



WelcomeSecurity
Enabling value through IT security

Security Kick-Off event

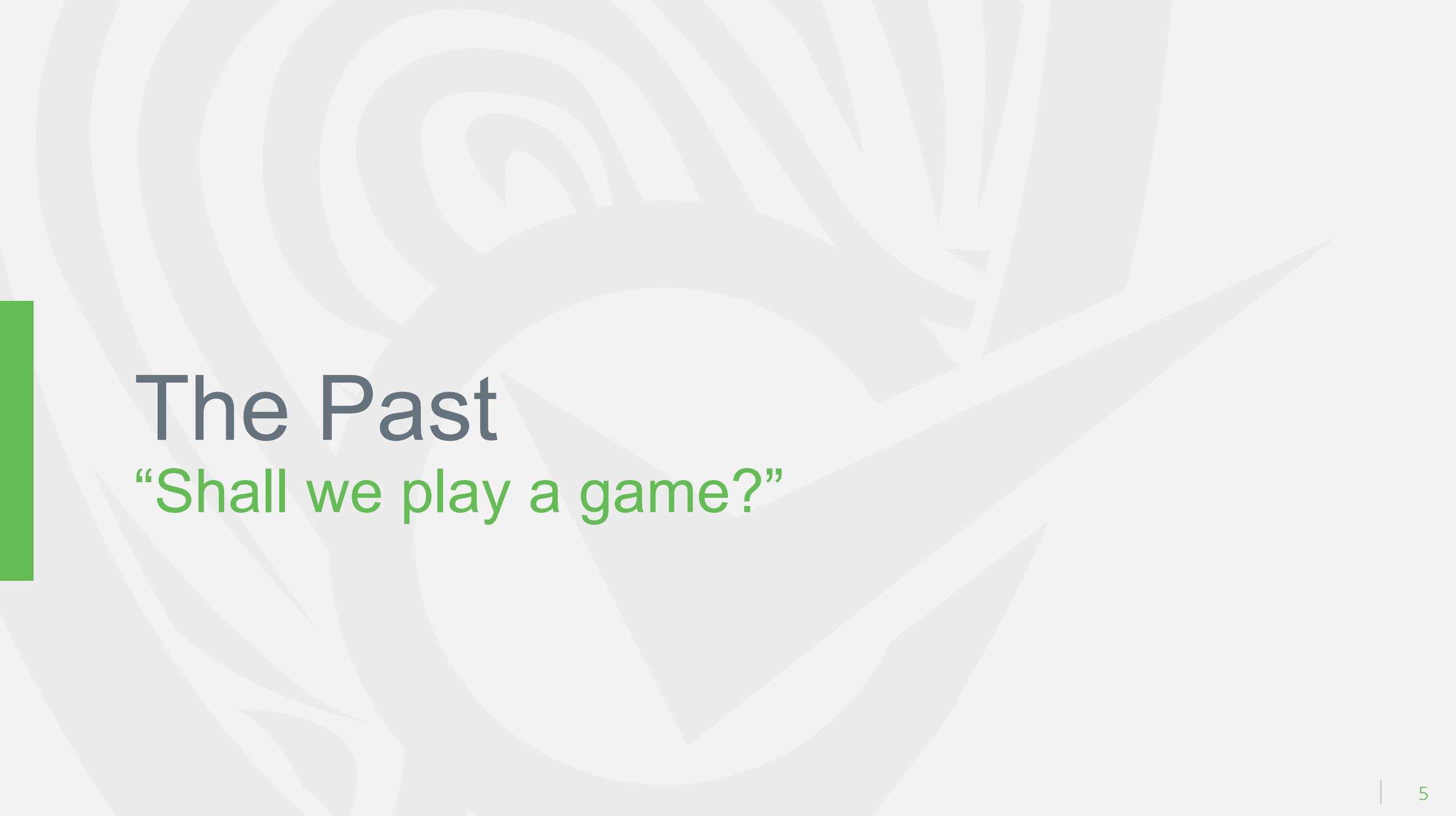
Timeslot	Topic / Agenda
13:00 – 13:30	Welcome to the “Kick Off” event
13:30 – 15:00	<p>What is happening right now and why is it different?!</p> <p>You open a newspaper and read about a new breach or compromise. Maybe you even got notified that your data has been a breach!</p> <p>But what is going on, and why did we get here?</p>
15:00 – 16:00	Break / Coffee and Cake / Network
16:00 – 16:45	<p>The way in – for it-criminals!</p> <p>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!</p>
16:45 – 17:00	Short Break
17:00 – 17:45	<p>Where do we go from here?</p> <p>What can we do to improve security both privately and at OK and how do we improve the security of the software we create?</p>
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 –	<i>WelcomeSecurity, Security Advisor and Owner</i>	
2019 –	<i>OWASP Co-chapter Lead, Aarhus</i>	
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?



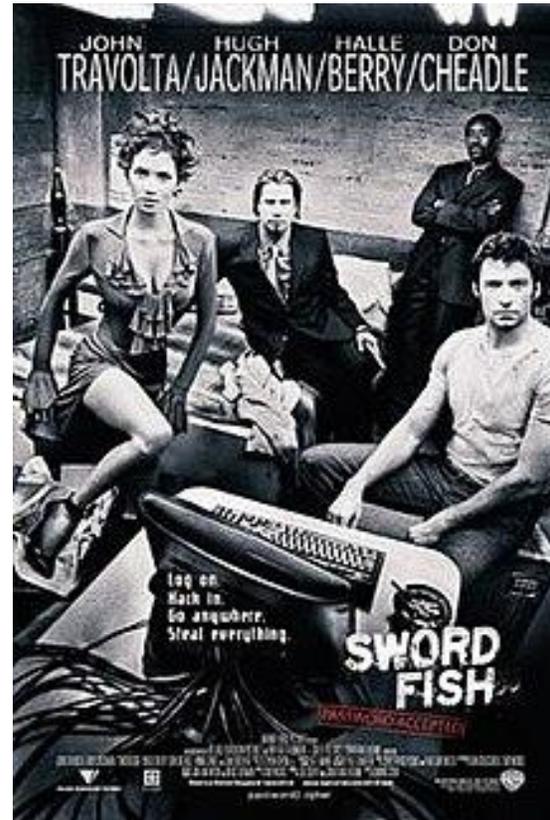
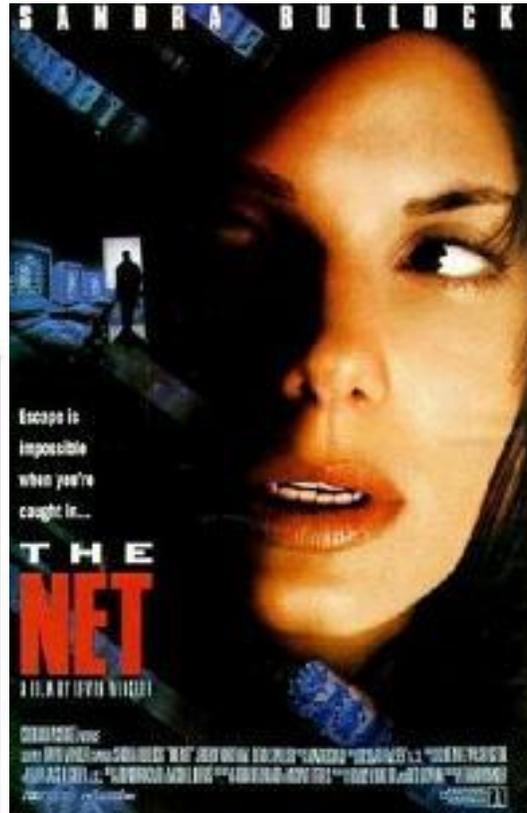
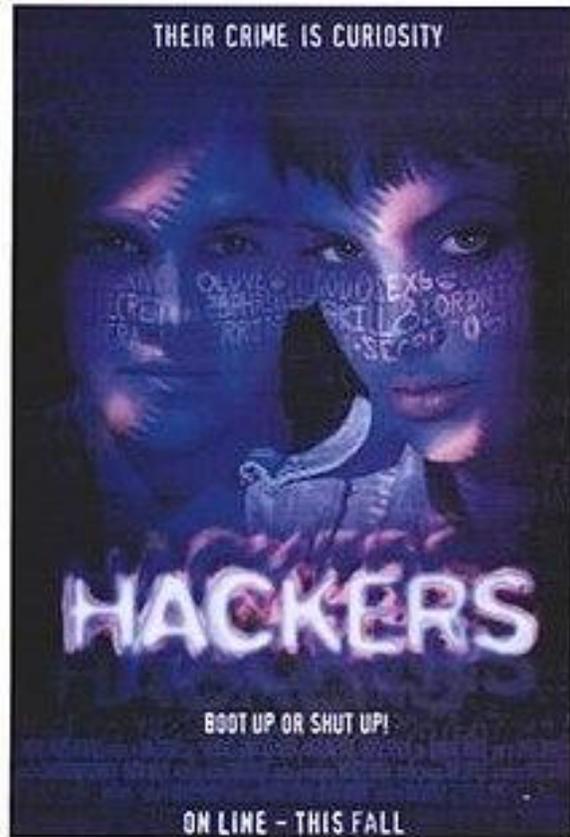
The Past

“Shall we play a game?”

Sometimes make mistakes.

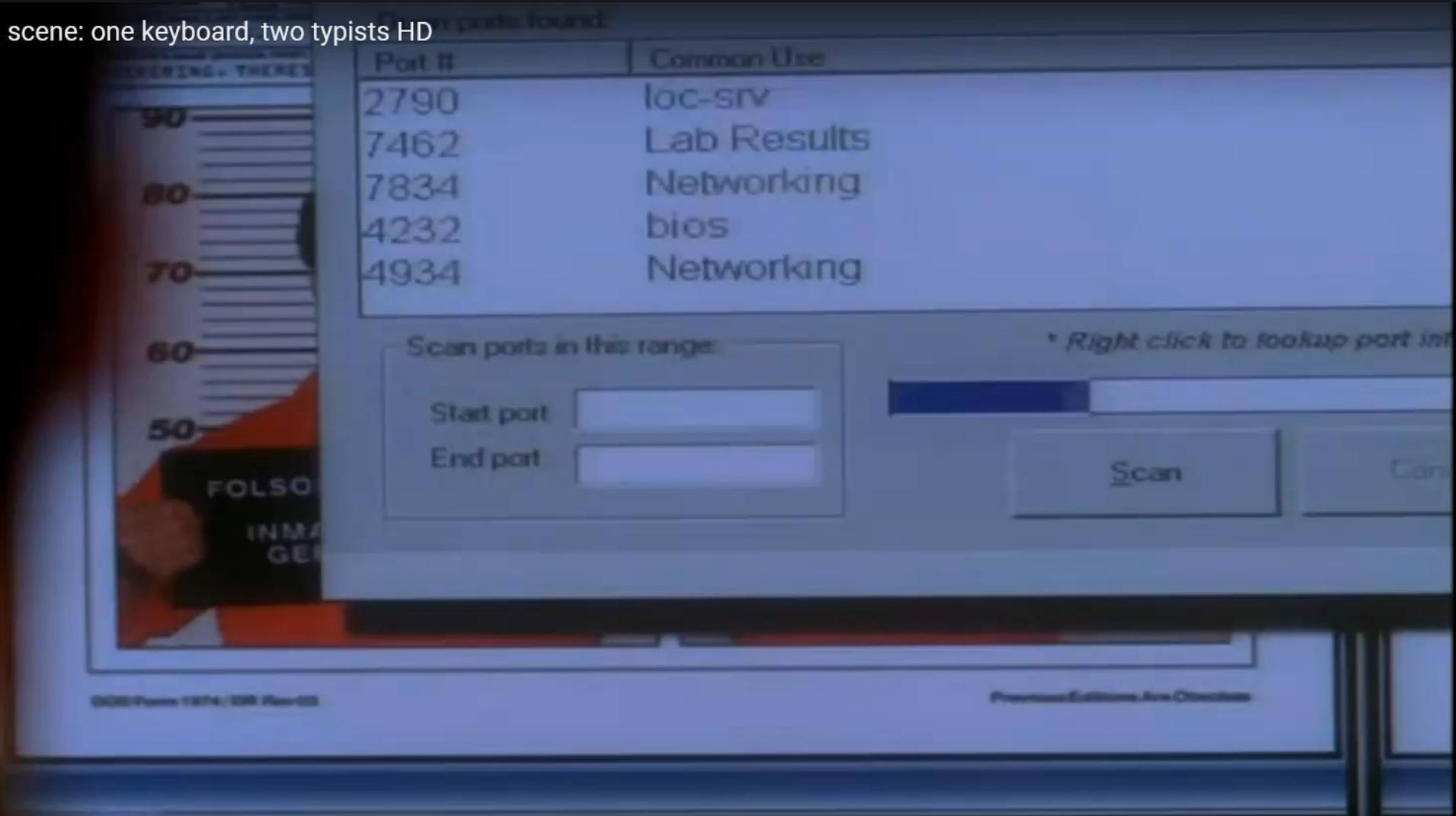
DO. SHALL WE PLAY A GAME?

Wargames, 1983, MGM, [https://www.mgm.com/#/our-titles/2117/WarGames-\(1983\)](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/The_Net_(1995_film)), [https://en.wikipedia.org/wiki/Hackers_\(film\)](https://en.wikipedia.org/wiki/Hackers_(film)), and [https://en.wikipedia.org/wiki/Swordfish_\(film\)](https://en.wikipedia.org/wiki/Swordfish_(film)))

NCIS ridiculous hacking scene: one keyboard, two typists HD



Pause (k)

0:00 / 0:58

Ruled for at se info

HD



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]

The Present

“We cannot be breached!”

Target Puts Data Breach Costs at \$148 Million, and Forecasts Profit Drop

By RACHEL ABRAMS AUG. 5, 2014

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

Massive data breach at health insurer Anthem could affect 80 million people

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



Amy Lee [Become a fan](#) [✉](#) [🐦](#) [👍](#)

Why Does Sony Keep Getting Hacked?

Posted: 06/08/2011 6:17 pm EDT | Updated: 08/08/2011 5:12 am EDT

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

Forbes.com Hacked by Syrian Electronic Army Because of "Hate for Syria"



By David Gilbert

February 14, 2014 10:20 GMT

[f](#) 42 [🐦](#) 63 [g+](#)

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

JP Morgan reveals data breach affected 76 million households



Elizabeth Weise, USATODAY 11:19 a.m. EDT October 3, 2014

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

10 April 2014 Last updated at 15:04 GMT



Heartbleed bug creates confusion online

By Mark Ward

Technology correspondent, BBC News

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

Lenovo hit by lawsuit over Superfish adware

Consumers and attorneys are already looking to the legal system for recourse following revelations that Lenovo installed potentially dangerous software on its PCs.

by Lance Whitney [🐦 @lancewhit](#) / February 24, 2015 9:29 AM PST

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

SecurID breach cost RSA \$66m

In 2nd quarter alone

27 Jul 2011 at 17:17, Dan Goodin

[🐦](#) 151

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

CCleaner hack affects 2.27 million computers -- here's what to do

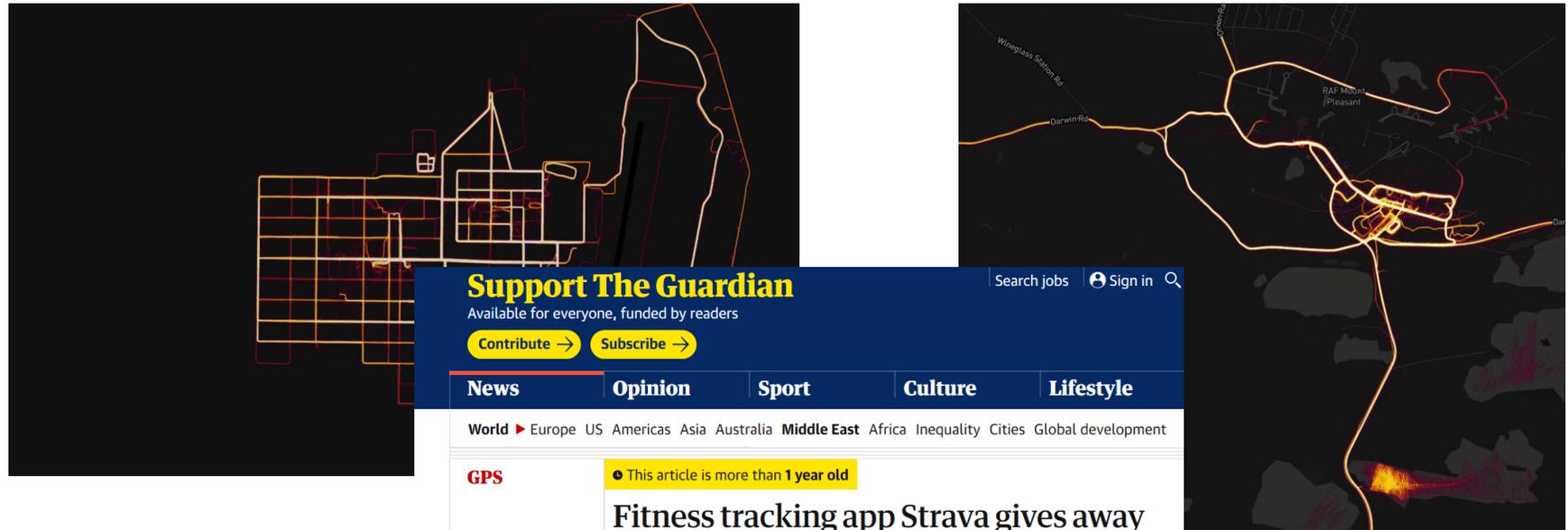
<https://www.cnet.com/how-to/ccleaner-was-hacked-heres-what-to-do-next/>

INTEGRATED INFRASTRUCTURE: CYBER RESILIENCY IN SOCIETY

Mapping the Consequences of an
Interconnected Digital Economy

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.



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>

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



MARKETS

BUSINESS

INVESTING

TECH

POLITICS

CNBC TV

Angry he wanted to double
pre...

Boris Johnson pushes Britain to brink of
an election: Here's what...

Hong Kong's leader will reportedly
announce withdrawal of bill...

Labour
election

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

SHARE



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>

Share



SHARE



TWEET



COMMENT



EMAIL



KIM ZETTER

IT WAS THE talk most anticipated
Usenix Enigma security conferer
that even the other speakers wei

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>

FRONTLINJEN

TIRSDAGE FRA 11-12

Hver dag deltager danske mænd og kvinder aktivt i missioner i uroprægede områder udenfor landets grænser, og samtidig løser Forsvaret samfundskritiske opgaver til lands, til vands og i luften herhjemme. Bag enhver operation ligger både taktik, politik og masser af isenkram. Journalist og tidligere reserveofficer Peter Ernstved Rasmussen tager dig med hele vejen fra den yderste militærpost og ind i de politiske baglokalder.



PETER ERNSTVED RASMUSEN

LIVE SENDEPLAN



27.10.20 (55 minutter)

TØR VI BRUGE VORES CYBERKAPACITETER?



Lyt med



Podcastsider

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 Løllesgaard 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 Rasmussen (Værten)

"Kan vi det?..."

