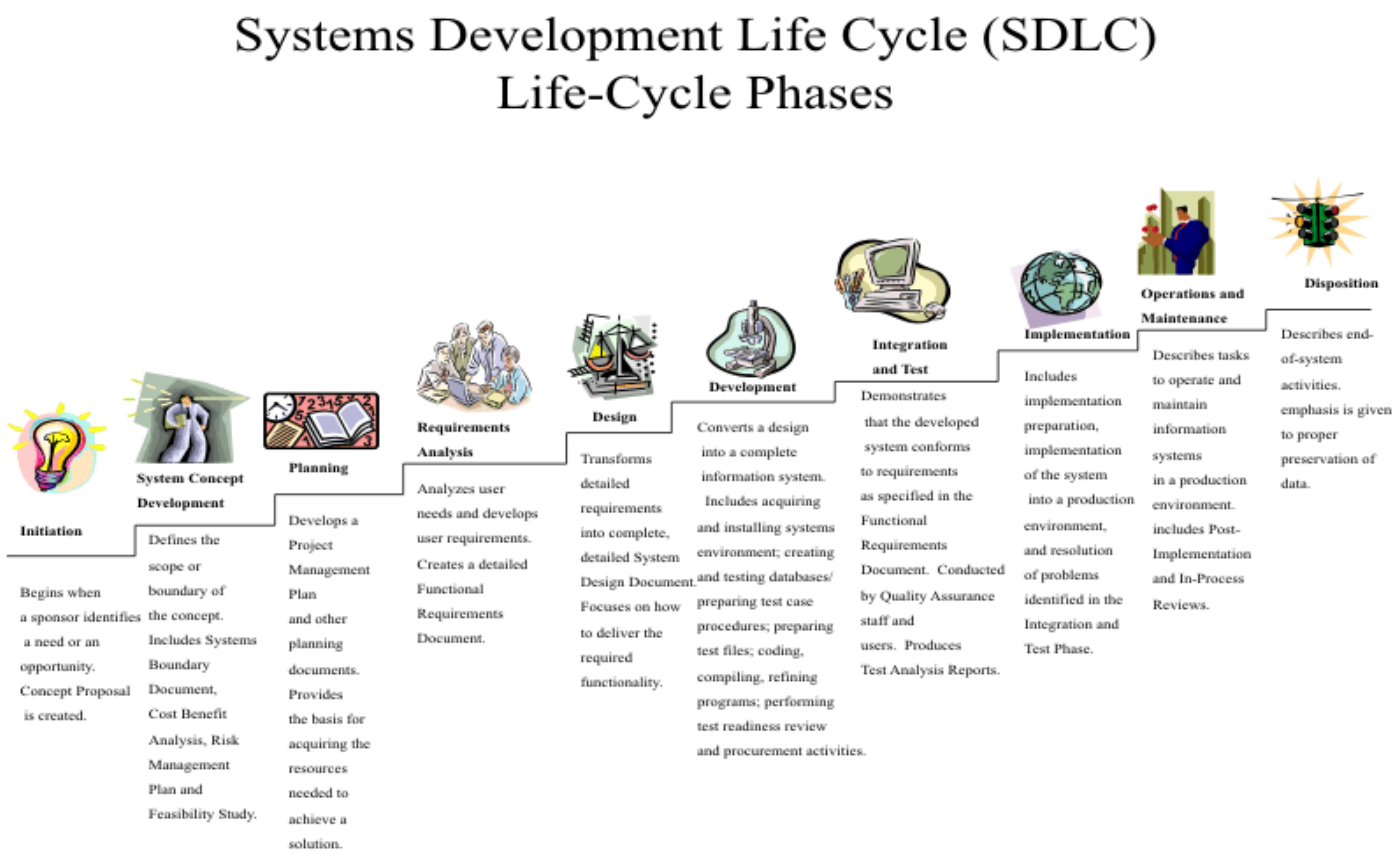
When you can rephrase your security challenge, you can look up the answer (and often the code)

This is the way!

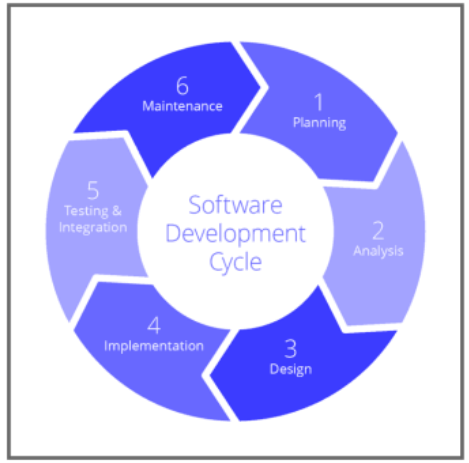
https://owasp.org/www-project-samm/



https://docs.microsoft.com/en-us/windows/security/threat-protection/msft-security-dev-lifecycle

