Experts Live Norway

Securing Windows in 2019 and Forward

Sami Laiho

Senior Technical Fellow, MVP

@samilaiho

Sami Laiho

Senior Technical Fellow
adminize.com / Sulava

- IT Admin since 1996 / MCT since 2001
- MVP in Windows OS since 2011
- Specializes in and trains:
  - Troubleshooting, Windows Internals
  - Security, Social Engineering, Auditing
  - Centralized Management, Active Directory
- Trophies:
  - Ignite 2018 – Session #1 and #2 (out of 1708) !
  - Best Speaker at NIC, Oslo 2016, 2017 and 2019
  - Best External Speaker at Ignite 2017
  - TechDays Sweden 2016, 2018 – Best Speaker
  - TechEd Europe and North America 2014 - Best session, Best speaker
  - TechEd Australia 2013 - Best session, Best speaker
  - TechEd Europe 2013 - Best Session by an external speaker

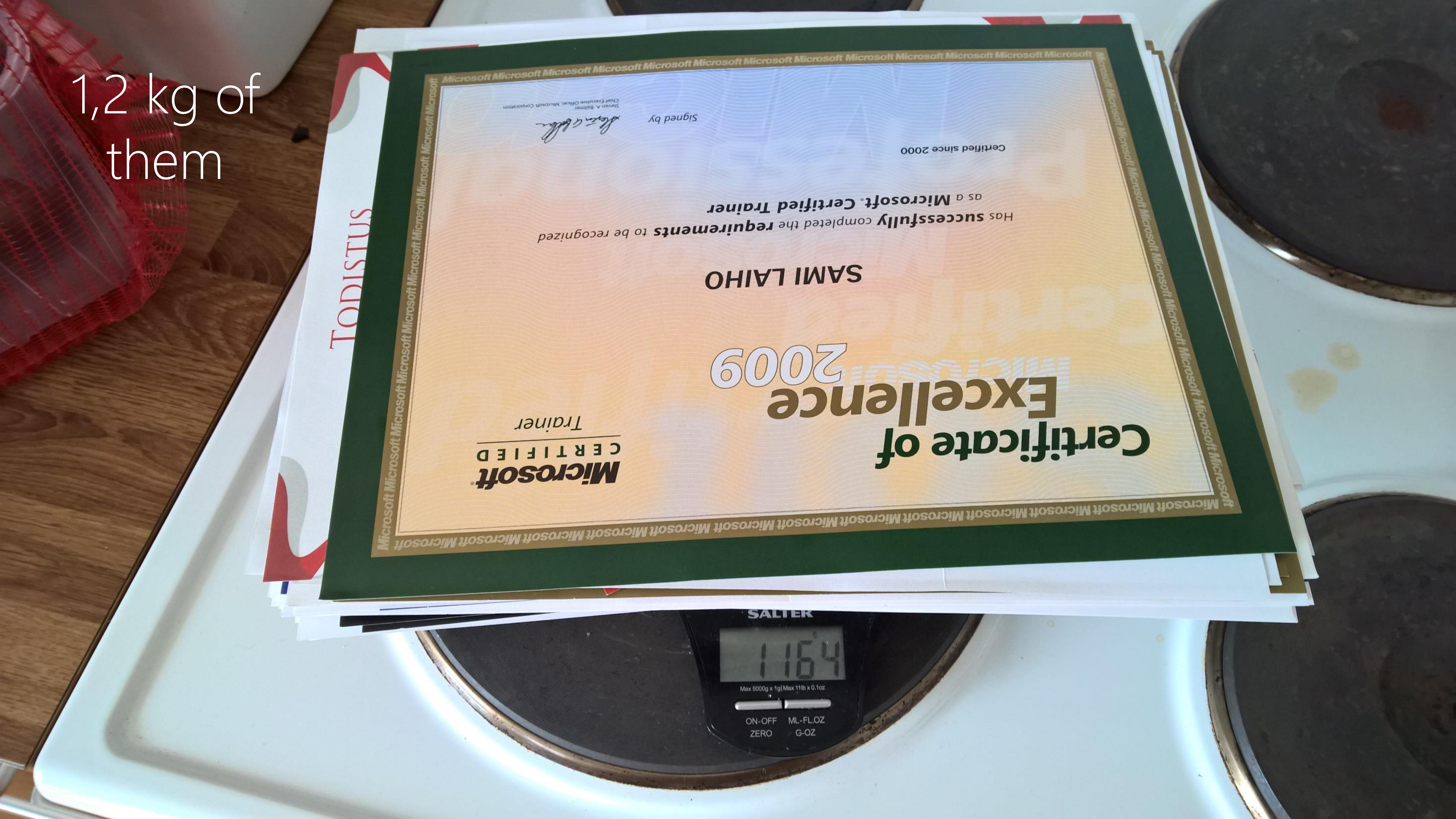
I got Certs

Microsoft Certified Trainer
Regional Lead
Certificate of Appreciation

In recognition of your leadership and service as a Microsoft Certified Trainer - Regional Lead in Finland. Thank you Sami Laiho for your participation in the Regional Lead Program.

Microsoft Certified Trainer Program Manager

1,2 kg of them



Certificate of Excellence 2009

SAMI LAIHO

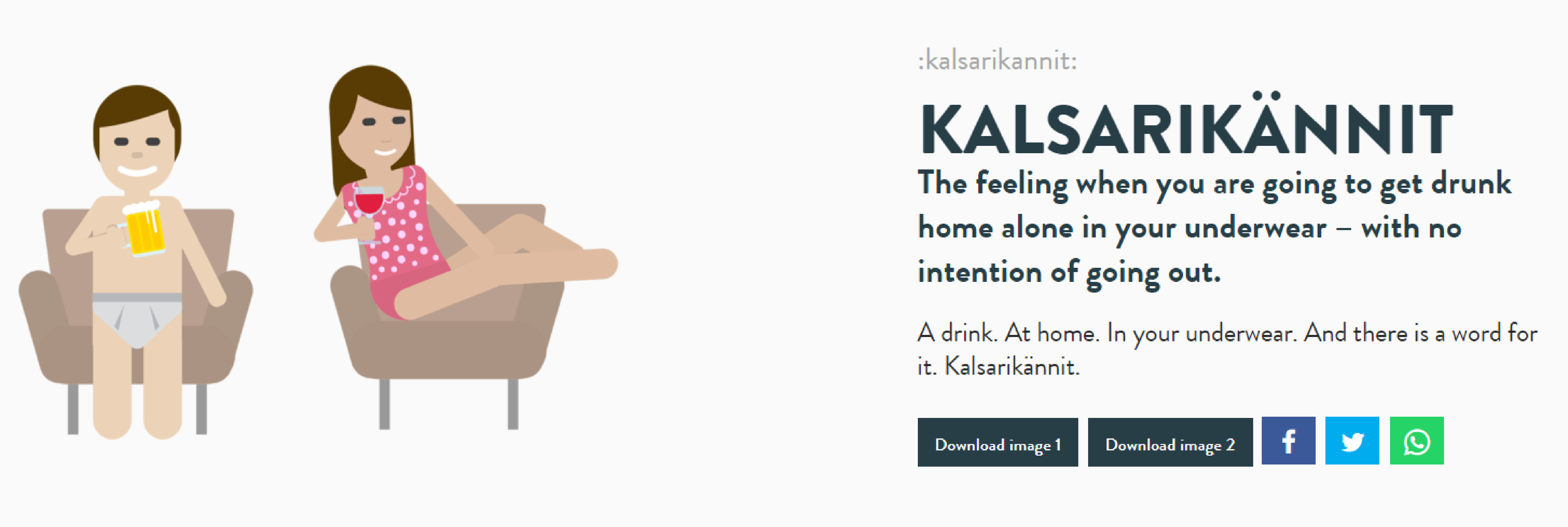
Has **successfully** completed the **requirements** to be recognized as a **Microsoft. Certified Trainer**