Naser Khadar

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



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 **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>

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-formalet-var-afpresning>



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-half-milliard>

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>

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



(Illustration: Aleksandr Kalugin/Shutterstock)

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

Caroline Butler og Helsing Nielsen @henningnph Torsdag, 19. marts 2019 - 10:30



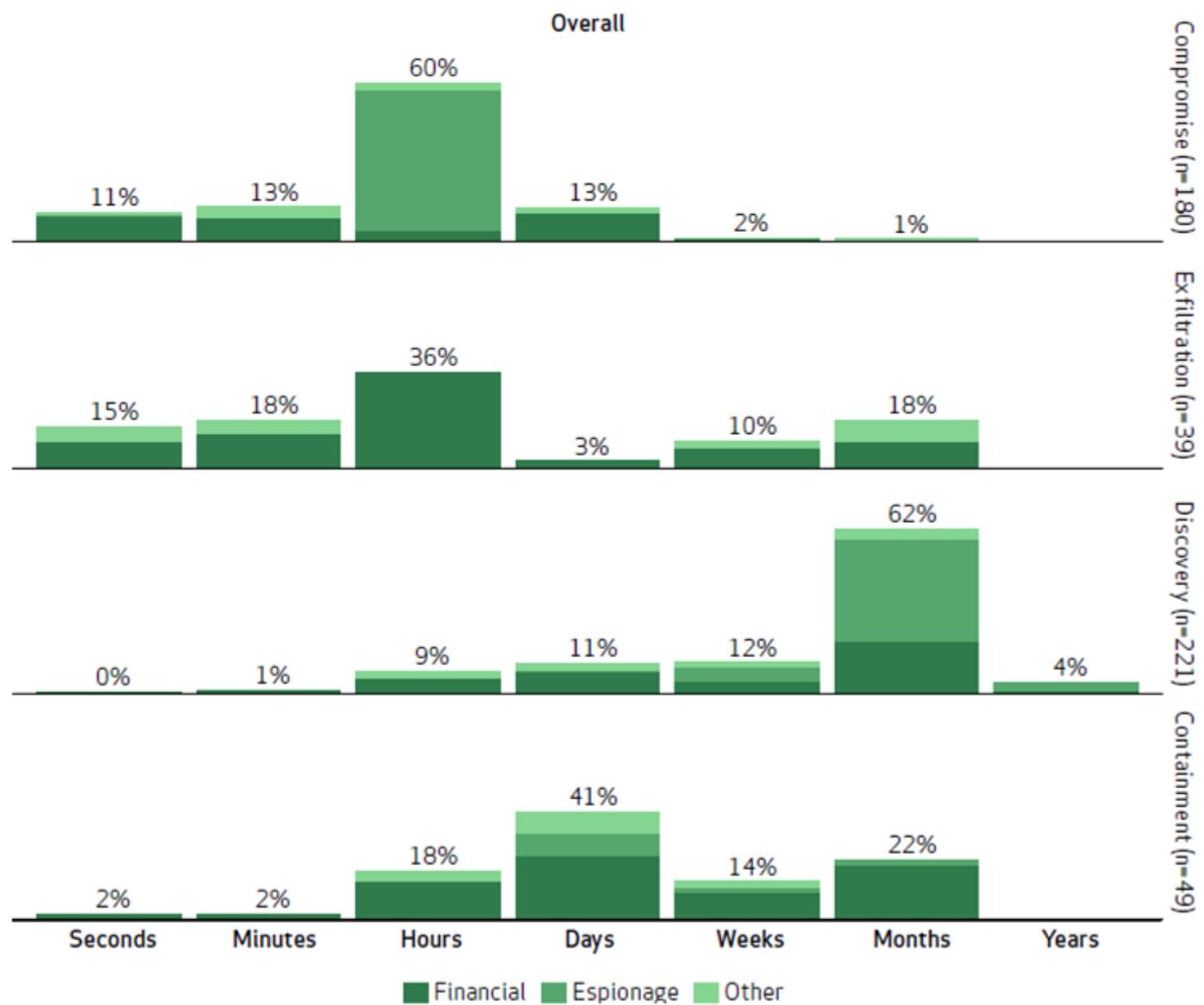
Opdateret kl. 11:51.

Norsk Hydro er udsat for et omfattende cyberangreb, som påvirker selskabets drift på flere parametre. Det skriver selskabet i en [børsmeldelse](#).

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

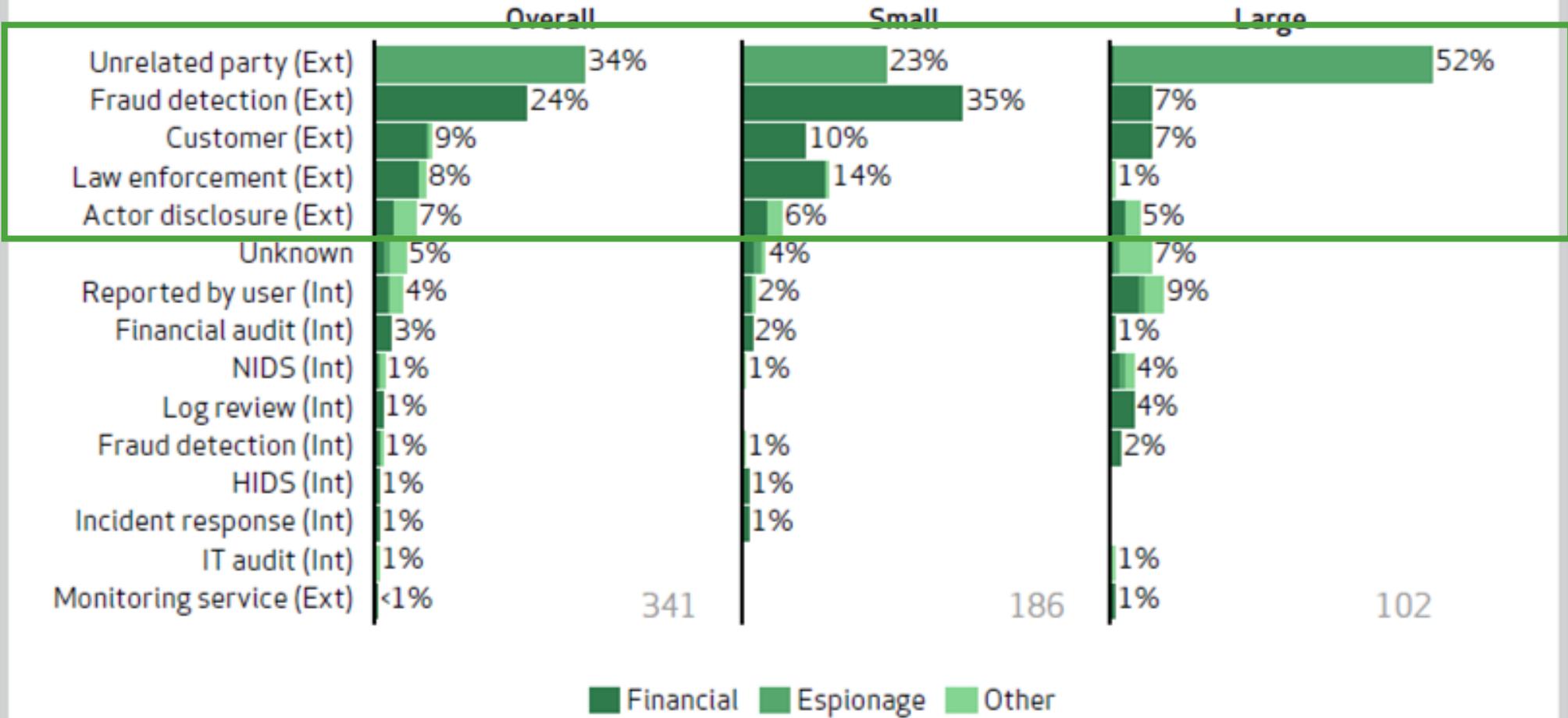
↓ Compromise
 Exfiltration
 Discovery
 Containment

Figure 41: Timespan of events

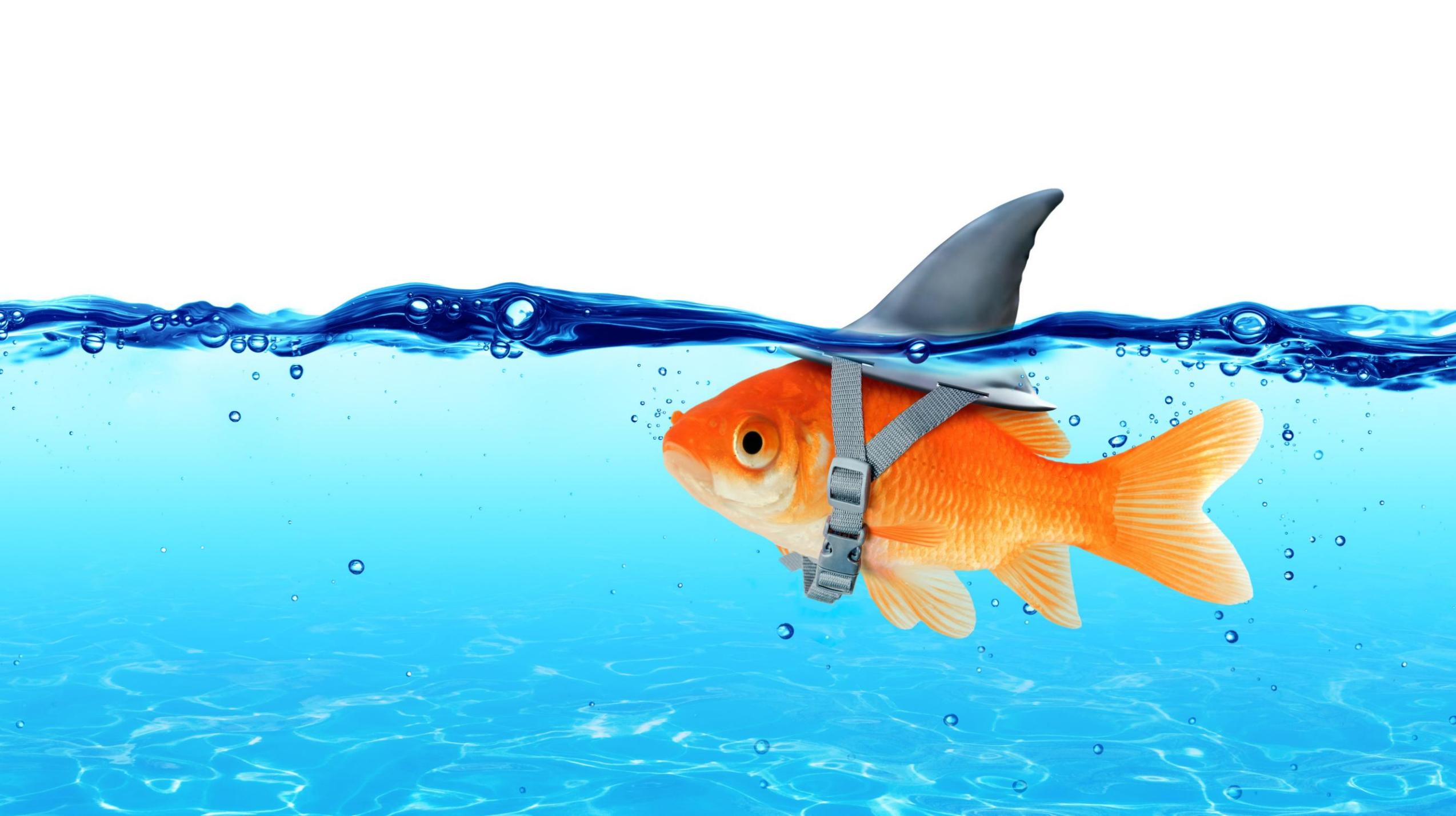


Sources: Verizon, 2013 Data Breach Investigations Report

Figure 44: Discovery methods



Sources: Verizon, 2013 Data Breach Investigations Report





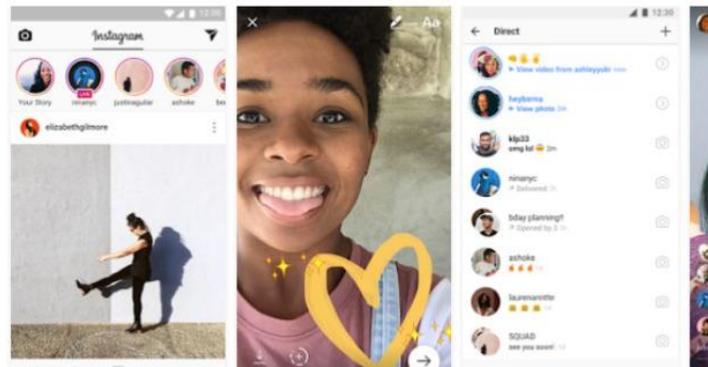

Instagram

instagram Communication ★★★★★ 128

PEGI 3

Contains ads
This app is compatible with your device.

Installed



Translate the description into English using Google Translate? Translate

Instagram is a simple way to capture and share the world's moments. Follow your friends and family to see what they're up to, and discover accounts from all over the world that are sharing things you love. Join the community of over 500 million people and express yourself by sharing all the moments of your day--the highlights and everything in between, too.

Use Instagram to:



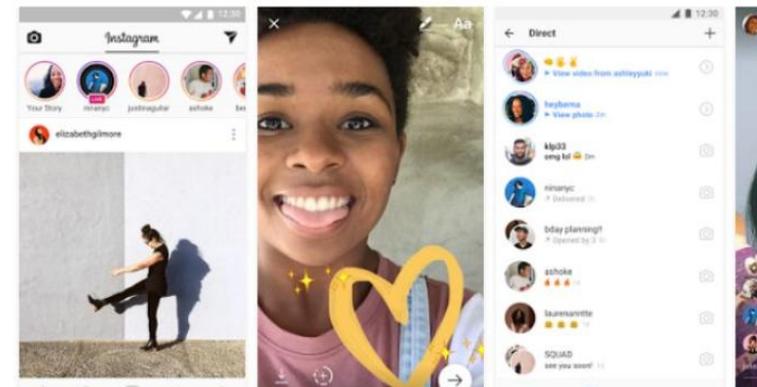
Instagram

Instagram Social ★★★★★ 54,023,710 Editors' Choice

Parental guidance

Contains ads
This app is compatible with your device.

Installed



Instagram is a simple way to capture and share the world's moments. Follow your friends and family to see what they're up to, and discover accounts from all over the world that are sharing things you love. Join the community of over 500 million people and express yourself by sharing all the moments of your day--the highlights and everything in between, too.

Use Instagram to:



21:48

Rasmus Seebach har udvekslet kontaktoplysninger med **Emma Larsen**.

- Emma Larsen er du rasmus seebach? 😊))) 21:48
- Rasmus Seebach ja da 21:48
- Emma Larsen hol da op hvor vilt 21:49
- jeg elsker dig! 21:50
- og din musik 21:50
- Rasmus Seebach 😞 21:50
- Emma Larsen hva laver du 21:50
- Rasmus Seebach ser tv 21:51
- Emma Larsen gider du ikke snakke 21:51
- ? 21:51
- Rasmus Seebach hvad 21:51
- Emma Larsen hva ser du i tv 21:52
- Rasmus Seebach er du forelsker 21:52
- Emma Larsen det ved jeg ikke.. måske 😊 21:53
- Rasmus Seebach i mig 21:53
- Emma Larsen det tror jeg 21:54
- Rasmus Seebach som hvad 21:54
- Emma Larsen som hvad? 21:54
- Rasmus Seebach vil du kys mig 21:55
- Emma Larsen det ved jeg ikke.. tror jeg mpske 21:55
- Rasmus Seebach må jeg kys dig 21:56
- Emma Larsen hihi.. måske.. 😊 21:56
- Rasmus Seebach hvor 21:56
- Emma Larsen min kind 21:57
- 📞 Opkald fra **Rasmus Seebach** 21:58



Rasmus Seebach

36 years old

SPONSORED:

[Vital Records](#) | [Social Profile](#) | [Username Report](#)

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



Rasmus Seebach, rasmus.seebach.55

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/_/10000352528600

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 kunde 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/022136f>

© Nets i Danmark (HQ)-kontoteamet



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



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/opsparringskonto.

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

Copyright © 2013 Skat.dk. Alle Rettigheder Forbeholdes.



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 kontakliste/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 hakede 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 kredittkort.
- Dine skatteoplysninger.
- Dine investeringer og pension.

Afresning

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>

© SANS Institute - You are free to print, distribute and post as many copies of this poster as you like; the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit www.securingthehuman.org/resources/posters

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 været 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

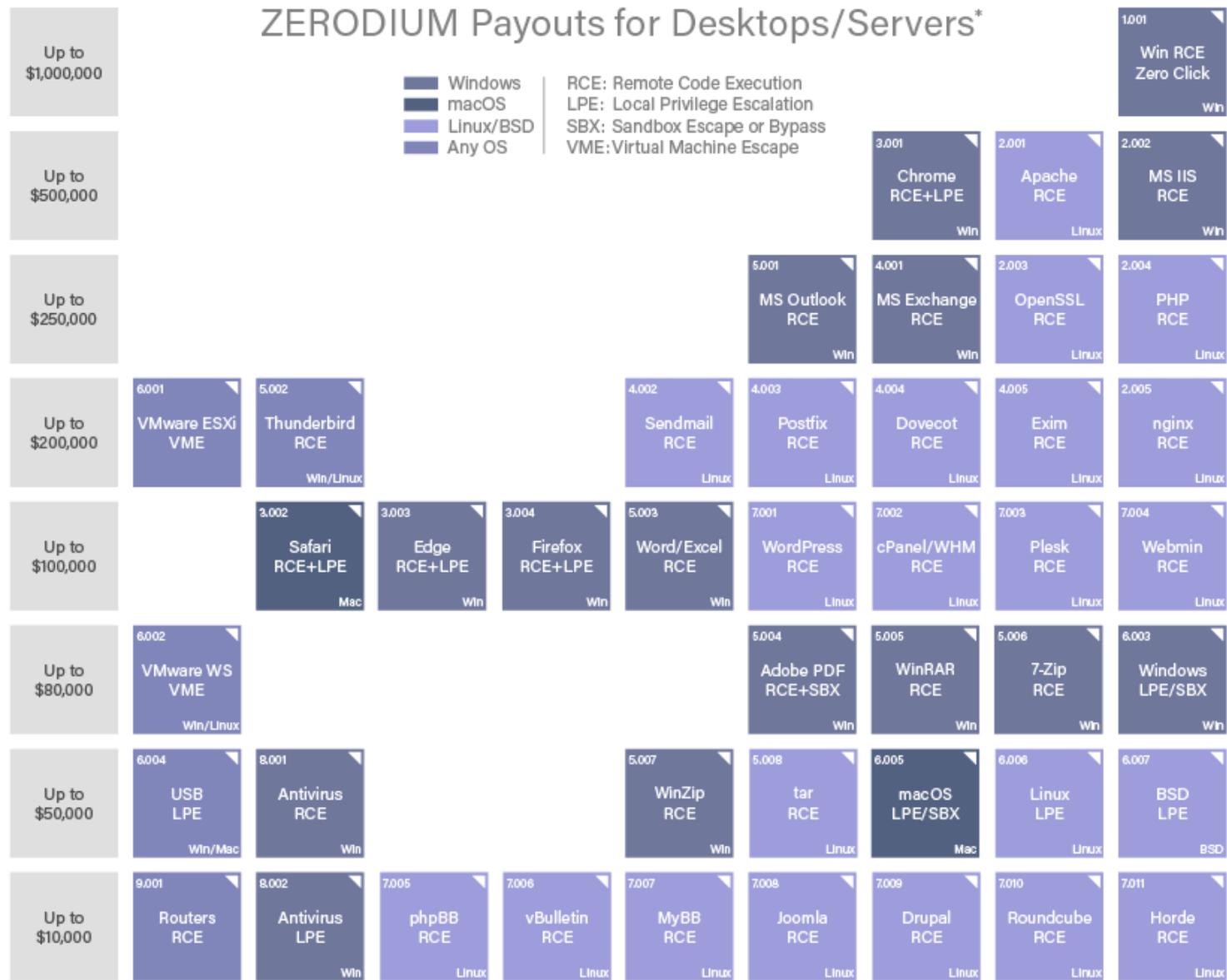
An attack is low risk and high ROI

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

ZERODIUM Payouts for Desktops/Servers*



* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

RDP
RUSSIAN MARKET

📧 🔔 🛒 📁 🔍 \$ 0

- 📰 News
- 📄 Dumps
- 🖥️ RDP
- 📁 SSH
- 🔒 Stealer Logs
- 💰 PayPal
- 🔍 Checkers
- 🔧 Tools
- 📦 My Purchases
- 🛠️ Support

IP:

Country:

State:

City:

OS:

ISP:

RAM:

In Speed:

Out Speed:

NAT:

Admin:

Paypal:

Vendor:

Per page:

Price: 33 \$

Mask	Country	State / City	Details	Info	Vendor	Blacklist	Price	Action
180.164**** ISP: China Telecom (Group)		Shanghai Huangpu	OS: Win2008/7 Proc: Intel Core i5 RAM: 6 GB @: 12.65 / 35.83 Mbit/s	Admin: No Paypal: No NAT: No	de###ck [platinum]	BL	\$ 5.00	<input type="button" value="Buy"/>
158.247**** ISP: Choopa, LLC		Seoul Seoul	OS: Win2008/7 Proc: Intel Core i5 RAM: 6 GB @: 12.65 / 35.83 Mbit/s	Admin: No Paypal: No NAT: No	de###ck [platinum]	BL	\$ 5.00	<input type="button" value="Buy"/>
103.45**** ISP: CHINANET Sichuan province Chengdu MAN network		Guangdong Shenzhen	OS: Win2008/7 Proc: Intel Core i5 RAM: 6 GB @: 12.65 / 35.83 Mbit/s	Admin: No Paypal: No NAT: No	de###ck [platinum]	BL	\$ 5.00	<input type="button" value="Buy"/>
183.69**** ISP: Triple T Internet Company Limited		Lampang Lampang	OS: Win2008/7 Proc: Intel Core i5 RAM: 6 GB @: 12.65 / 35.83 Mbit/s	Admin: No Paypal: No NAT: No	de###ck [platinum]	BL	\$ 5.00	<input type="button" value="Buy"/>
175.143**** ISP: Trinet, Telekom Malaysia Bhd.		Perak Ipoh	OS: Win2008/7 Proc: Intel Core i5 RAM: 6 GB @: 12.65 / 35.83 Mbit/s	Admin: No Paypal: No NAT: No	de###ck [platinum]	BL	\$ 5.00	<input type="button" value="Buy"/>
51.145**** ISP: Microsoft Corporation		England London	OS: Win2016 Proc: Intel Xeon CPU E5-2673 v4 2.30GHz RAM: 1 GB @: 29.33 / 34.69 Mbit/s	Admin: No Paypal: - NAT: Yes	i##### [platinum]	BL	\$ 6.00	<input type="button" value="Buy"/>

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/>

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	

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



TOTAL RESULTS

7

TOP COUNTRIES



[View Report](#) [View on Map](#)

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

Object moved

2022-10-03

20.224.244.100
 ok-upgrade1f396bb0c
 d95f648adevpos.axclo
 ud.dynamics.com
 ok-upgrade1f396bb0c
 d95f648adevecom.axc
 loud.dynamics.com
 ok-upgrade1f396bb0c
 d95f648adevaos.axclo
 ud.dynamics.com
 ok-upgrade1f396bb0c
 d95f648adevaossoap.
 axcloud.dynamics.com
 ok-upgrade1f396bb0c
 d95f648adevret.axclou
 d.dynamics.com
[Microsoft Corporation](#)

 Netherlands, Amsterdam

SSL Certificate

Issued By:
 |- Common Name:
Microsoft Azure TLS
Issuing CA 06
 |- Organization:
Microsoft
Corporation
Issued To:
 |- Common Name:
 ok-
 upgrade1f396bb0cd95f648adevaos.axcloud.dynamics.com
 |- Organization:
Microsoft
Corporation

HTTP/1.1 302 Found
 Cache-control: private
 Content-Type: text/html; charset=utf-8
 Location: https://login.windows.net/ok.dk/wsfeed?wa=wsignin1.0&wtrealm=spn%3a06



Host Filters

Autonomous System:

- 10 TDC TDC AS
- 3 MICROSOFT-CORP-MSN-AS-BLOCK
- 2 AMAZON-02
- 1 AS5413
- 1 GLOBALCONNECT-AS31027

[More](#)

Location:

- 12 Denmark
- 3 Netherlands
- 2 Ireland
- 1 United Kingdom

Service Filters

Hosts

Results: 18 Time: 0.29s

[54.194.133.85 \(ec2-54-194-133-85.eu-west-1.compute.amazonaws.com\)](#)

-  AMAZON-02 (16509)  Leinster, Ireland
-  80/HTTP  443/HTTP
-  services.tls.certificates.leaf_data.names: email.ok.dk
-  services.tls.certificates.leaf_data.subject.common_name: email.ok.dk

[54.77.59.67 \(ec2-54-77-59-67.eu-west-1.compute.amazonaws.com\)](#)

-  AMAZON-02 (16509)  Leinster, Ireland
-  80/HTTP  443/HTTP
-  services.tls.certificates.leaf_data.names: email.ok.dk
-  services.tls.certificates.leaf_data.subject.common_name: email.ok.dk

[62.242.37.183](#)

Bring a company offline?



The Future

“Assume Breach – Detect Compromise”

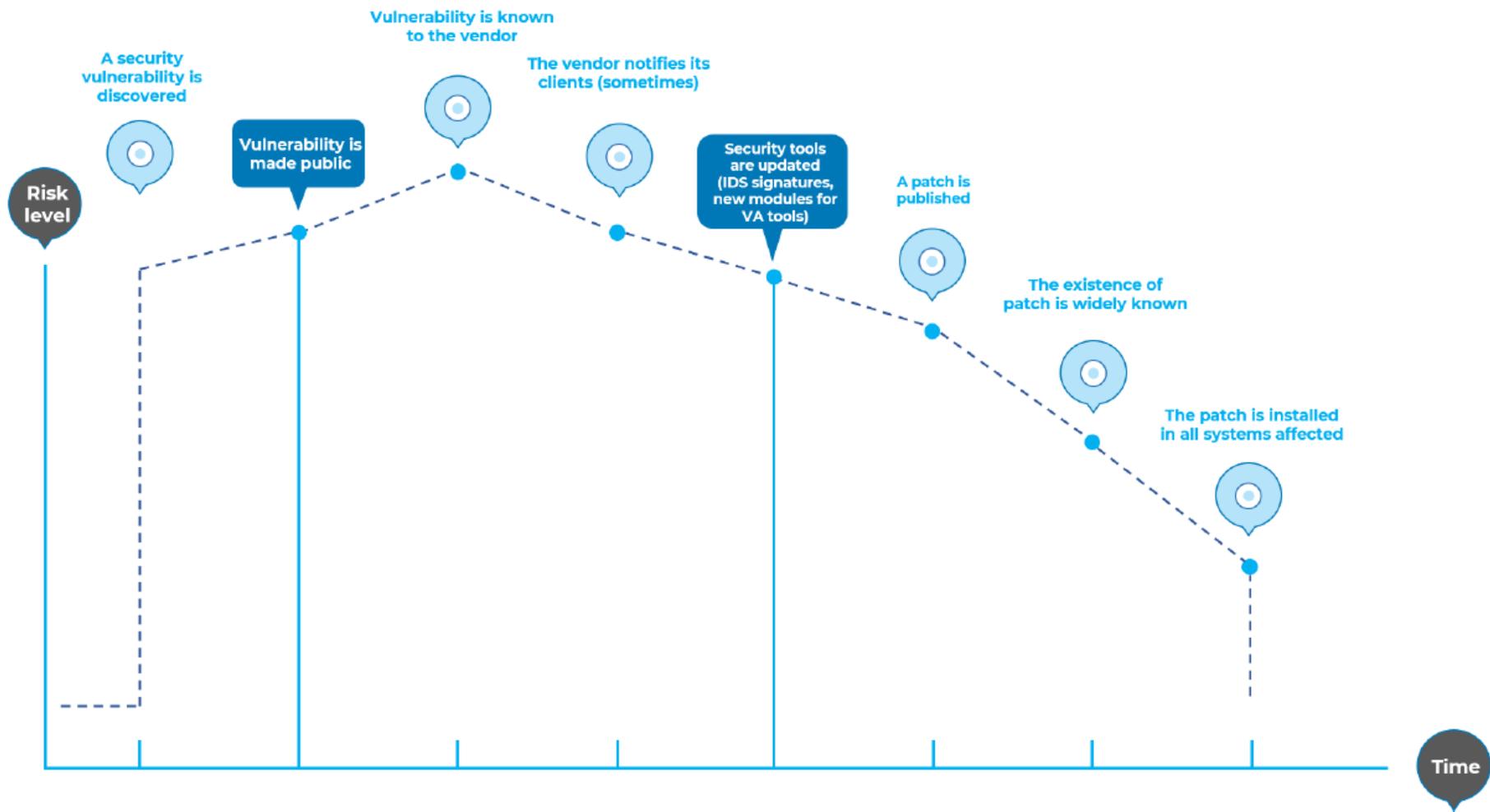
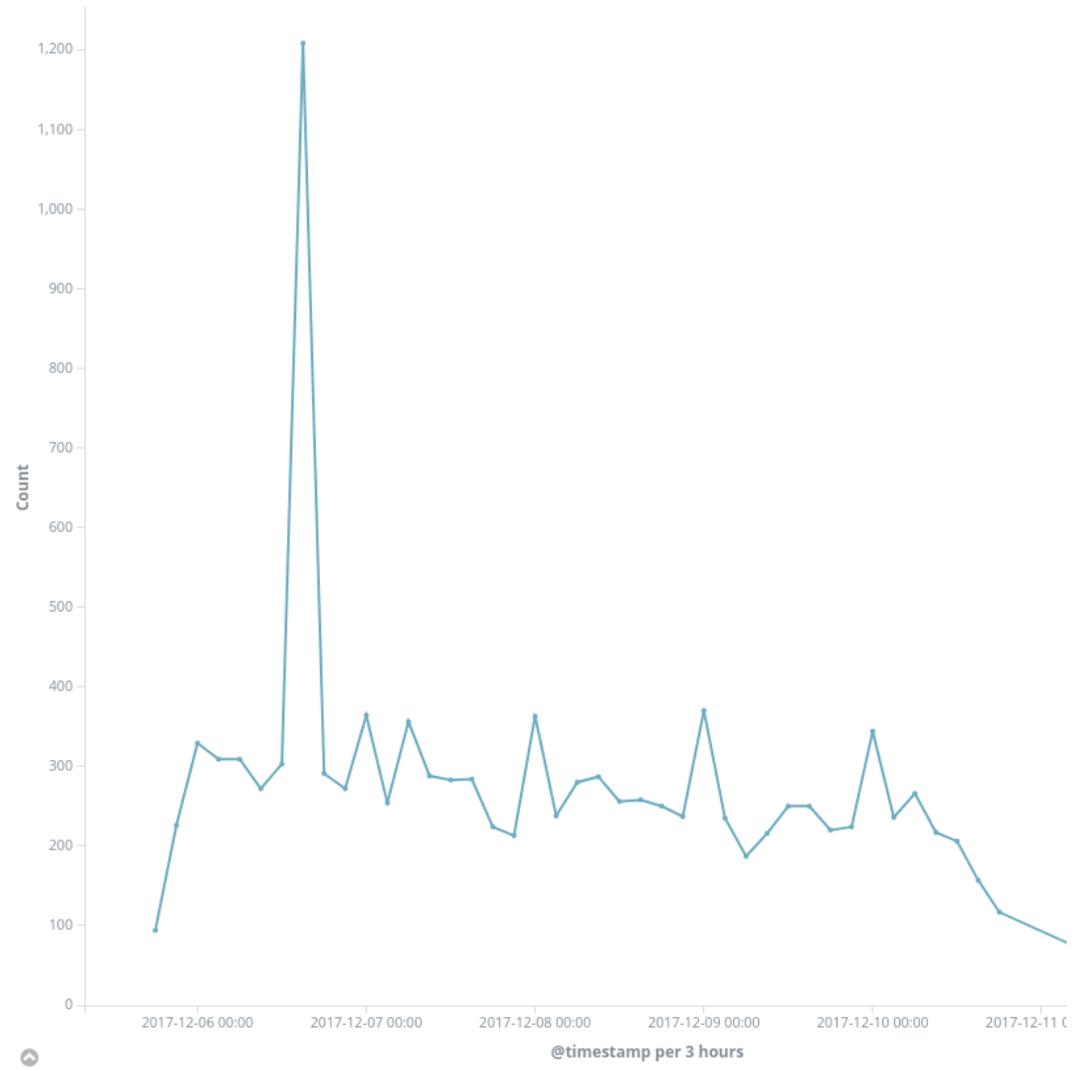
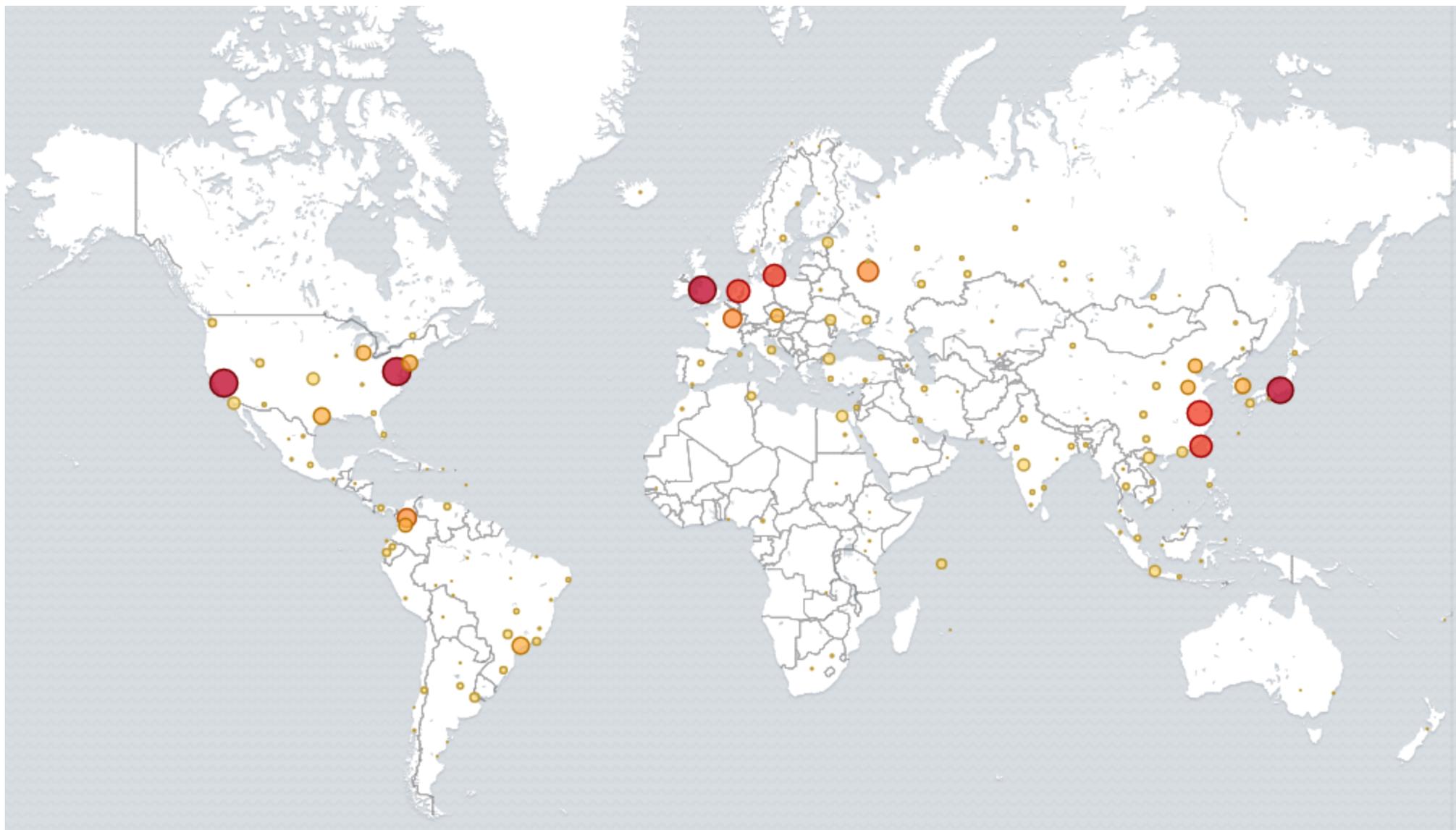


Figure 2-2: Window of Vulnerability

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





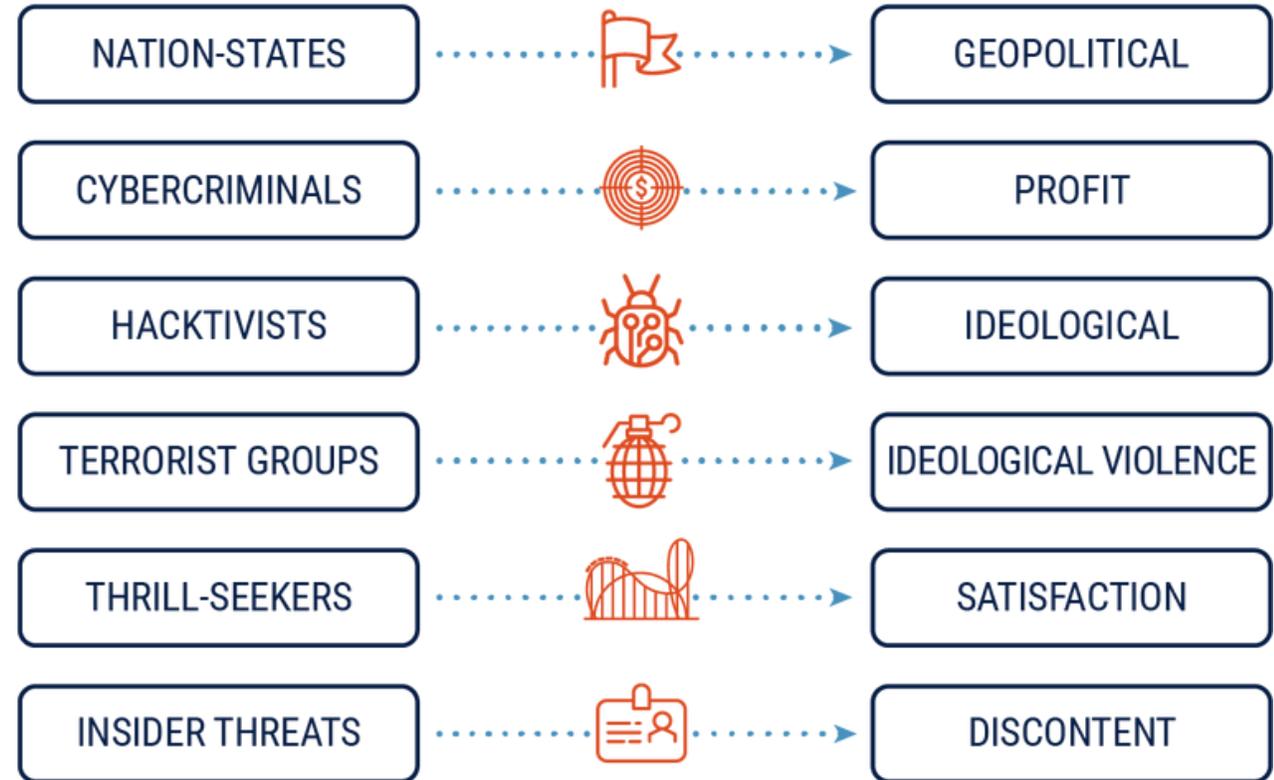
“There are only two types of companies: Those that **have been hacked**, and those that **will be**.”

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

CYBER THREAT ACTOR



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



The DFIR Report @TheDFIRReport · Nov 5

Ryuk Speed Run, 2 Hours to Ransom

- ➔ Discovery using Net, Nltest, 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...

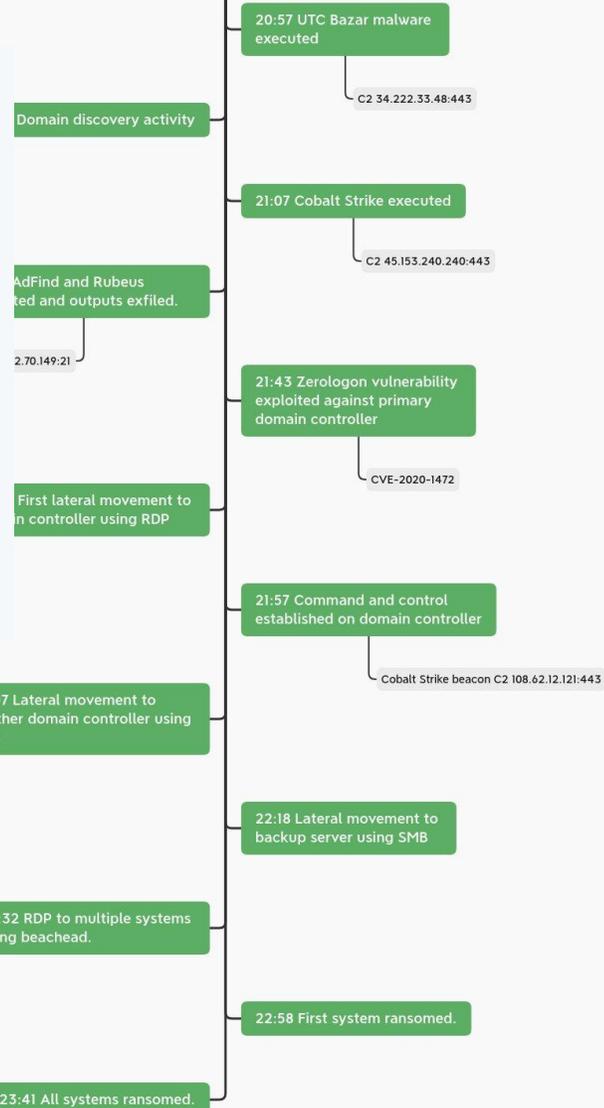
The screenshot shows a timeline of events for the 'Ryuk Speed Run, 2 Hours to Ransom' incident. The events listed are:

- 21:02 Domain discovery activity
- 20:57 UTC Bazar malware executed (C2 34.222.33.48:443)
- 21:07 Cobalt Strike executed (C2 45.153.240.240:443)

 Below the timeline is a screenshot of a network traffic analysis tool showing a list of connections and their details, including source and destination IP addresses and ports.