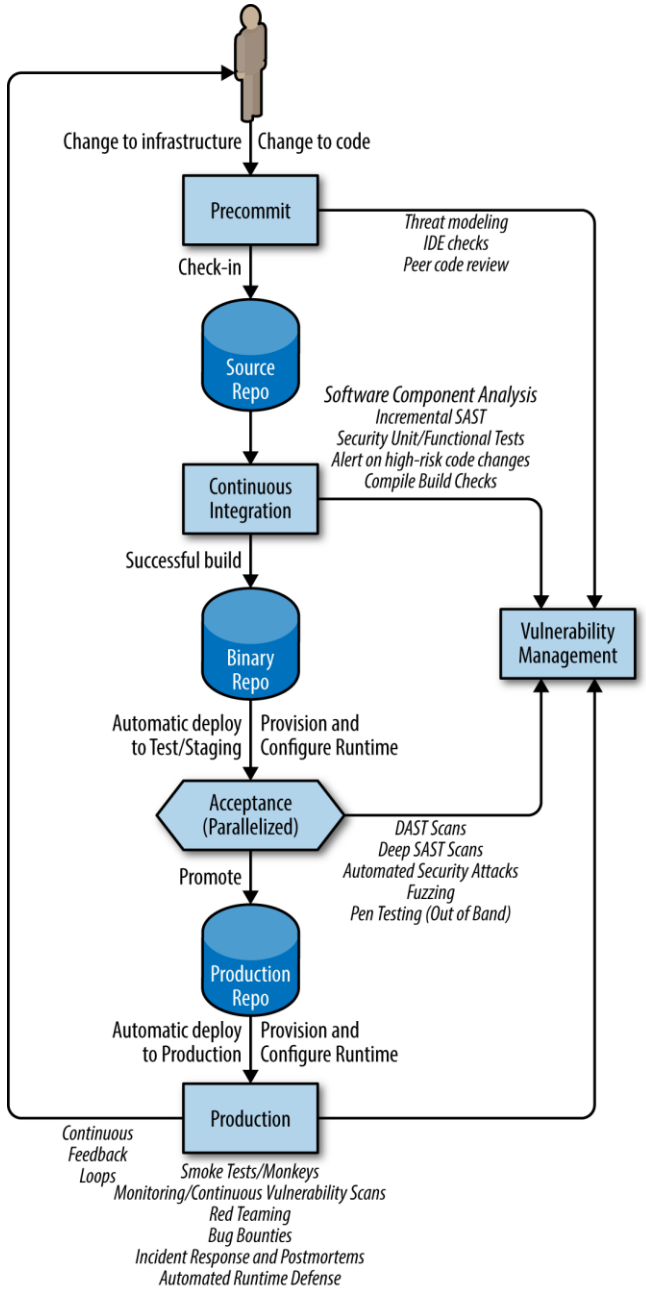


https://en.wikipedia.org/wiki/Systems_development_life_cycle

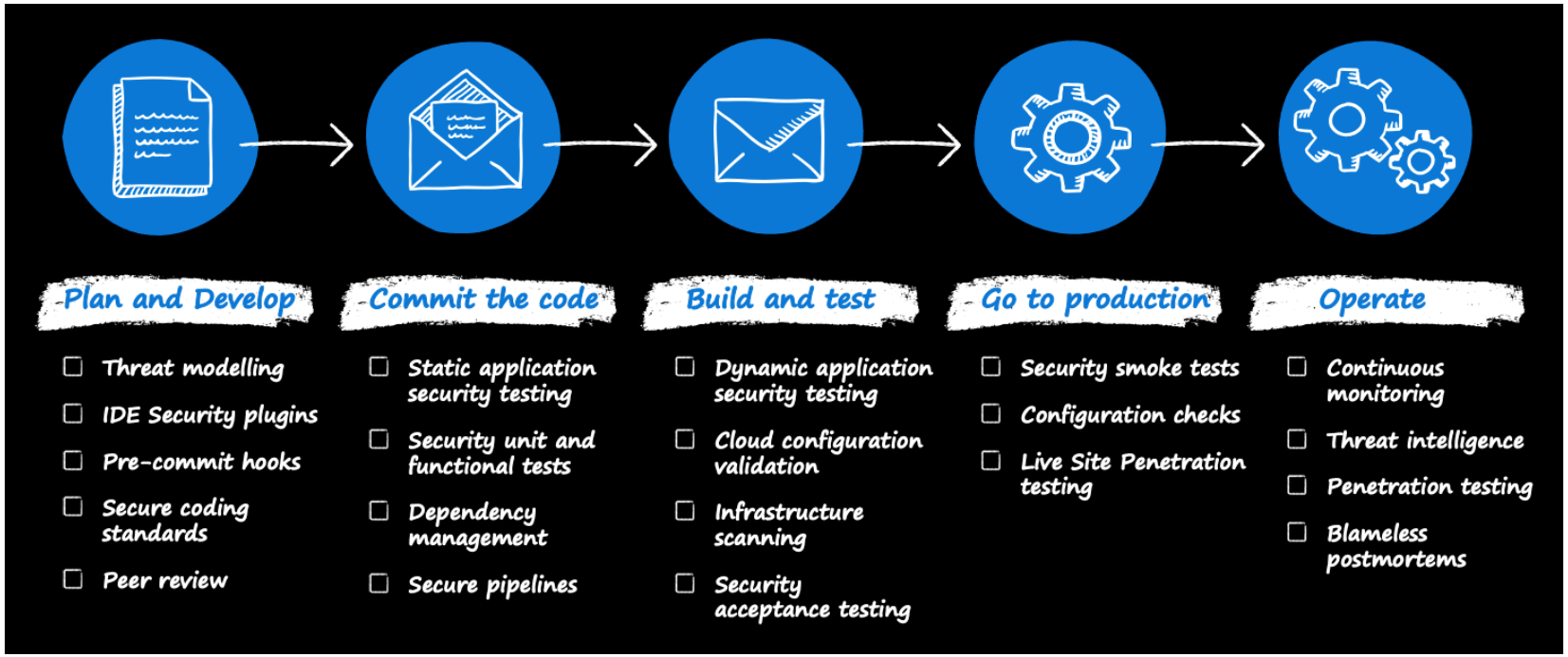


A typical SDLC representation

https://owasp.org/www-project-integration-standards/writeups/owasp_in_sdlc/



https://www.oreilly.com/library/view/devopssec/9781491971413/ch04.html



https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

Security Tools in Your Tool Belt

Choosing what to ignore?

Static analysis (SAST)

Dynamic analysis (DAST)

Runtime detection

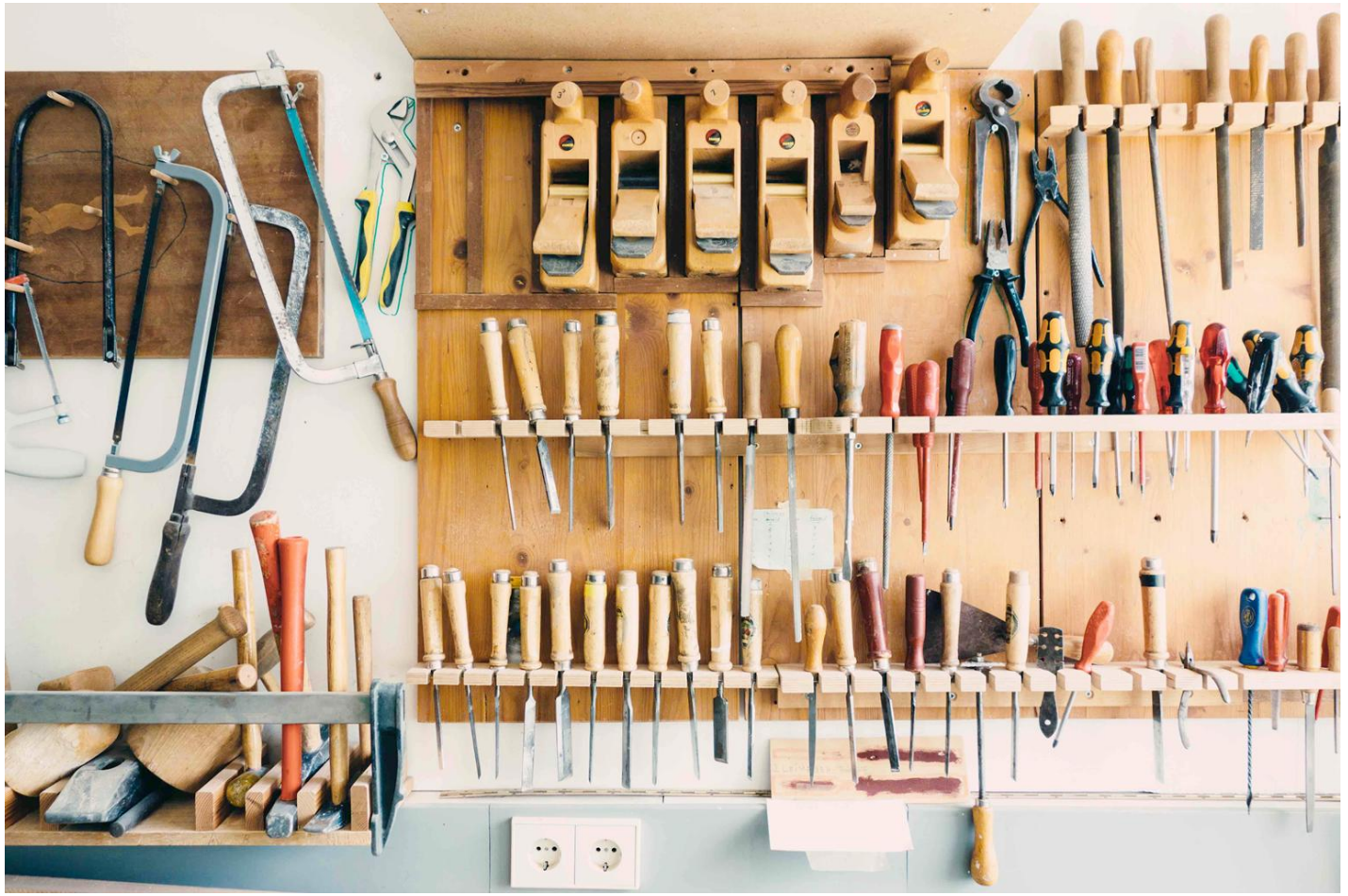
Fuzzing

Pen tests

Secure wrapper libraries

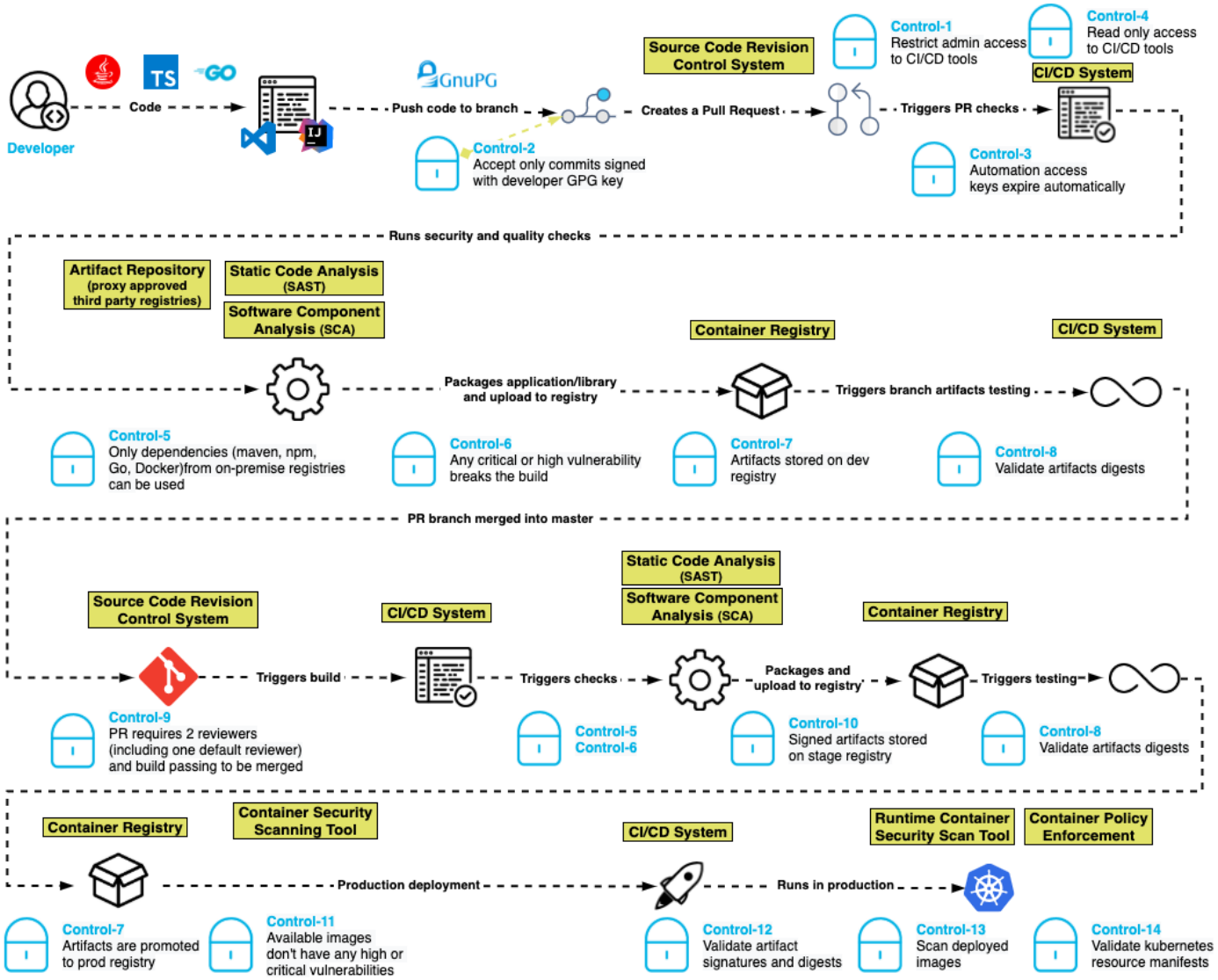