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

Ryuk Speed Run, 2 Hours to Ransom

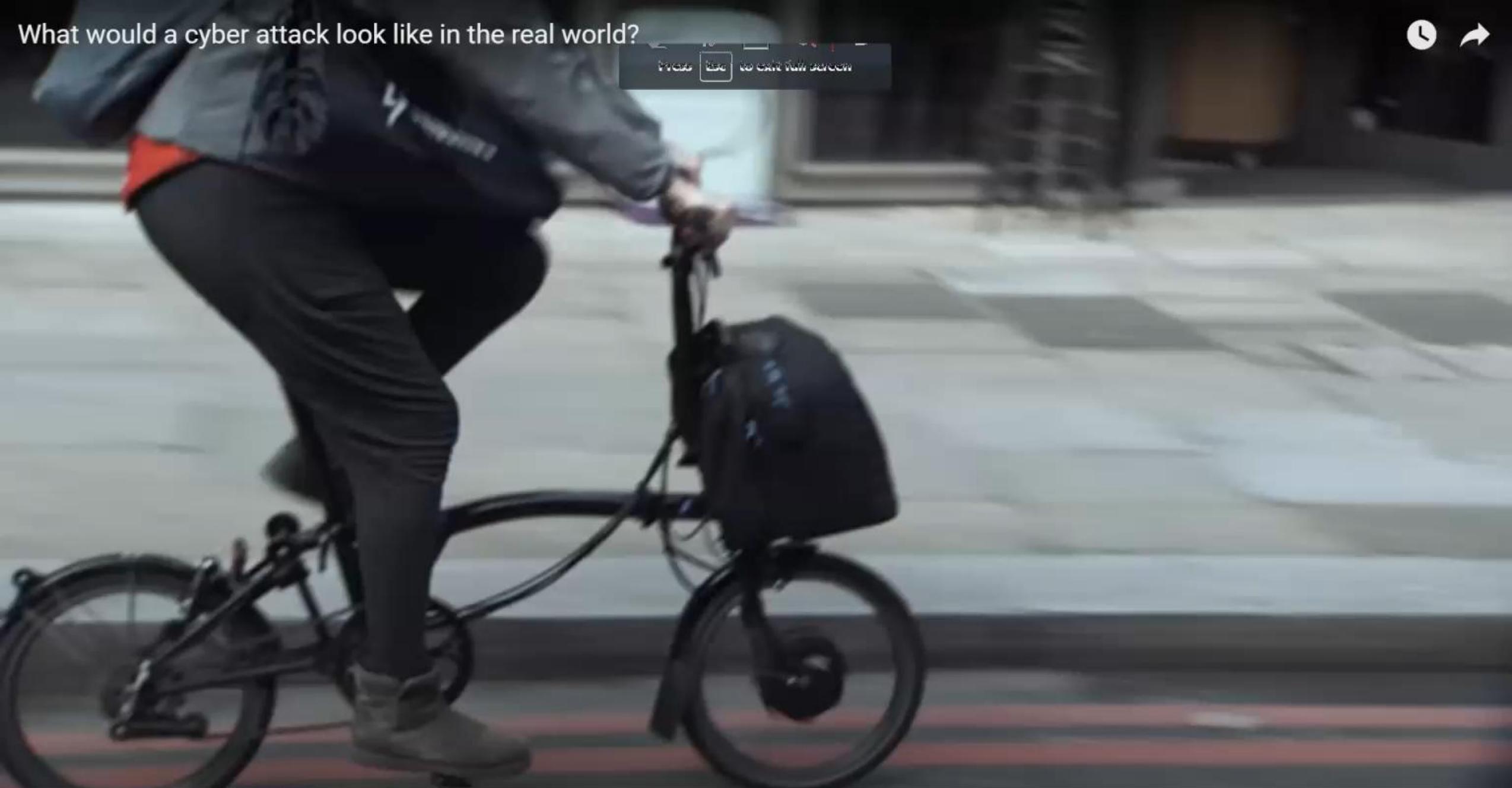


<https://twitter.com/TheDFIRReport/status/1324408962318557184/photo/1>

What would a cyber attack look like in the real world?



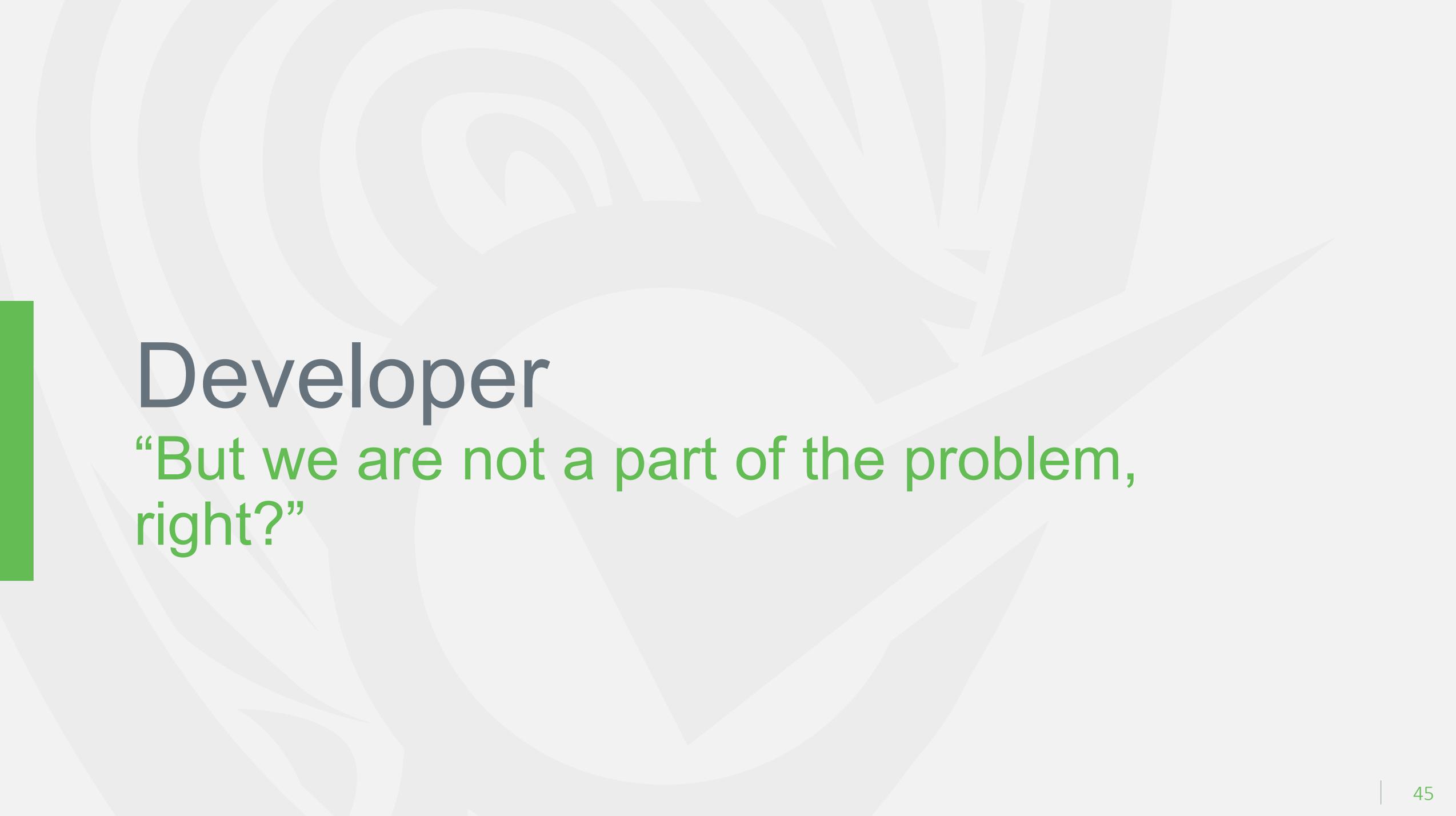
Press Esc to exit full screen



0:00 / 2:49

Scroll for details



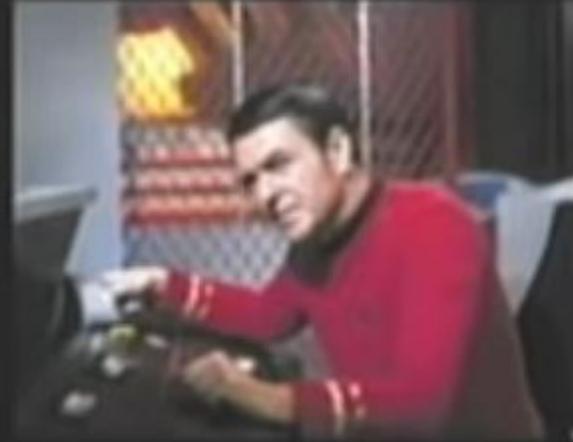


Developer

“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 ...



Rolling Stones "Start me up"



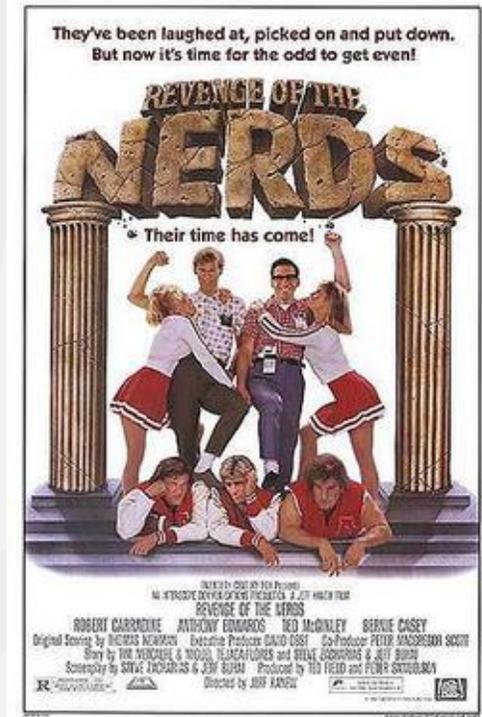
Windows 95 Launch

5.525.158 visninger...

👍 98.353

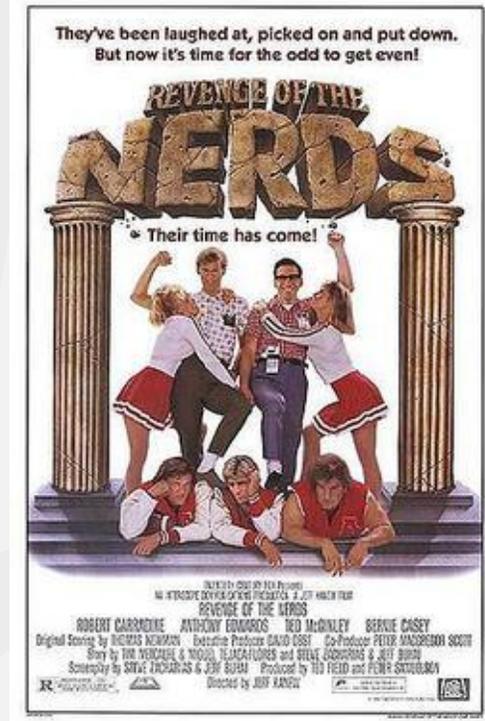
👎 KAN IKKE LIDE

🔗 DEL ⚙️ GEM ⋮



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 ⋮





Press Esc to exit full screen



Building Blocks and Abstraction



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

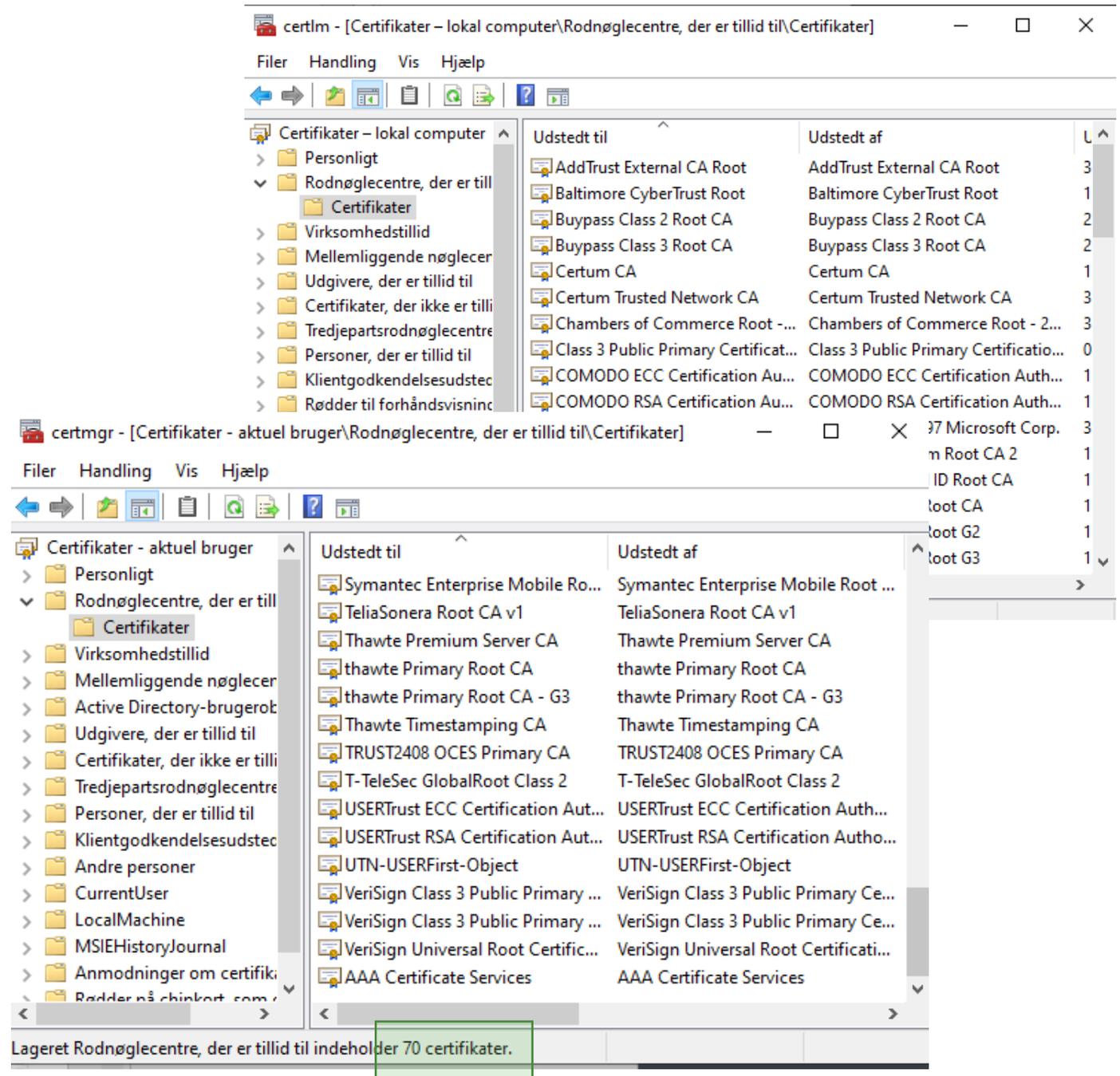


https://en.wikipedia.org/wiki/Turtles_all_the_way_down

Whom do we trust to impersonate everyone else!?

Certificate Manager – Local and Personal

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



- > 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, Docker Daemon configuration and more, and learn to automate security testing

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 (Scored)
[WARN] 2.13 - Ensure centralized and remote logging is configured (Scored)
[WARN] 2.14 - Ensure containers are restricted from acquiring new privileges (Scored)
[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 appropriate (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
dpkg                    1.21.1ubuntu2           1.21.1ubuntu2.1
e2fsprogs               1.46.5-2ubuntu1
libcom-err2             1.46.5-2ubuntu1
libext2fs2              1.46.5-2ubuntu1
libgmp10                2:6.2.1+dfsg-3ubuntu1
libpcre2-8-0            10.39-3build1
libpcre2-8-0            10.39-3build1
libpcre3                2:8.39-13build5
libpcre3                2:8.39-13build5        2:8.39-13ubuntu0.22.04.1
libss2                  1.46.5-2ubuntu1
libssl3                 3.0.2-0ubuntu1        3.0.2-0ubuntu1.1
libsc13                 2.0-0ubuntu1