Threat modeling

Bug bounty

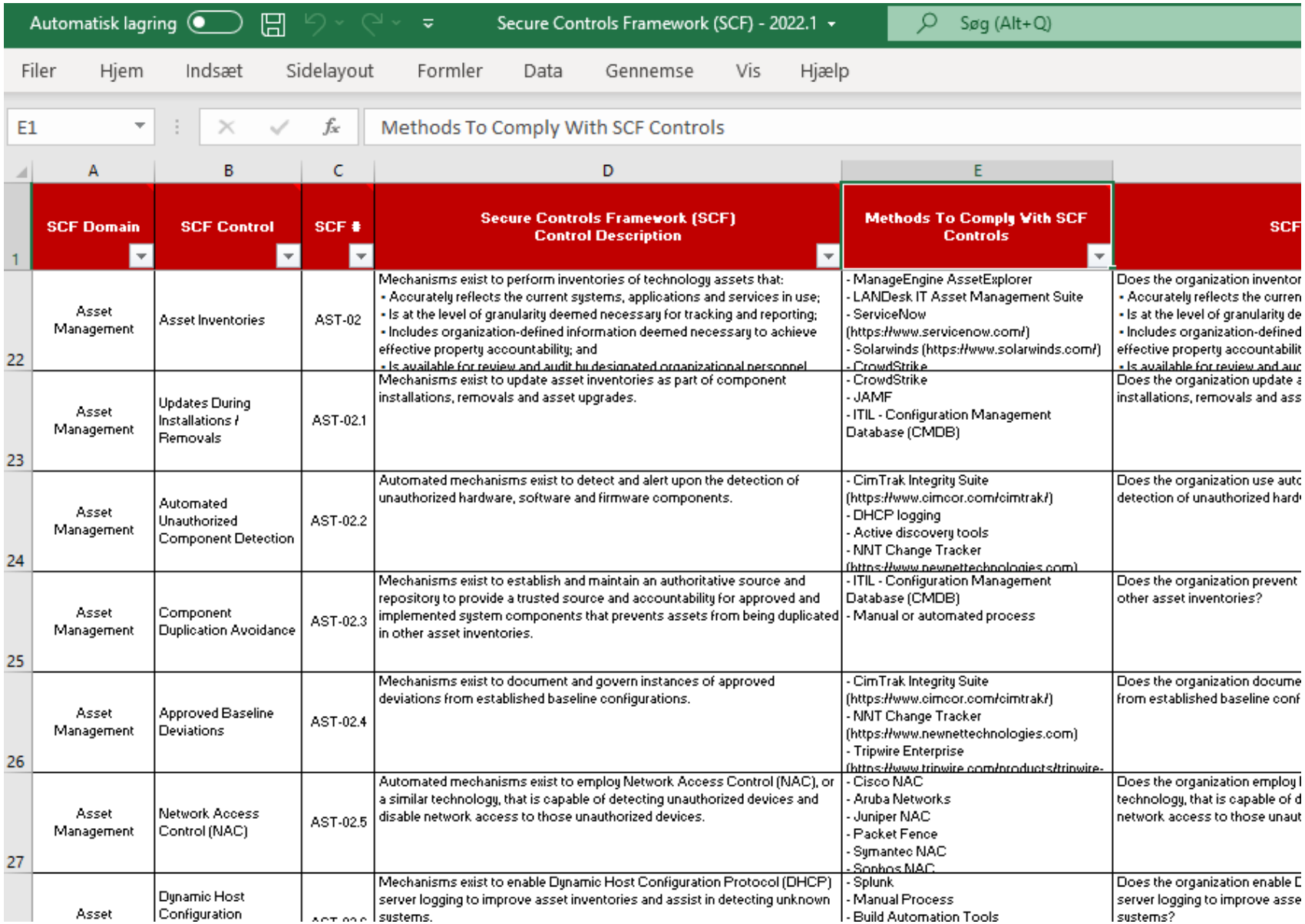


Adapted from “How to 10X Your Security” by Clint Gibler

See https://docs.google.com/presentation/d/1lfEvXtw5RTj3JmXwSQDXy8or87_BHrFbo1ZtQQlHbq0/ and https://www.youtube.com/watch?v=tWA_EBNsQH8

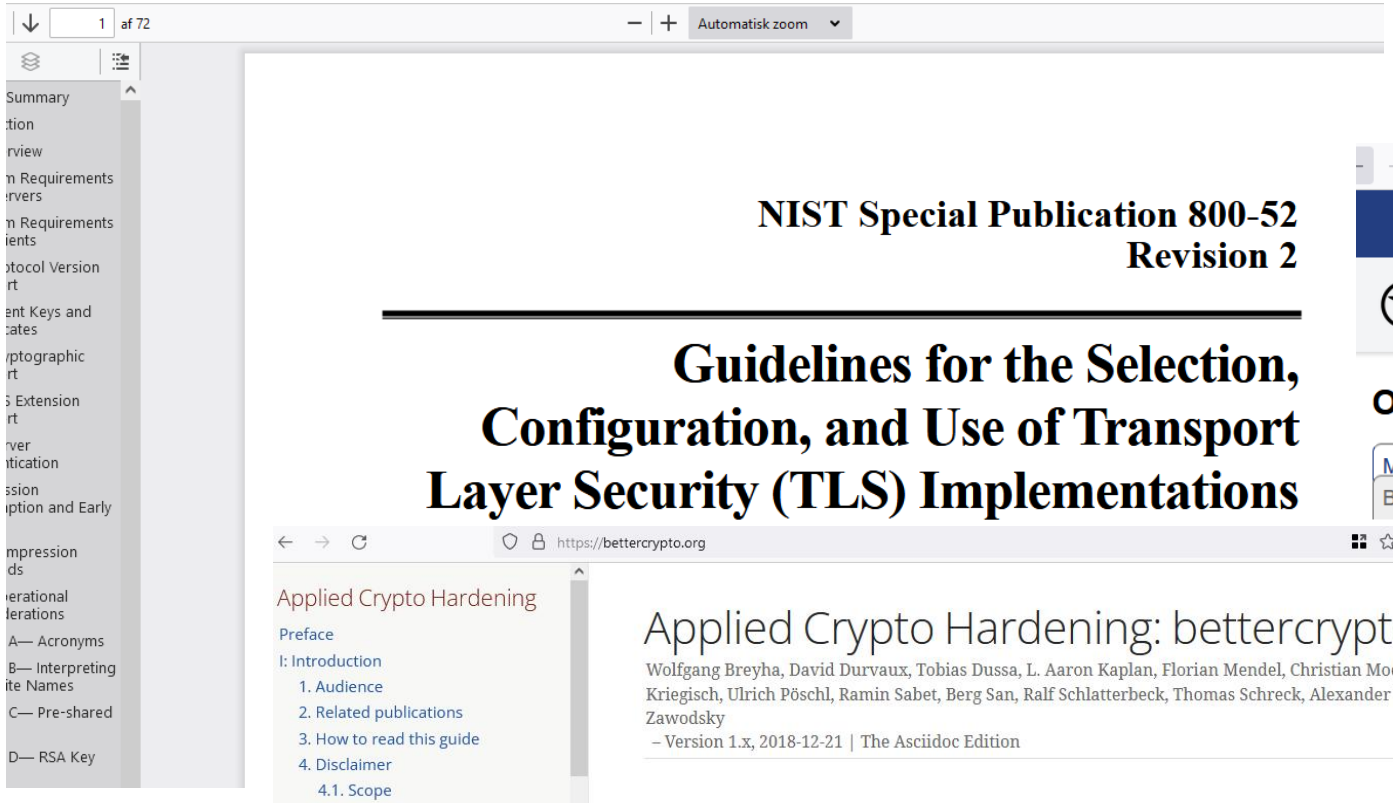


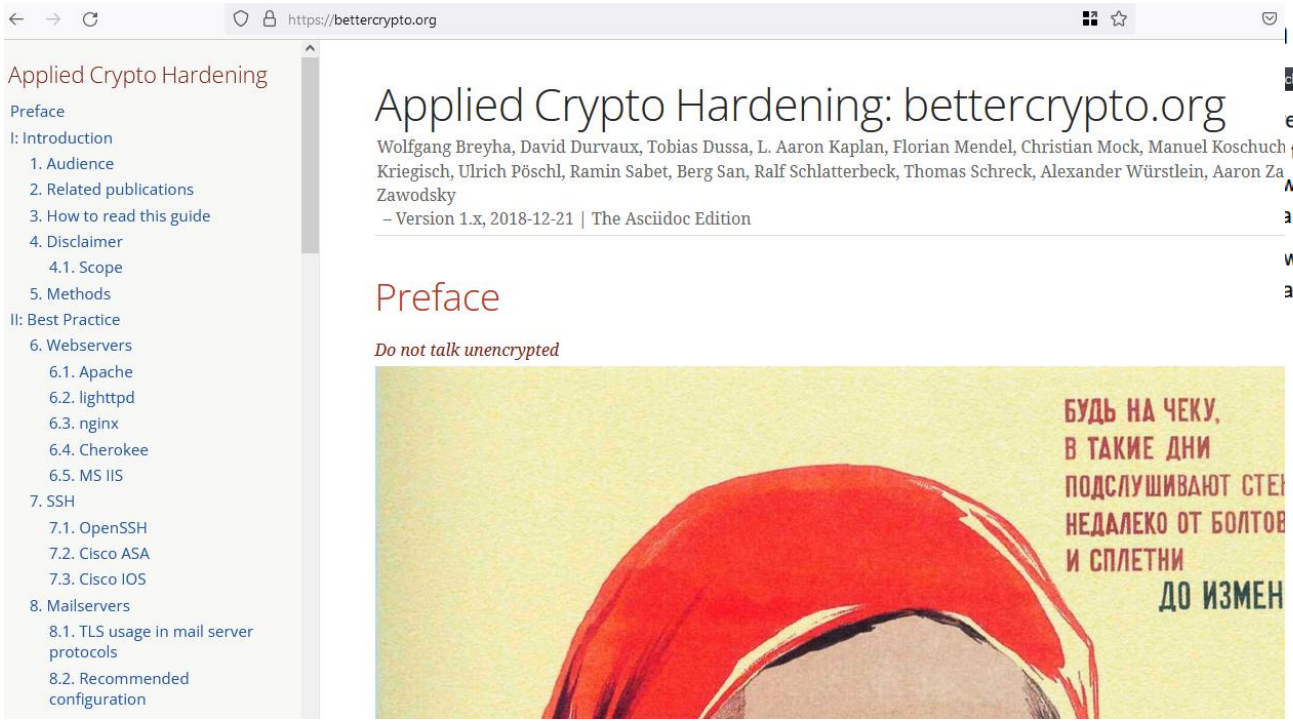
https://about.gitlab.com/blog/2021/08/30/secure-pipeline-with-single-sign-in/