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$ █

```

JavaScript-bibliotek overskriver russiske filer med hjertesymboler

It-sikkerhed | 18. marts kl. 10:10 | 8



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

Microsoft-ansatte lækker login-oplysninger til interne systemer på Github

Dataleæk | 17. august kl. 12:00

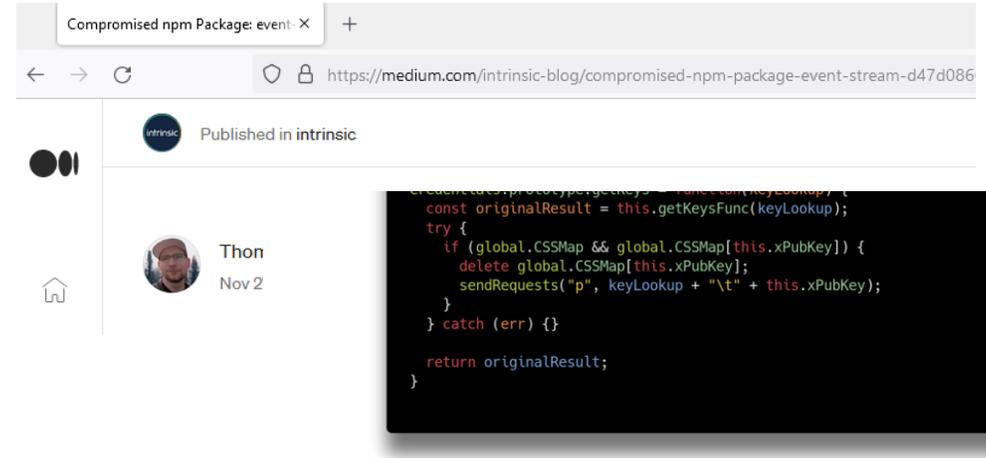


<https://www.version2.dk/artikel/microsoft-ansatte-laekker-login-oplysninger-til-interne-systemer-paa-github>

APPLICATION SECURITY | VULNERABILITIES

Alert: peacenotwar module sabotages npm developers in the node-ipc package to protest the invasion of Ukraine

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



Compromised npm Package: event-stream

Ownership of a popular npm package, `event-stream`, was transferred by the original author to a malicious user `right9ctrl`. This package receives over

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



Dev corrupts NPM libs 'colors' and 'faker' breaking thousands of apps

By [Ax Sharma](#)

January 9, 2022 09:17 AM 32



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



How an irate developer briefly broke JavaScript

/ Unpublishing 11 lines of code

Npm is all about packages built on other packages, which is how left-pad ended up everywhere. According to `npm` stats, left-pad has been installed 2,550,569 times in the last month — mostly as part of a package called "line-numbers," which adds line numbers to text. In addition to many other projects, line-numbers was included in the "Babel" package, which in turn broke thousands of JavaScript projects relying on Babel.

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



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.

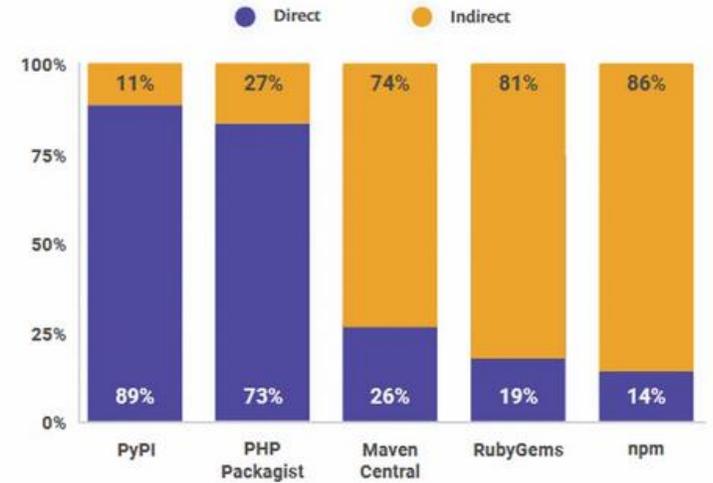


Written by Catalin Cimpanu, Contributor on June 26, 2020



"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."

Vulnerabilities from direct versus indirect dependencies



But the Snyk team also pointed to another quirk 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.

THE LATEST DRM-DEFEATING KIT FOR APPLE'S ITUNES.



UserFriendly.org

<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.



DON'T GET HOOKED!

WHAT IS PHISHING?

Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to almost any message-based attack. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well-known store.

These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or responding to a scam. Cyber criminals craft these convincing-looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people they will have the opportunity to hack. In addition, cyber criminals are not limited to just email but will use other methods, such as instant messaging or social media posts.

WHAT IS SPEAR PHISHING?

The concept is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. With spear phishing, the cyber attackers research their intended targets, such as by reading the intended victims' LinkedIn or Facebook accounts or any messages they posted on public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

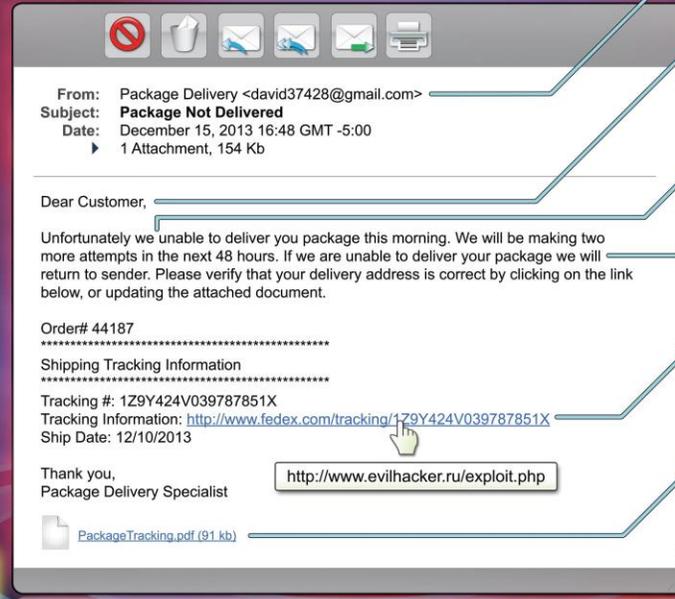
This poster was developed as a community project. Contributors include: Cheryl Conley (Lockheed Martin), Tim Harwood (BP), Tonia Dudley (Honeywell), Elen Powers (MITRE Corporation), Shanah Johnson (Reserve Bank of Atlanta) and Terri Chihota.

WHY SHOULD I CARE?

You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them: YOU are the most effective way to detect and stop phishing. If you identify an email you think is a phishing attack, or you are concerned you may have fallen victim, contact your help desk or security team immediately. To learn more about phishing or to demo the SANS Securing The Human phishing testing platform, please visit <http://www.securingthehuman.org/phishing>.

PHISHING INDICATORS

- A** Check the email addresses. If the email appears to come from a legitimate organization, but the "FROM" address is someone's personal account, such as @gmail.com or @hotmail.com, this is most likely an attack. Also, check the "TO" and "CC" fields. Is the email being sent to people you do not know or do not work with?
- B** Be suspicious of emails addressed to "Dear Customer" or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also ask yourself, am I expecting an email from this company?
- C** Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.
- D** Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.
- E** Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different then what is shown in the email, this is an indication of an attack.
- F** Be suspicious of attachments. Only click on those you are expecting.
- G** Be suspicious of any message that sounds too good to be true. No, you did not just win the lottery.
- H** Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.



© SANS Institute - You are free to print, distribute and post as many copies of this poster as you like, the only limitation is you cannot modify or sell it. For digital copies of this and other security awareness posters, visit www.securingthehuman.org/resources/posters

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

Demo

Phishing

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

Kære kunde 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/022136f>

© Nets i Danmark (HQ)-kontoteamet



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 forsendesetiketten, 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



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>

Copyright © 2013 Skat.dk. Alle Rettigheder Forbeholdes.

';--have i been pwned?

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.



Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles



LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords



Verifications.io: In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

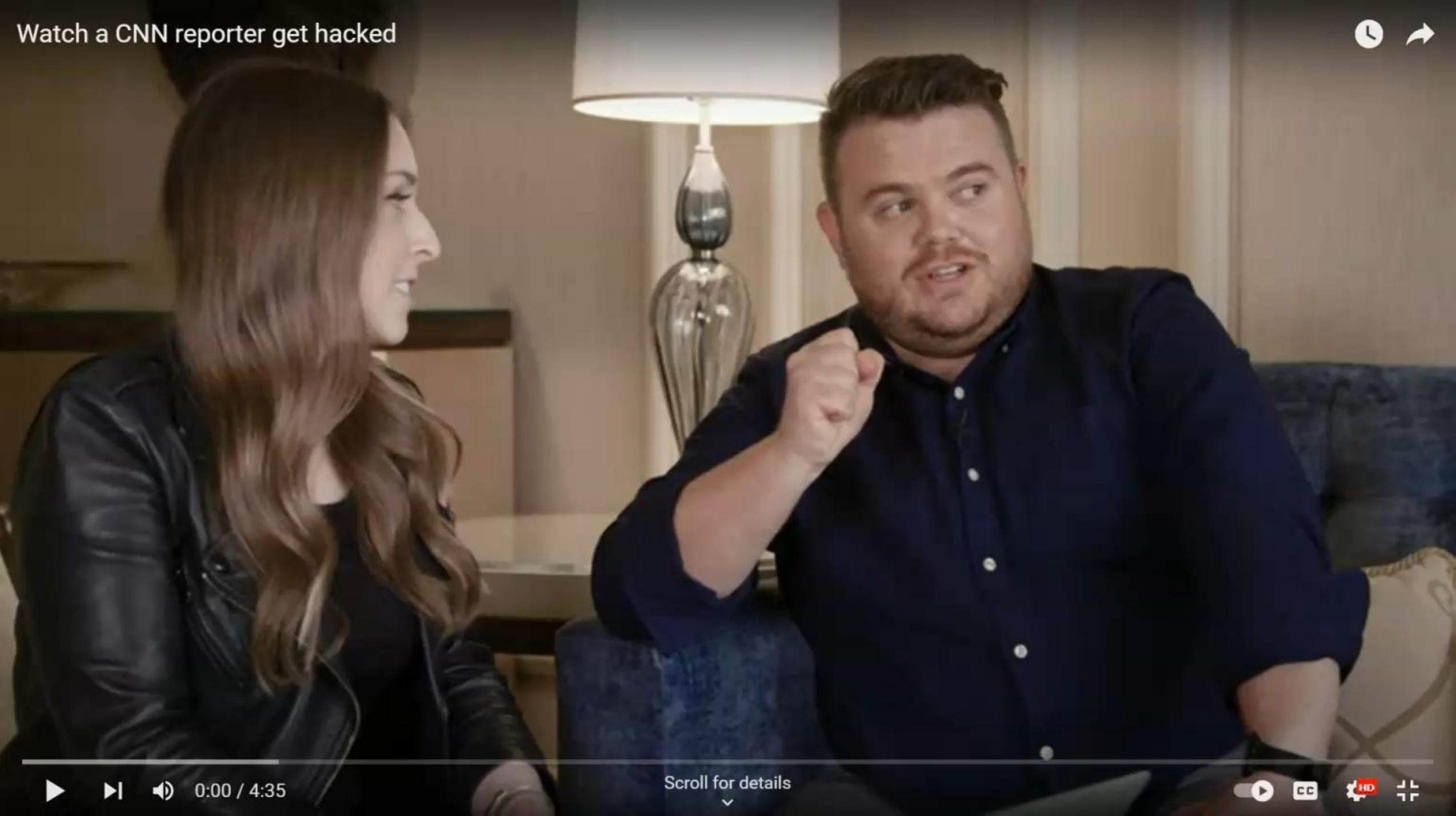
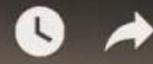
Compromised data: Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses,

<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		

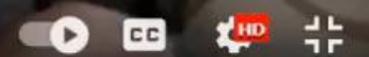
Row Labels	Count of password
ok **** ko	55
to **** un	46
al **** 12	46
qa **** 12	25
mr **** dw	23
12 **** 45	21
si **** on	18
so **** ri	18
he **** he	18

Watch a CNN reporter get hacked



▶ ⏪ 🔊 0:00 / 4:35

Scroll for details
▼





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 bekræftet!

04 Klik ikke på links

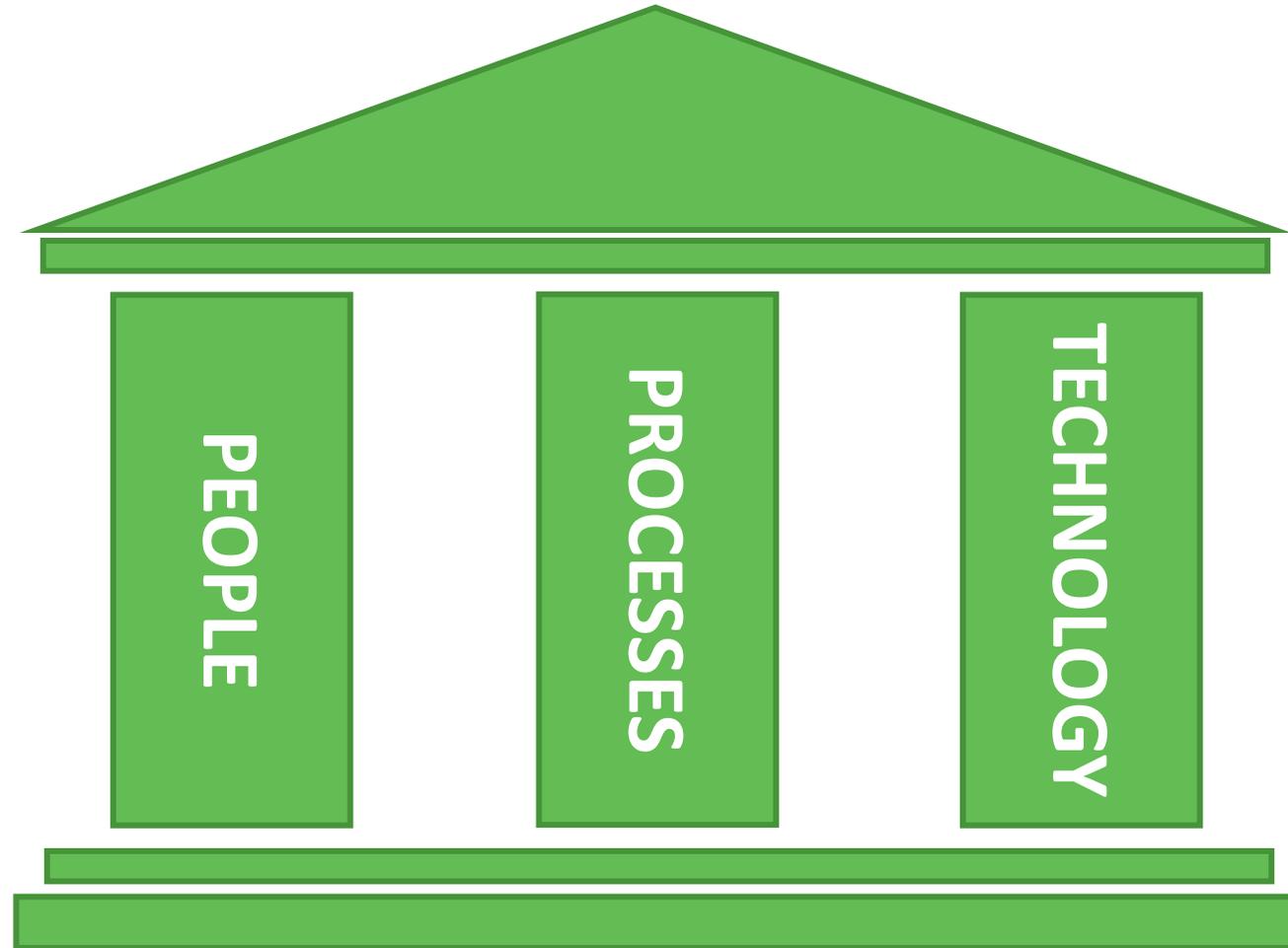
Lad være med at klikke på alle links, du modtager! Overvej evt. at taste dem selv!

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!

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

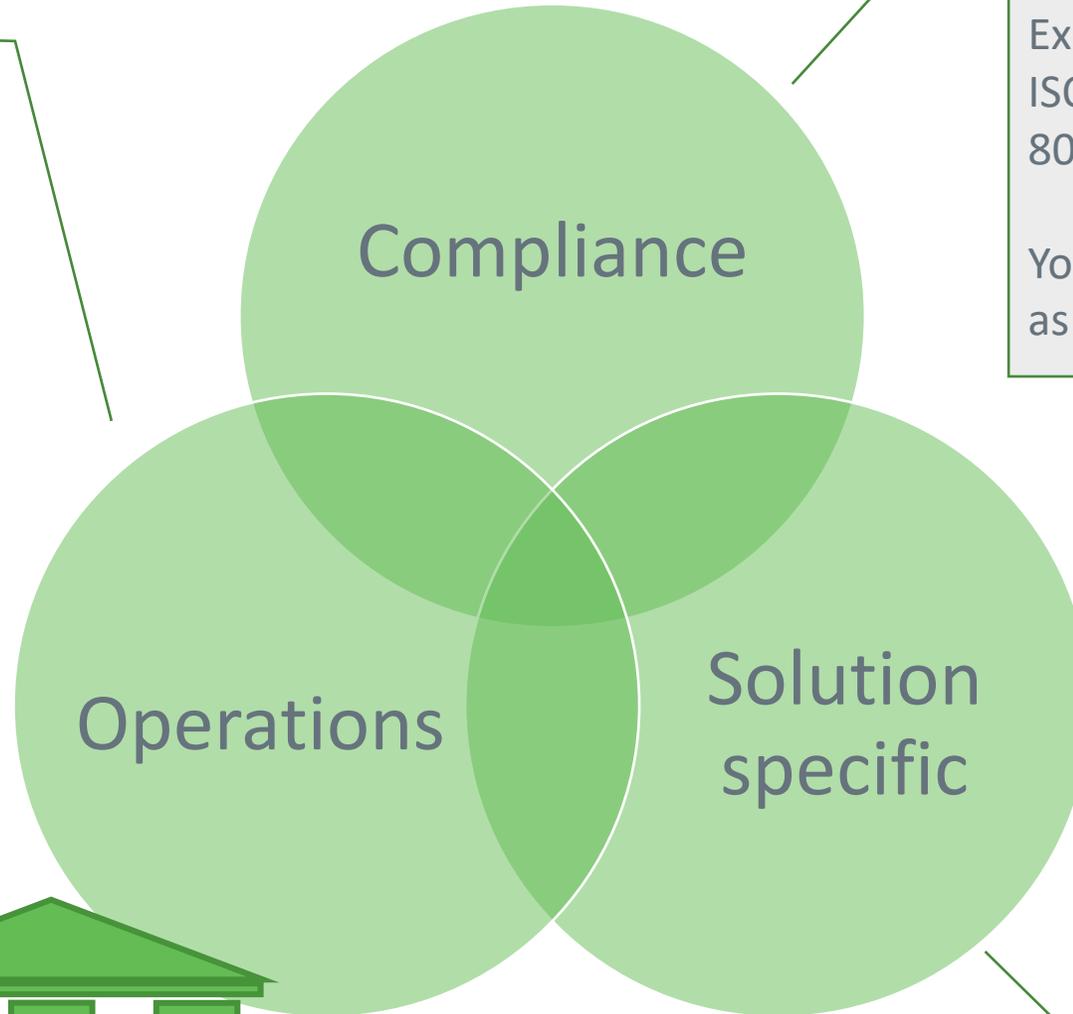
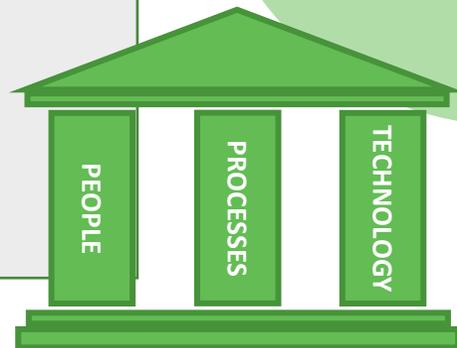
Catalog of Security Controls:

OWASP Proactive Controls
ISO 27002
NIST SP 800-53

Other:

MITRE ATTACK
Misuse/abuse cases

OWASP Software Assurance Maturity Model (SAMM)

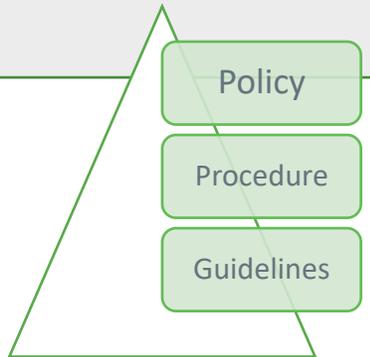


Regulatory, Company-wide, etc.

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!

Informationsteknologi – Sikkerhedsteknikker – Ledelsesystemer for information

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://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

1
(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>

Home Research Events Infographics Sources Audio podcasts

The NIS2 Directive: A high common level of cybersecurity in the EU

19-02-2021
The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market. To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by the NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term. Within the European Parliament, the file has been assigned to the Committee on Industry, Research and Energy. First action: The 'Fit 11' initiative in 'Proactive'

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

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



Critical Security Controls



Confidence in the Connected World

Quick Links:

[CIS Controls](#)

[CIS Benchmarks](#)

[CIS Hardened Images](#)

[Cybersecurity Best Practices](#)

[Cybersecurity Tools](#)

[Cybersecurity Threats](#)

CIS SecureSuite[®]
Membership

[Apply](#) [Learn more](#) [Logi](#)

Home • CIS Controls

CIS Controls™

Follow our prioritized set of actions to protect your organization and data from known cyber attack vectors.

[Download all CIS Controls \(PDF & Excel\) →](#)



→ [Learn about the 20 individual CIS Controls and other resources](#)

THE CYBER KILL CHAIN[®]

The New York Times

Stolen Data Is Tracked to Hacking at Lockheed

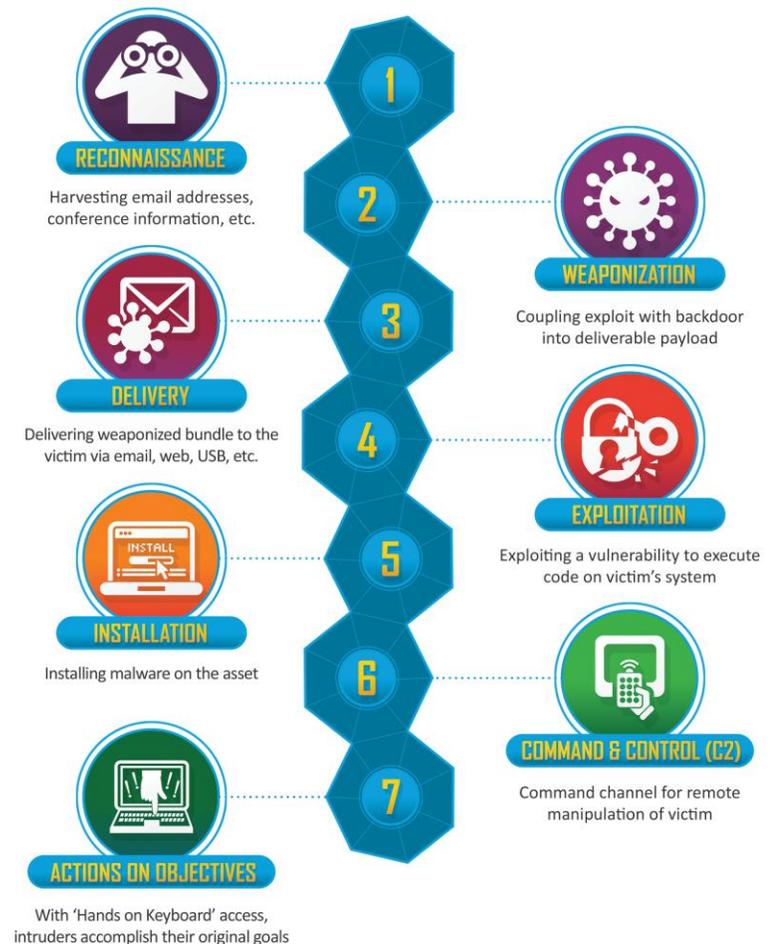
By CHRISTOPHER DREW JUNE 3, 2011

[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>

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 of 492



ICS > 35 > 35.030

ISO/IEC 27002:2013

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

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>

BUY THIS STANDARD

FORMAT

LANGUAGE

PDF + COLOR PDF + EPUB

English

PDF + EPUB

English



10 Critical Security Areas That Software Developers Must

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

eficode

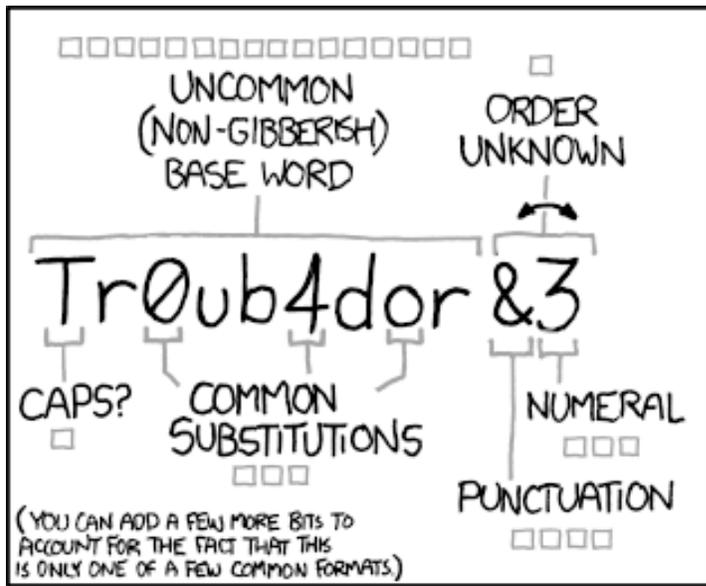
8 - Introduction

[https://www.eficode.com/hubfs/guides/DevOps and cloud guide - Eficode.pdf](https://www.eficode.com/hubfs/guides/DevOps%20and%20cloud%20guide%20-%20Eficode.pdf)

<https://agilemanifesto.org/>

- Kent Beck
- Mike Beedle
- Arie van Bennekum
- Alistair Cockburn
- Ward Cunningham
- Martin Fowler
- James Grenning
- Jim Highsmith
- Andrew Hunt
- Ron Jeffries
- Jon Kern
- Brian Marick
- Robert C. Martin
- Steve Mellor
- Ken Schwaber
- Jeff Sutherland
- Dave Thomas





~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

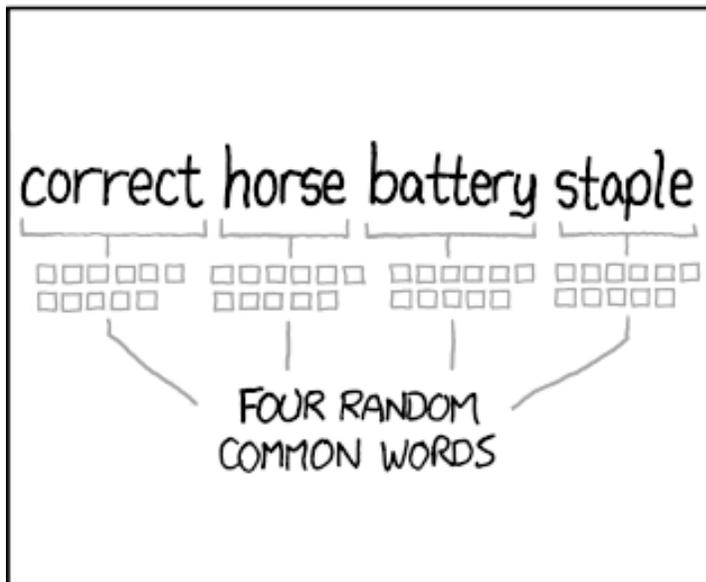
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Security is a **process** not a goal!

You will never be secure against everything.

It is about choosing what to secure against.



cje 🌻 🗳️ @caseyjohnellis · 20/04/2021 ...

threat actor = someone who wants to punch you in the face

threat = the punch being thrown

vulnerability = your inability to defend against the punch

risk = the likelihood of getting punched in the face

84

584

1.670



cje 🌻 🗳️ @caseyjohnellis ...

acceptable risk = your willingness to be punched in the face



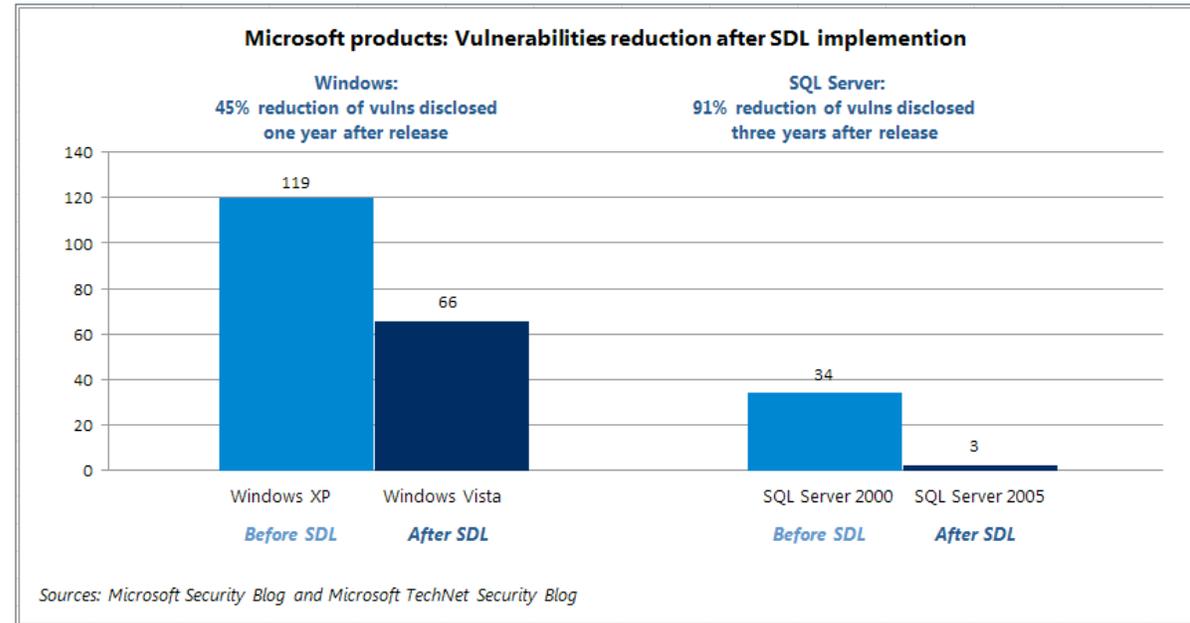
Memo from Bill Gates

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>

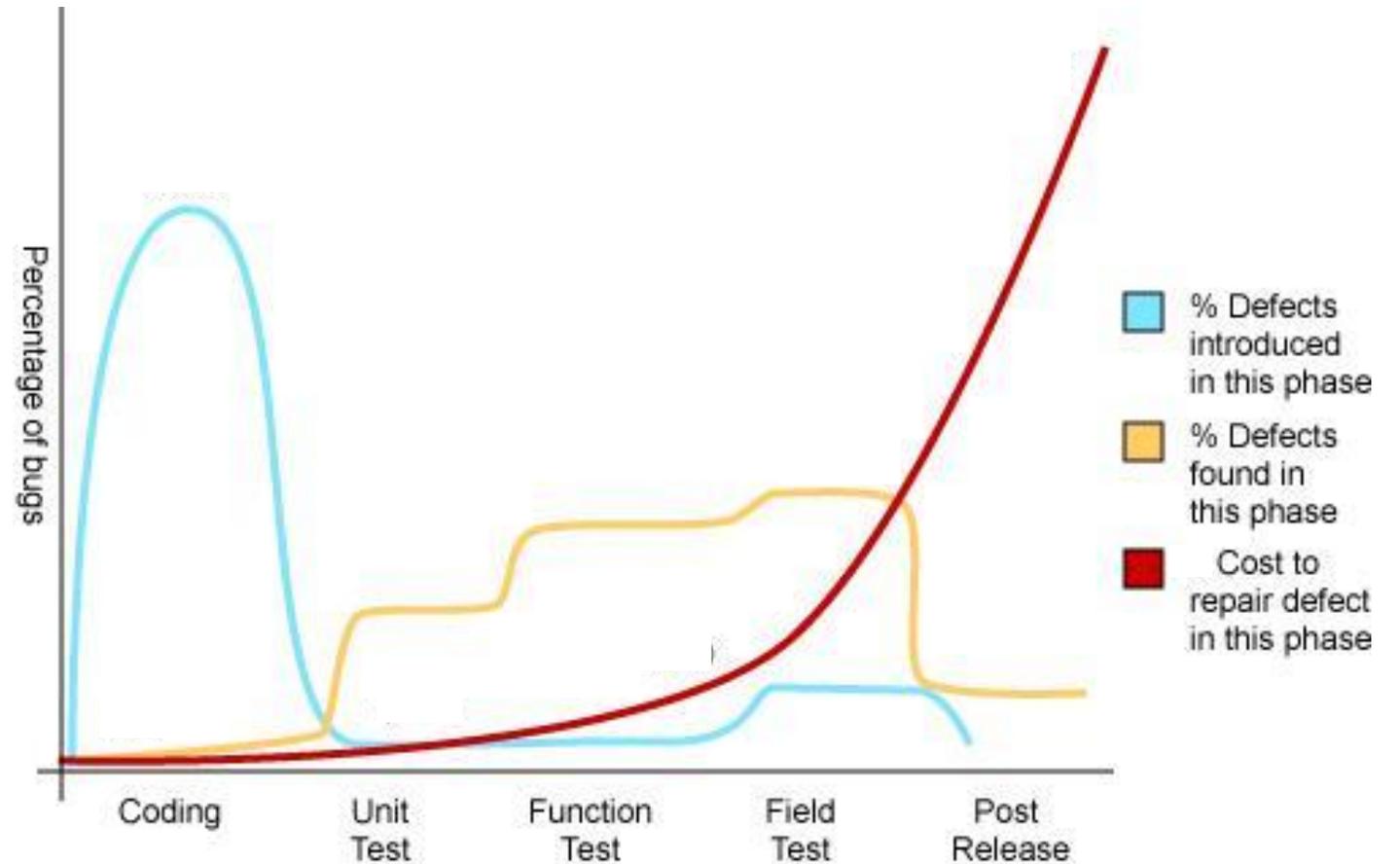
	Millions LOC	Estimated Number of Defects
Simple iOS game	0,01	10 – 250
Win32/Simile virus	0,01	10 – 250
Google Chrome	6,7	6.700 – 167.500
Windows XP	40,00	40.000 – 1.000.000
Windows 7	40,00	40.000 – 1.000.000
Software typical car, 2013	100,00	100.000 – 2.500.000

<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

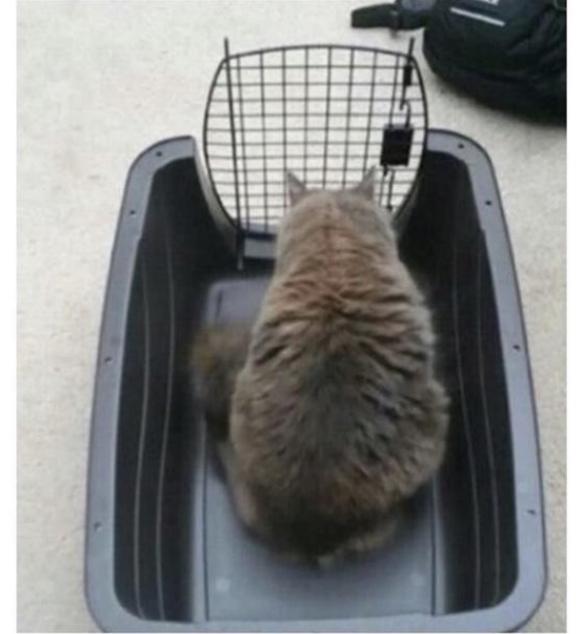


Adapted from “Applied Software Measurement, Capers Jonas, 1996

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

Establishing Security Requirement

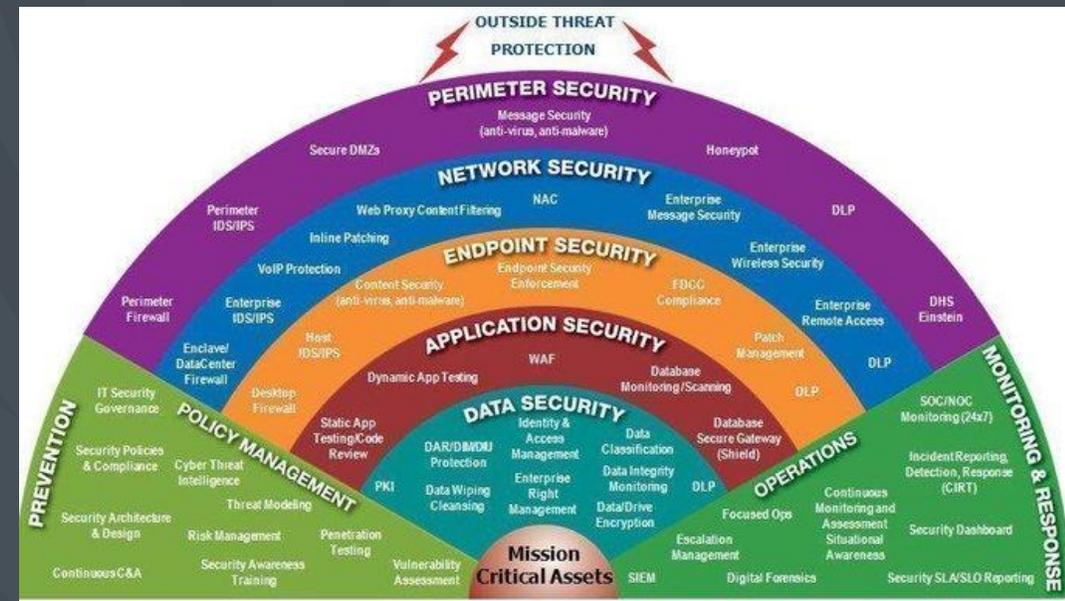
If you focus too hard on the problem..



..the solution can often evade you.

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

– Or what are we building?



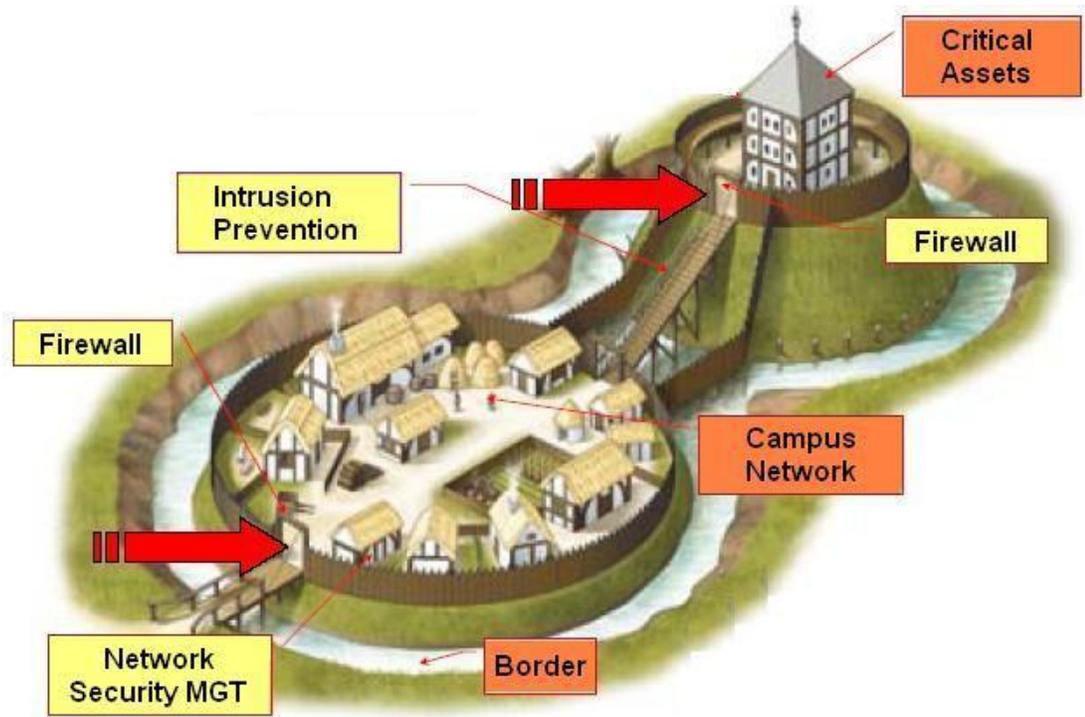
<https://twitter.com/Fisher85M/status/1030976170181976064>

Defense in Depth

– Overlapping Security Controls

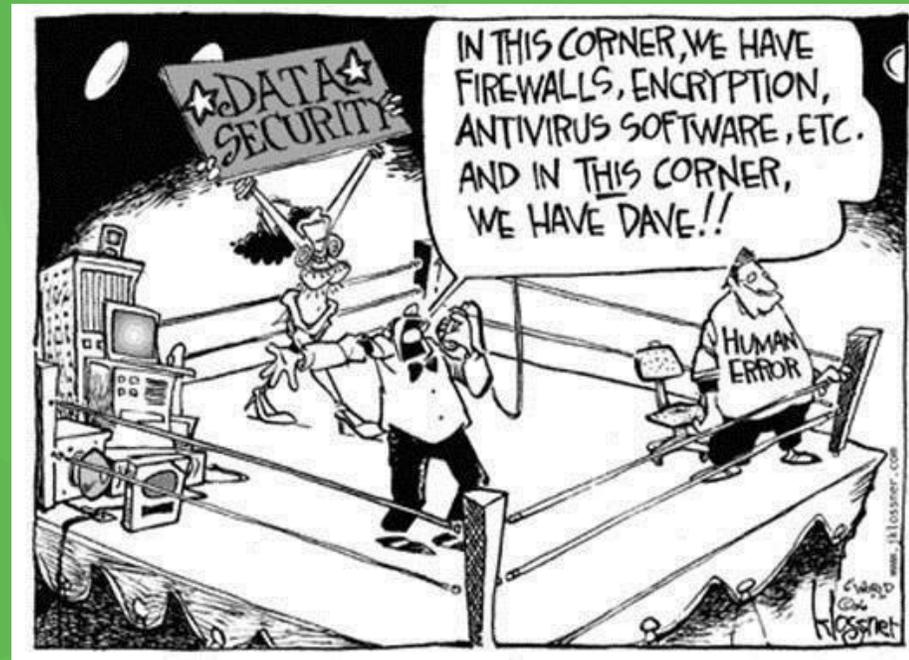