	A	B	C	D	E	
1	SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Methods To Comply With SCF Controls	SCF
22	Asset Management	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: • Accurately reflects the current systems, applications and services in use; • Is at the level of granularity deemed necessary for tracking and reporting; • Includes organization-defined information deemed necessary to achieve effective property accountability; and • Is available for review and audit by designated organizational personnel	- ManageEngine AssetExplorer - LANDesk IT Asset Management Suite - ServiceNow (https://www.servicenow.com/) - Solarwinds (https://www.solarwinds.com/) - CrowdStrike	Does the organization inventor • Accurately reflects the curren • Is at the level of granularity de • Includes organization-defined effective property accountabilit • Is available for review and auc
23	Asset Management	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	- CrowdStrike - JAMF - ITIL - Configuration Management Database (CMDB)	Does the organization update a installations, removals and ass
24	Asset Management	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - DHCP logging - Active discovery tools - NNT Change Tracker (https://www.newnettechnologies.com)	Does the organization use autc detection of unauthorized hard
25	Asset Management	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	- ITIL - Configuration Management Database (CMDB) - Manual or automated process	Does the organization prevent other asset inventories?
26	Asset Management	Approved Baseline Deviations	AST-02.4	Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com) - Tripwire Enterprise (https://www.tripwire.com/products/tripwire-	Does the organization docume from established baseline conf
27	Asset Management	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, that is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	- Cisco NAC - Aruba Networks - Juniper NAC - Packet Fence - Symantec NAC - Sophos NAC	Does the organization employ t technology, that is capable of d network access to those unaut
	Asset	Dynamic Host Configuration		Mechanisms exist to enable Dynamic Host Configuration Protocol (DHCP) server logging to improve asset inventories and assist in detecting unknown systems.	- Splunk - Manual Process - Build Automation Tools	Does the organization enable D server logging to improve asse systems?

https://www.securecontrolsframework.com





https://bettercrypto.org/, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf and https://owasp.org/www-project-secure-headers/

README.md

Ultimate DevSecOps library

Contribution rules

If you want to contribute to this library of knowle

Tooling

Pre-commit time tools

In this section you can find lifecycle helpers, precommit hook tools and threat modeling tools. Threat modeling tools are specific category by themselves allowing you to simulate and discover potential gaps before you start to develop the software or during the process.

Modern DevSecOps tools allow using Threat modeling as code or generation of threat models based on the existing code annotations.

Name	URL	Description	Meta
git-secrets	https://github.com/awslabs/git-secrets	AWS labs tool preventing you from committing secrets to a git repository	
git-hound	https://github.com/tillson/git-hound	Searchers secrets in git	
goSDL	https://github.com/slackhq/goSDL	Security Development Lifecycle checklist	
	https://github.com		

https://github.com/sottlmarek/DevSecOps

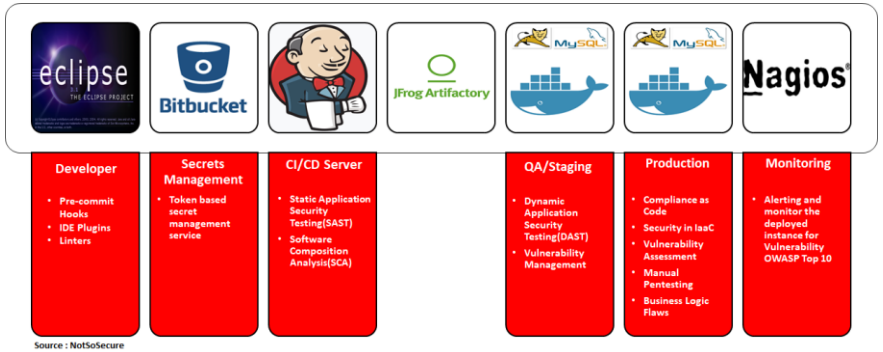
analysis tools

This repository lists **static analysis tools** for all programming languages, build tools, config files and more
The official website, analysis-tools.dev is based on this repository and adds rankings, user c
resources like videos for each tool.

CI passing

Other
- Angular
- Ansible
- Azure Resource Manager
- Binaries
- Build tools
- CSS/SASS/SCSS
- Config Files
- Configuration Management
- Containers
- Continuous Integration
- Deno
- Embedded
- Embedded Ruby (a.k.a. ERB, eRuby)
- Gherkin
- HTML
- JSON

https://github.com/analysis-tools-dev/static-analysis



https://notsosecure.com/achieving-devsecops-open-source-tools

https://docs.gitlab.com/ee/user/application_security/sast/

GitLab | Docs Search What's new?

- Set up your organization
- Organize work with projects
- Plan and track work
- Build your application
- Secure your application
  - Security Configuration
  - Container Scanning
  - Dependency Scanning
  - Static Application Security Testing
    - SAST Analyzers
  - Infrastructure as Code (IaC) Scanning

Static Application Security Testing (SAST)

ALL TIERS

All open source (OSS) analyzers were n

The whitepaper "A Seismic Sl
application based. Downloac

If you're using GitLab CI/CD, you ca
for known vulnerabilities. You can ru
reports as job artifacts.