<http://commons.wikimedia.org/wiki/File:EU-EE-Tallinn-Kesklinn-Kassisaba.JPG>



<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
110,799

Groups
248

Countries
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



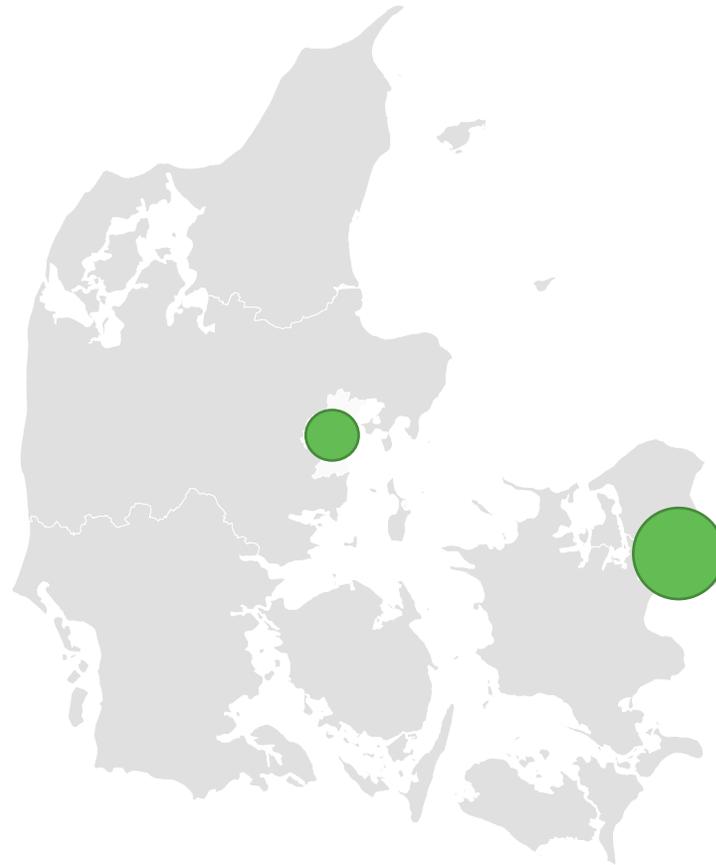
Mikkel Rømer · 1.
Trusec | Cyber Security Expert | SEC699 | eCCPTv2 | DSO I Malware Dev | DSO 2 Adversary Emulation | Sitecore Platform Associate Developer | SC .NET Developer XP 8.0

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. Aalborg
Headhunter/ Nerd/ Happy volunteer in OWASP & BSides
Copenhagen/ Friend of the community
København og omegn · [Kontaktoplysninger](#)

andrada.son@owasp.org

Leveret af Bing
© GeoNames, Microsoft, TomTom

Information Security IndustryScope

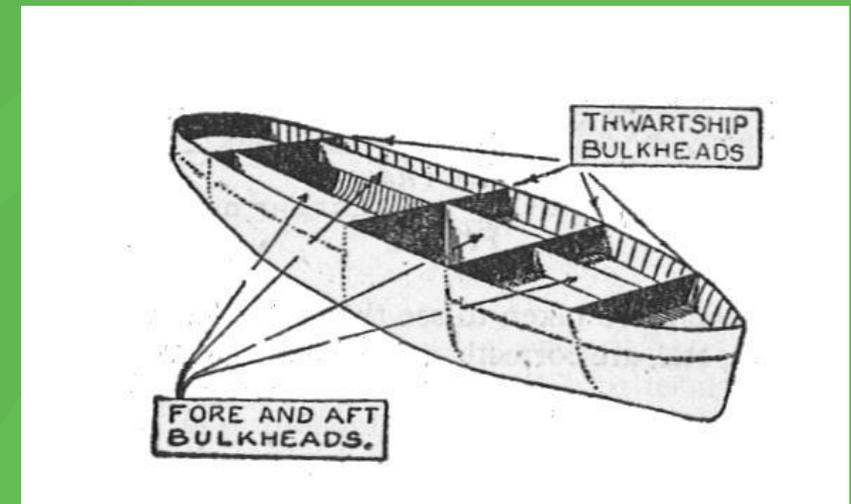
The image displays a comprehensive grid of information security industry logos, organized into 24 distinct panels. Each panel is titled with a specific security domain and contains a variety of company logos representing leading players in that space.

- SECURITY MANAGEMENT AND COMPLIANCE:** Managed Security Service Providers (IBM, at&t, Verizon, Raytheon, HP, NTT, CSC, Symantec), SIEM (HP, BMC, RSA, McAfee, Splunk, TIBCO, LogRhythm, Tenable, NetIQ, etc.), Security Training (SANS, Wombat, SCIPP, etc.), Governance, Risk and Compliance (SAP, IBM, Cymark, etc.).
- ENDPOINT SECURITY:** Secure Email Gateways (SOPHOS, Barracuda, etc.), Data Loss Prevention (Absolute Software, etc.), Endpoint Protection & Anti-virus (SOPHOS, F-Secure, etc.), Endpoint Threat Detection & Response (DTEX, etc.).
- IDENTITY AND ACCESS MANAGEMENT:** User Authentication (HID, EMC, RSA, etc.), Identity Governance and Administration (SAP, etc.).
- INFRASTRUCTURE SECURITY:** Data Masking (IBM, etc.), Enterprise Network Firewalls (Hillstone, Juniper, etc.), Intrusion Prevention Systems (Stonesoft, McAfee, etc.), Network Access Control (Juniper, etc.), Unified Threat Management (Hillstone, etc.).
- APPLICATION SECURITY:** Application Security Testing (Qualium, etc.), Web Application Firewalls (Imperva, etc.), Application Control (Luminate, etc.).
- SECURITY PARTNERS:** A collection of partner logos including UNISYS, FISHER SECURITY, neXum, etc.
- CYBER SECURITY:** Secure Web Gateways (Blue Coat, etc.), Network Forensics (Blue Coat, etc.), Threat Intelligence Services (EMC, RSA, etc.).
- CLOUD SECURITY:** LogCloud, Welsense, etc.
- MOBILE SECURITY:** Mobile Data Protection (Intel, etc.), Mobile Device Management (SAP, etc.).
- SECURITY ORGANIZATIONS:** Education & Academic (IANS, etc.), Professional Associations & Certification (ISC, etc.), Government (NIST, etc.).
- SECURITY CONFERENCES:** Gartner, Blackhat, etc.
- ANALYST HOUSES:** Gartner, etc.

Version 1
November 2014



Breach Containment, Breach Detection, or Assume Breach

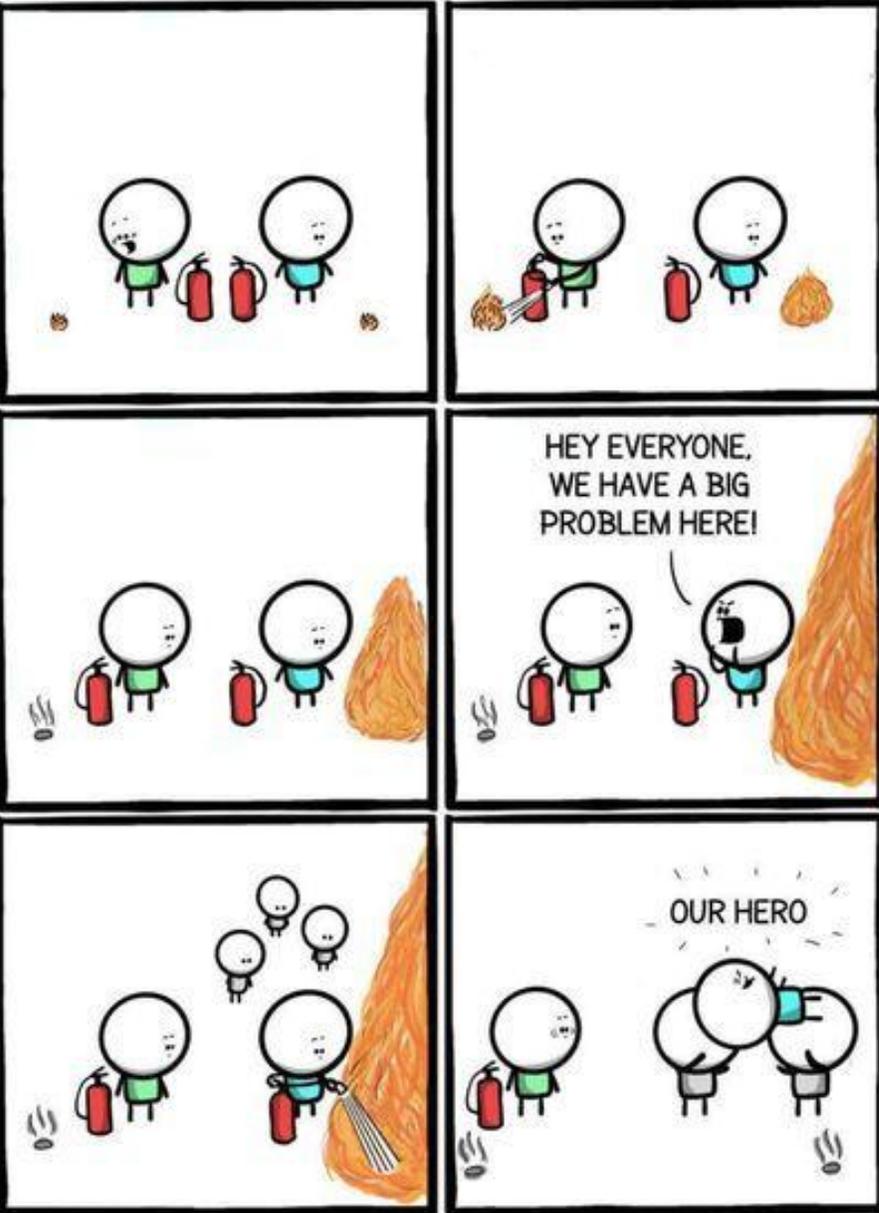




Supply chain attacks

– 3rd party and CI/CD

One person's development is another person's production



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

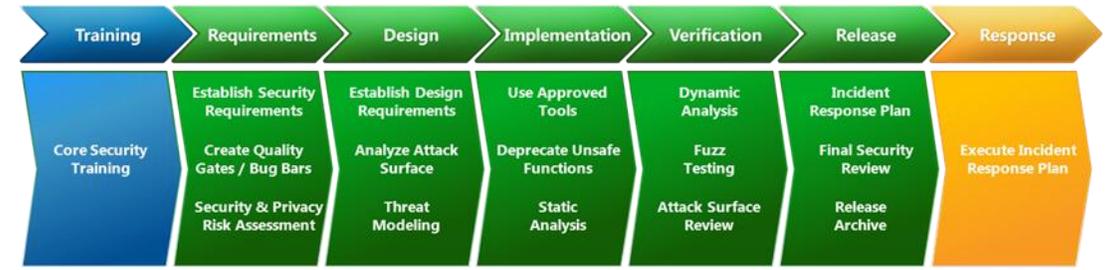
But security uses a different language – often more than one!

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

This is the way!

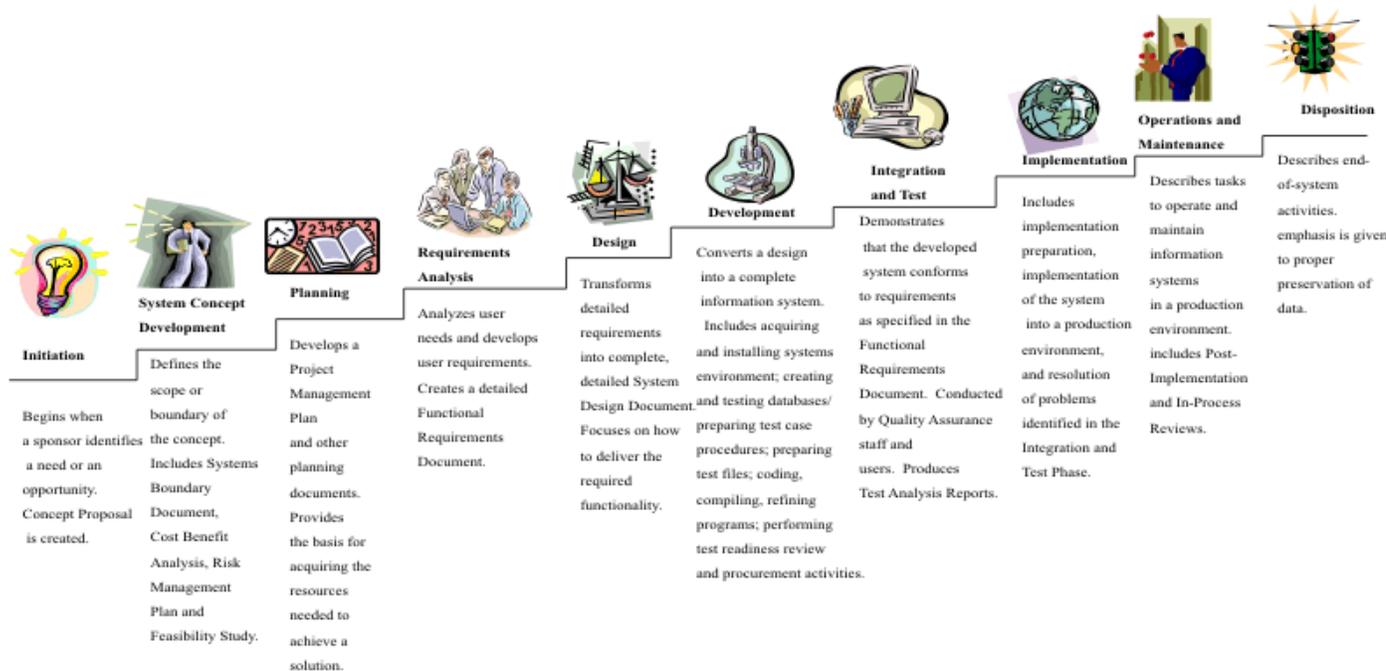
Business functions	Governance	Design	Implementation	Verification	Operations
Practices	Strategy & Metrics Create & promote Measure & improve	Threat Assessment Application risk profile Threat modeling	Secure Build Build process Software dependencies	Architecture Assessment Architecture validation Architecture compliance	Incident Management Incident detection Incident response
	Policy & Compliance Policy & standards Compliance management	Security Requirements Software requirements Supplier security	Secure Deployment Deployment process Secret management	Requirements-driven Testing Control verification Misuse/abuse testing	Environment Management Configuration hardening Patch & update
	Education & Guidance Training & awareness Organization & culture	Secure Architecture Architecture design Technology management	Defect Management Defect tracking Metrics & feedback	Security Testing Scalable baseline Deep understanding	Operational Management Data protection Legacy management
	Stream A Stream B	Stream A Stream B	Stream A Stream B	Stream A Stream B	Stream A Stream B

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

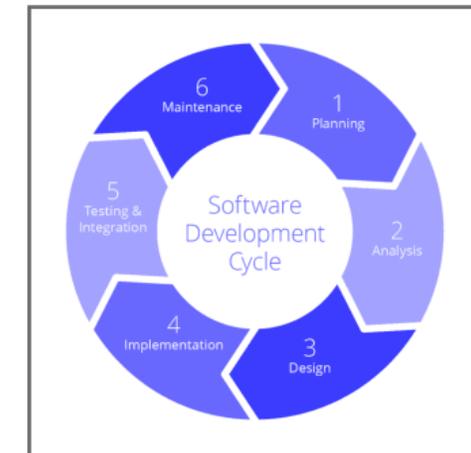


<https://docs.microsoft.com/en-us/windows/security/threat-protection/msft-security-dev-lifecycle>

Systems Development Life Cycle (SDLC) Life-Cycle Phases

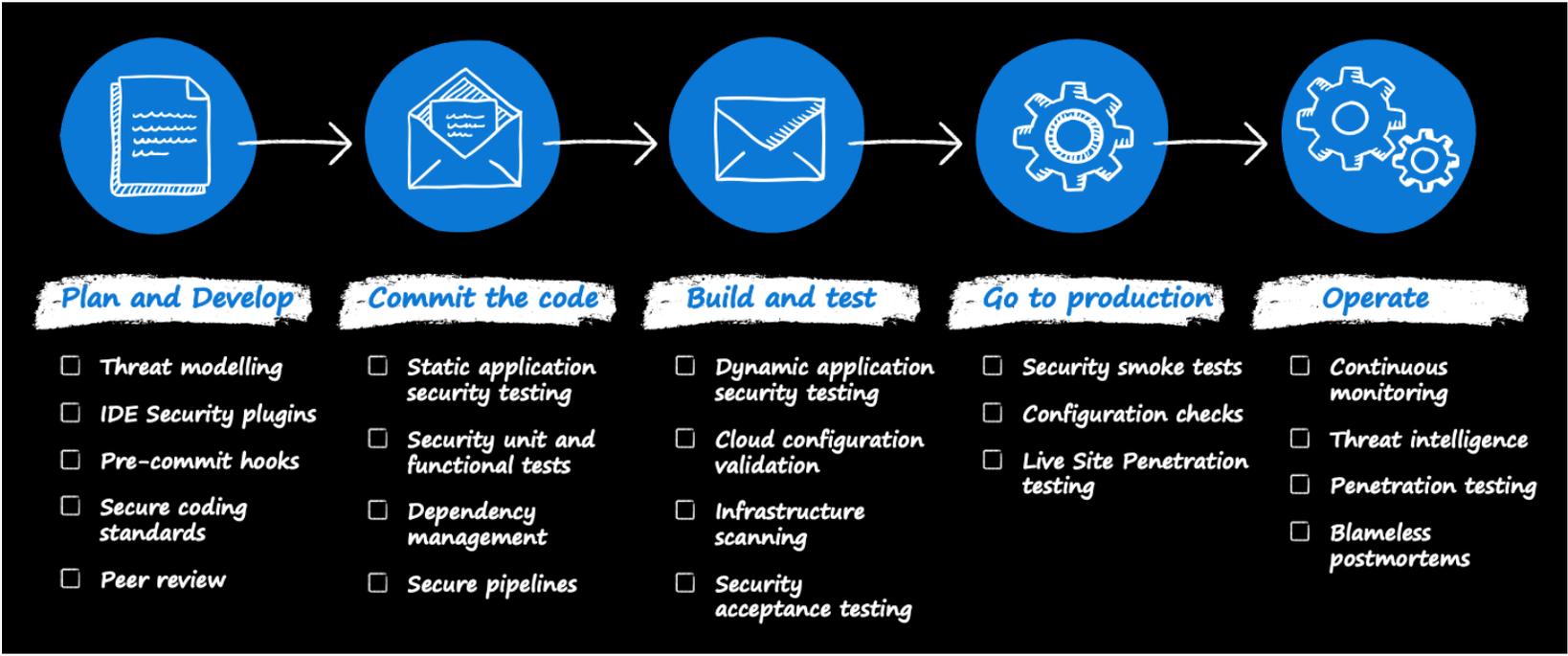
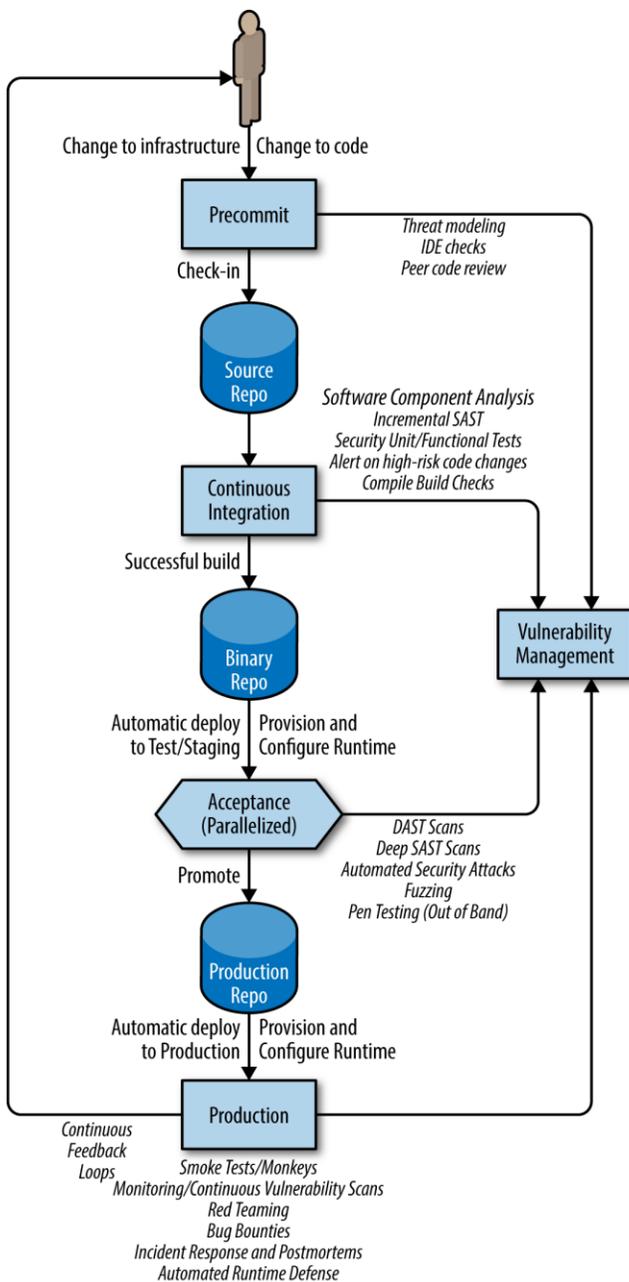


https://en.wikipedia.org/wiki/Systems_development_life_cycle



A typical SDLC representation

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



<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

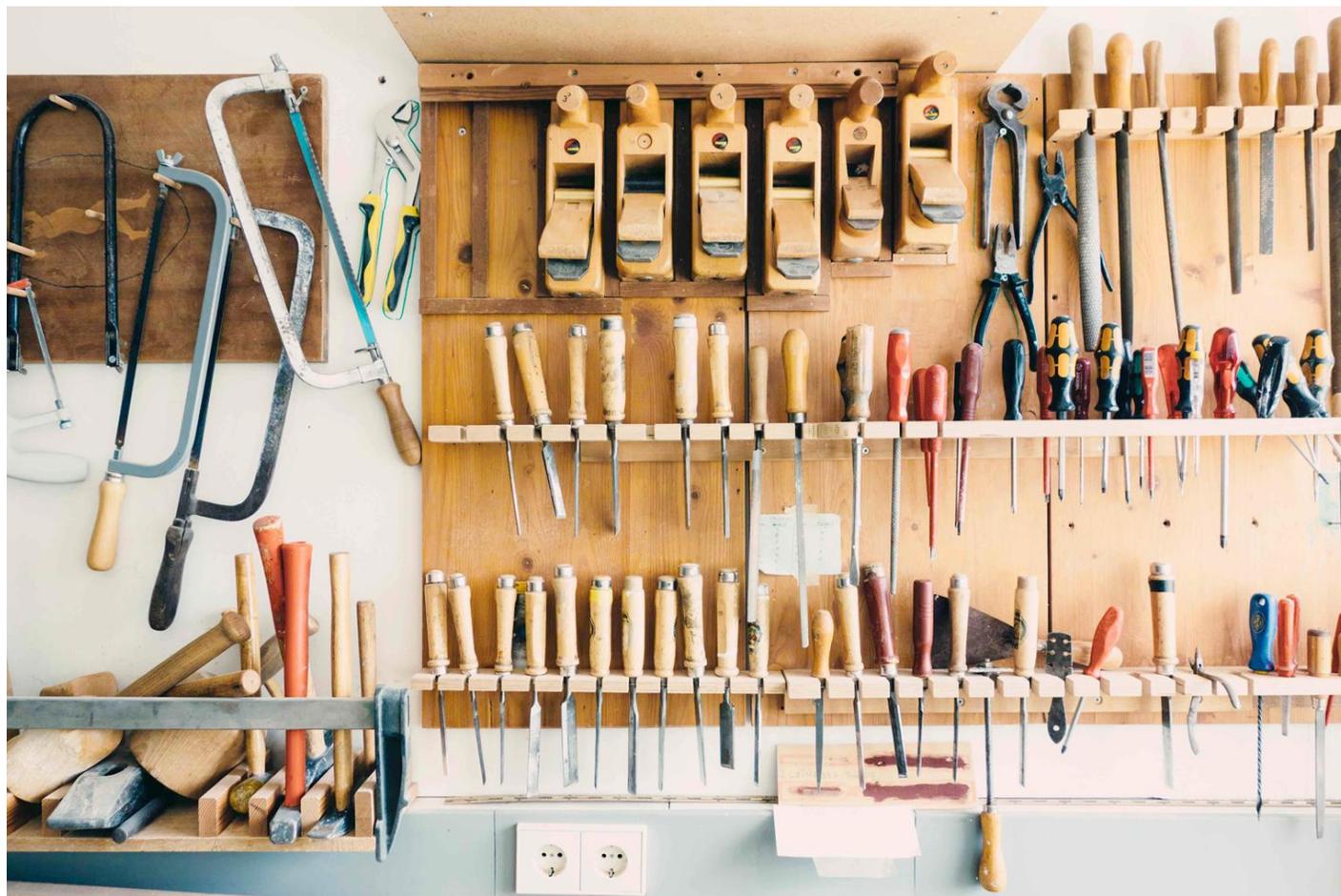
Fuzzing

Pen tests

Secure wrapper libraries

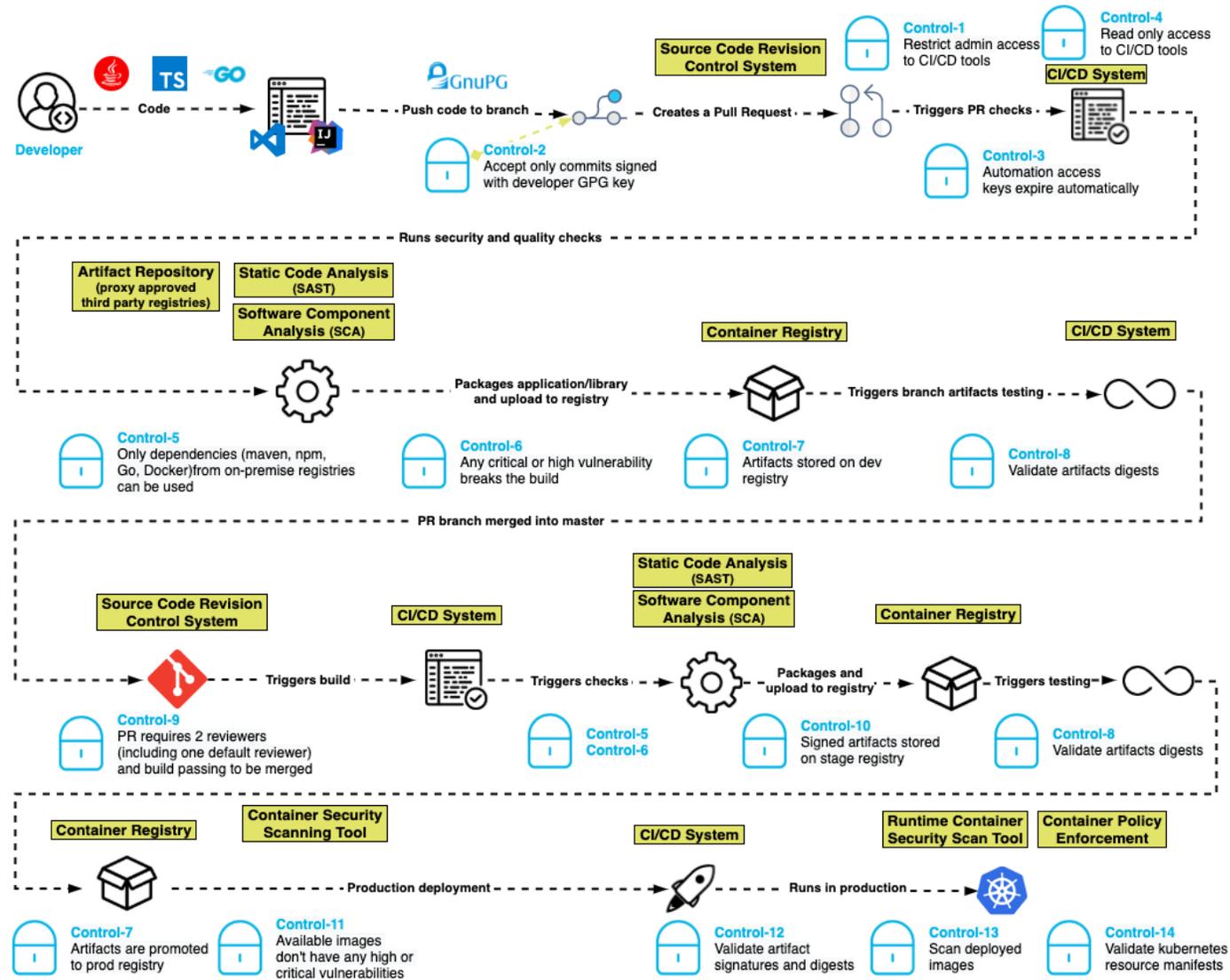
Threat modeling

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/>

Automatisk lagring Secure Controls Framework (SCF) - 2022.1 Søg (Alt+Q)						
File Hjem Indsæt Sidelayout Formler Data Gennemse Vis Hjælp						
E1 Methods To Comply With SCF Controls						