Language (package managers) / framework	Scan tool	Introduced in GitLa
.NET Core	Security Code Scan	11.0
.NET Framework	Security Code Scan	13.0
Apex (Salesforce)	PMD	12.1
C	Semgrep	14.2
C/C++	Flawfinder	10.7

https://docs.gitlab.com/ee/user/application_security/sast/

OWASP PROJECTS CHAPTERS EVENTS ABOUT

Source Code Analysis Tools

Contributor(s): Dave Wichers, itamarlavender, will-obrien, Eitan Worcel, Prabhu Subramanian, kingl

				Note
				.NET, C\#, VB.net
42Crunch		Commercial		REST API security platform that includes Security Audit (SAST), dynamic conformance scan, runtime protection, and monitoring.
Apiiro		Open Source	Windows	ASP, ASP.NET, C\#, Java, Javascript,

https://owasp.org/www-community/Source_Code_Analysis_Tools

Please support the OWASP mission to improve software security through open source initiatives and

OWASP PROJECTS CHAPTERS EVENTS ABOUT Search OWAS

Vulnerability Scanning Tools

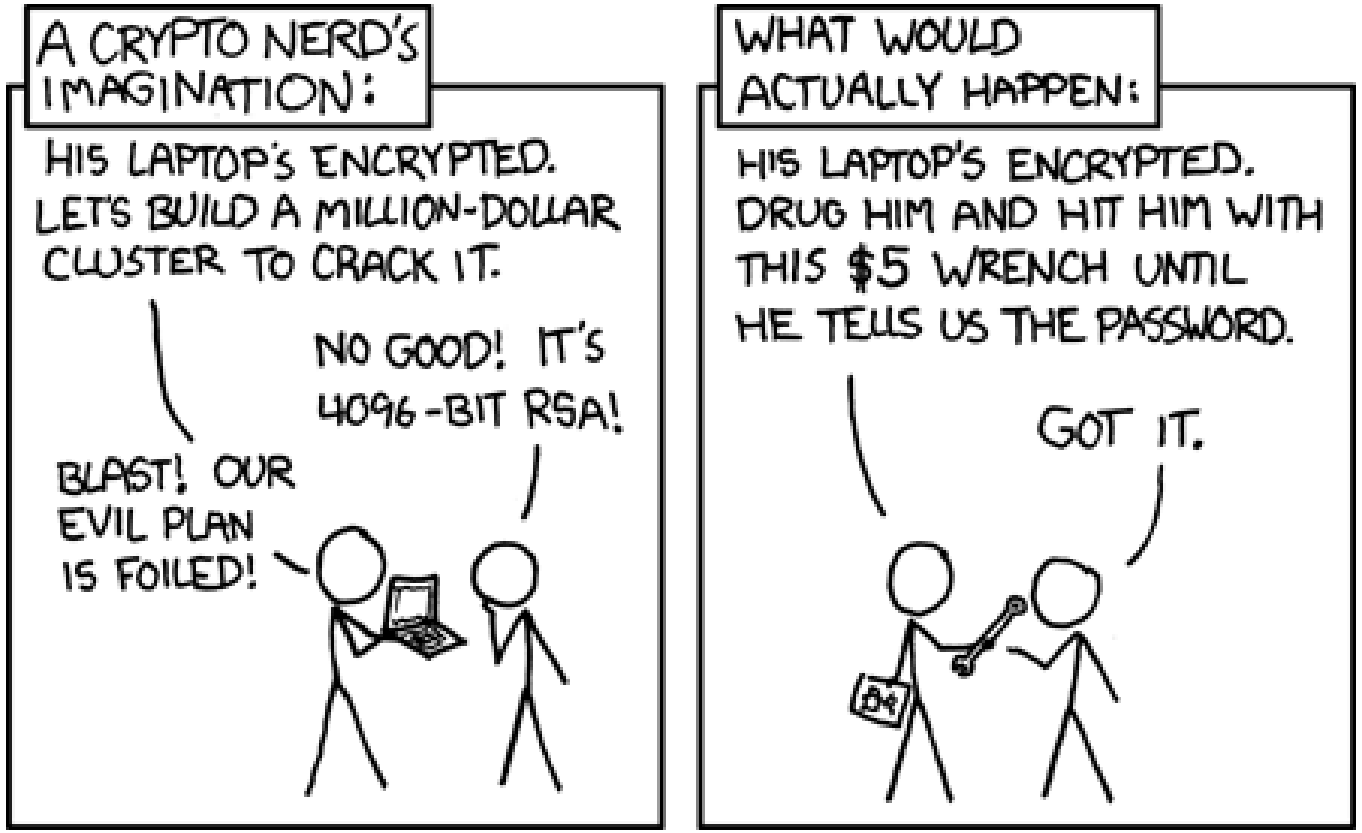
Description

Web Application Vulnerability Scanners are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as Cross-site scripting, SQL Injection, Command Injection, Path Traversal and insecure server configuration. This category of tools is frequently referred to as Dynamic Application Security Testing (DAST) Tools. A large number of both commercial and open source tools of this

https://owasp.org/www-community/Vulnerability_Scanning_Tools

The question isn't "Is activity X useful?" but rather "Is activity X a better use of time than activity Y?"

Adam Shostack



Source:https://xkcd.com/538/

Why do we have brakes in the car?

Why do we have brakes in the car?

to go faster!

WelcomeSecurity
Enabling value through IT security

TAK!

www.welcomesecurity.net

+45 2158 1410
Info@welcomesecurity.net