	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: <ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> - ManageEngine AssetExplorer - LANDesk IT Asset Management Suite - ServiceNow (https://www.servicenow.com/) - Solarwinds (https://www.solarwinds.com/) - CrowdStrike 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> - CrowdStrike - JAMF - ITIL - Configuration Management Database (CMDB) 	<ul style="list-style-type: none"> • Does the organization update s • 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.	<ul style="list-style-type: none"> - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - DHCP logging - Active discovery tools - NNT Change Tracker (https://www.newnettechnologies.com/) 	<ul style="list-style-type: none"> • Does the organization use aut • 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.	<ul style="list-style-type: none"> - ITIL - Configuration Management Database (CMDB) - Manual or automated process 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com/) - Tripwire Enterprise (https://www.tripwire.com/products/tripwire- 	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> - Cisco NAC - Aruba Networks - Juniper NAC - Packet Fence - Symantec NAC - Sophos NAC 	<ul style="list-style-type: none"> • Does the organization employ l • technology, that is capable of d • network access to those unaut
	Asset	Dynamic Host Configuration	AST-02.6	Mechanisms exist to enable Dynamic Host Configuration Protocol (DHCP) server logging to improve asset inventories and assist in detecting unknown systems.	<ul style="list-style-type: none"> - Splunk - Manual Process - Build Automation Tools 	<ul style="list-style-type: none"> • Does the organization enable l • server logging to improve asse • systems?

af 72 Automatisk zoom

NIST Special Publication 800-52 Revision 2

Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

Applied Crypto Hardening

- Preface
- I: Introduction
 - Audience
 - Related publications
 - How to read this guide
 - Disclaimer
 - Scope
 - Methods
- II: Best Practice
 - Webservers
 - Apache
 - lighttpd
 - nginx
 - Cherokee
 - MS IIS
 - SSH
 - OpenSSH
 - Cisco ASA
 - Cisco IOS
 - Mailservers
 - TLS usage in mail server protocols
 - Recommended configuration

https://bettercrypto.org

Applied Crypto Hardening: bettercrypto.org

Wolfgang Breyha, David Durvaux, Tobias Dussa, L. Aaron Kaplan, Florian Mendel, Christian Mock, Manuel Koschuch, Kriegisch, Ulrich Pöschl, Ramin Sabet, Berg San, Ralf Schlatterbeck, Thomas Schreck, Alexander Würstlein, Aaron Zawodsky
– Version 1.x, 2018-12-21 | The Asciidoc Edition

Preface

Do not talk unencrypted



https://owasp.org/www-project-secure-headers/

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

OWASP PROJECTS CHAPTERS EVENTS ABOUT Search OWASP

OWASP Secure Headers Project

Main Response Headers Compatibility Matrix Technical Resources Top Websites Examples
Best Practices Miscellaneous Case Studies

`click_validity_of_all_external_links` passing

The OWASP Secure Headers Project (also called OSHP) describes HTTP response headers that you can use to increase the security of your application. Once set, these HTTP response headers can help protect your users from running into easily preventable vulnerabilities. The OWASP Secure Headers Project helps raise awareness and use of these headers.

These headers are well-known and also despised. Seeking a balance between usability and security, developers can use these headers to increase application quality through the headers that can make applications more versatile or secure. But in practice

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

Ultimate DevSecOps library

Contribution rules

If you want to contribute to this library of knowledge, you are adding following these set of rules:

Tooning

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/Hillsong/git-hound	Searchers secrets in git	
goSDL	https://github.com/slackhq/goSDL	Security Development Lifecycle checklist	
	https://oithub.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

- Angular
- Ansible
- Azure Resource Manager
- Bitbucket
- Build tools
- CSS/SASS/SCSS
- Config Files
- Configuration Management
- Containers
- Continuous Integration
- Demo
- Embedded
- Embedded Ruby (a.k.a. ERB, erbuby)
- Checkin
- HTML
- JSON

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

Developer	Secrets Management	CI/CD Server	QA/Staging	Production	Monitoring
<ul style="list-style-type: none"> • Pre-commit Hooks • IDE Plugins • Linters 	<ul style="list-style-type: none"> • Token based secret management service 	<ul style="list-style-type: none"> • Static Application Security Testing(SAST) • Software Composition Analysis(SCA) 	<ul style="list-style-type: none"> • Dynamic Application Security Testing(DAST) • Vulnerability Management 	<ul style="list-style-type: none"> • Compliance as Code • Security in IaC • Vulnerability Assessment • Manual Pentesting • Business Logic Flaws 	<ul style="list-style-type: none"> • Alerting and monitor the deployed instance for Vulnerability OWASP Top 10

Source : NotSoSecure

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

Static Application Security Testing (SAST)

ALL TIERS

All open source (OSS) analyzers were n

The whitepaper "A Seismic S application based. Download

If you're using GitLab CI/CD, you ca for known vulnerabilities. You can r 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/

Source Code Analysis Tools

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

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

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

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

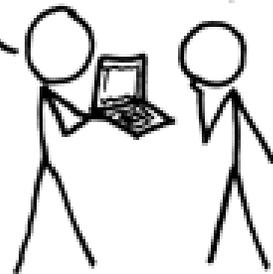


A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

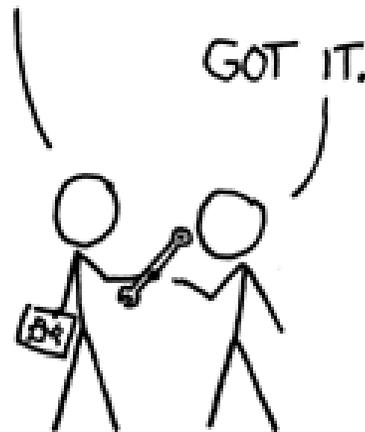
NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!

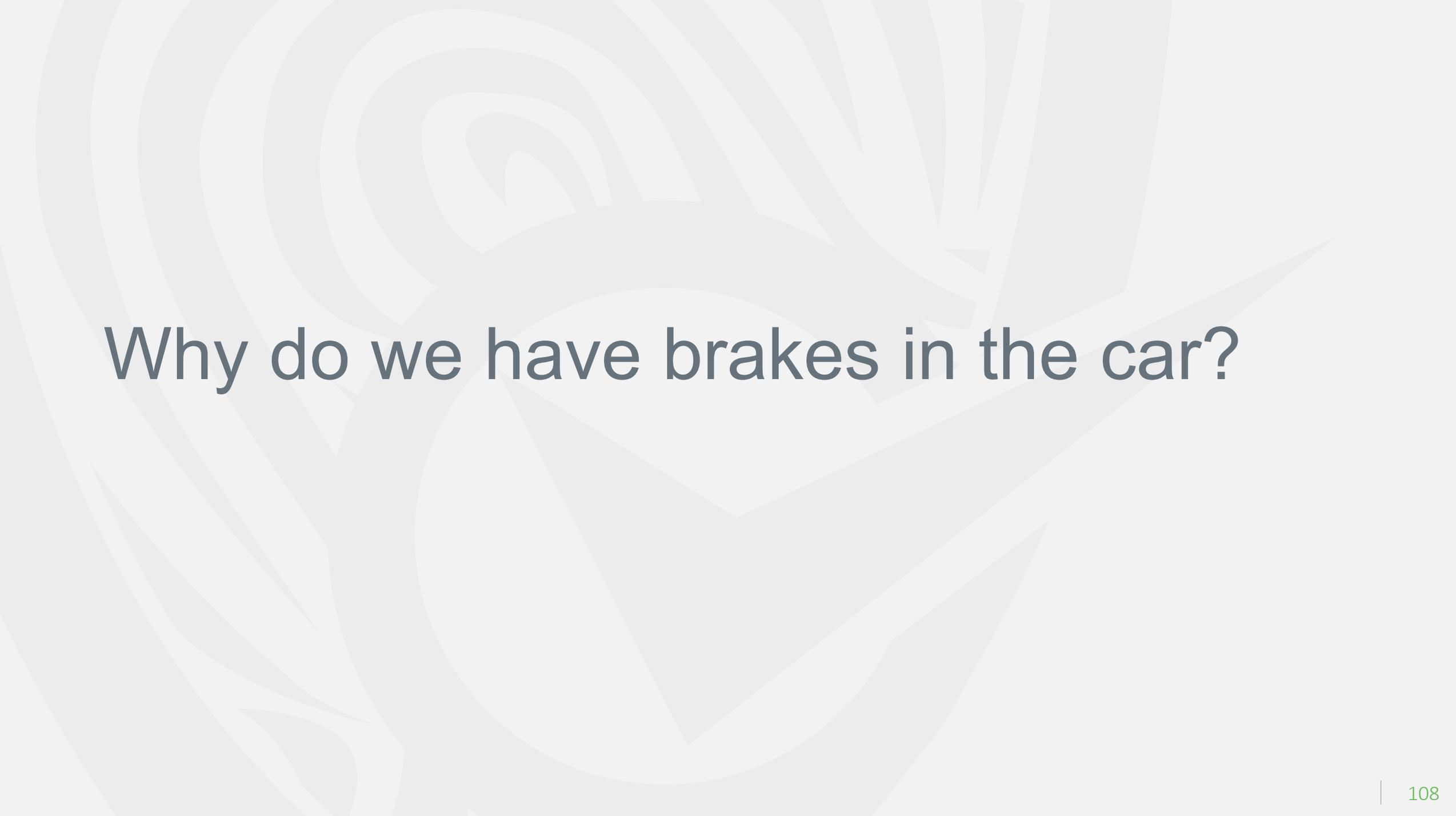


WHAT WOULD
ACTUALLY HAPPEN:

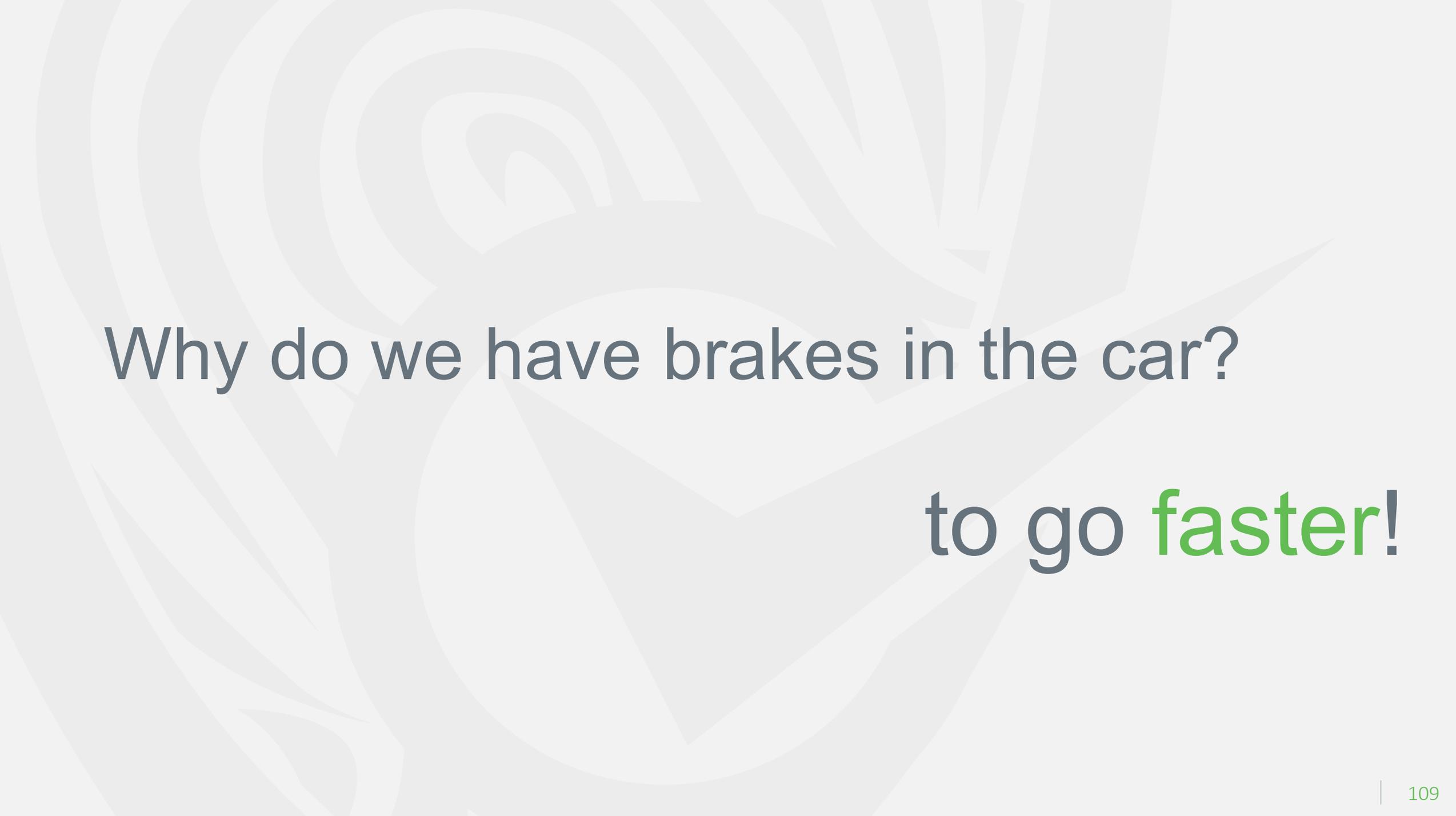
HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.



GOT IT.



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

[t](#) [f](#) [in](#)