Certified since 2000

Signed by

Steven A. Ballmer
Chief Executive Officer, Microsoft Corporation

Microsoft CERTIFIED Trainer

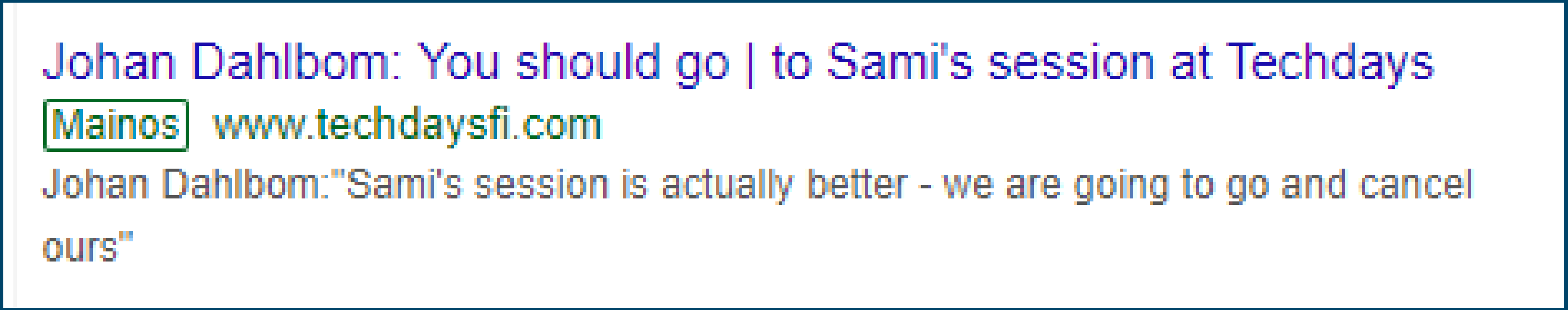


:kalsarikannit:

KALSARIKÄNNIT

The feeling when you are going to get drunk home alone in your underwear – with no intention of going out.

A drink. At home. In your underwear. And there is a word for it. Kalsarikännit.



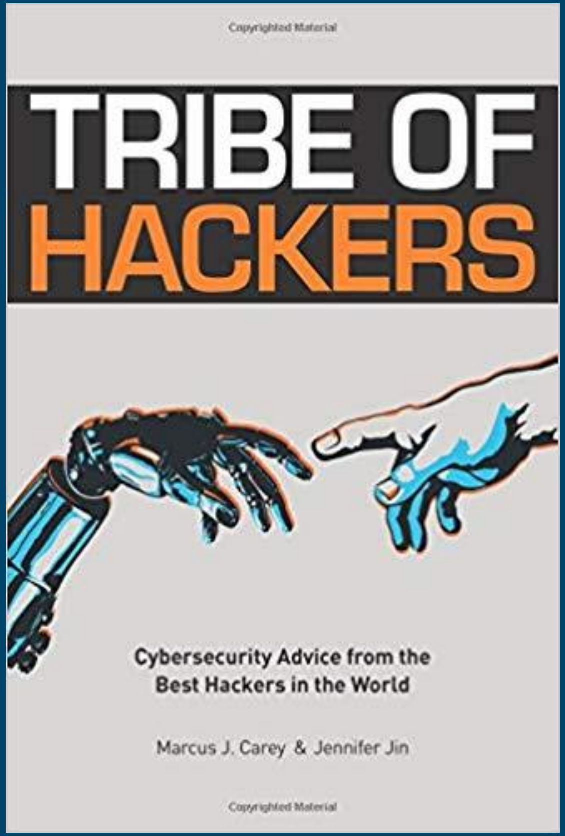
Johan Dahlbom: You should go | to Sami's session at Techdays

Mainos www.techdaysfi.com

Johan Dahlbom:"Sami's session is actually better - we are going to go and cancel ours"

@samilaiho

If you are not on Twitter – get on Twitter!


Copyrighted Material

TRIBE OF HACKERS

Cybersecurity Advice from the Best Hackers in the World

Marcus J. Carey & Jennifer Jin

Copyrighted Material

70 Best hackers in the world invited (#36)

- Super proud to be included in this book
- All profits go to charity!
- https://www.amazon.com/Tribe-Hackers-Cybersecurity-Advice-World/dp/1793464189

Gartner, NIST and others

- Say that the most important security feature to implement in 2018 was Whitelisting
- 2017 and 2016 it has been the Principle of Least Privilege

2019 by Gartner

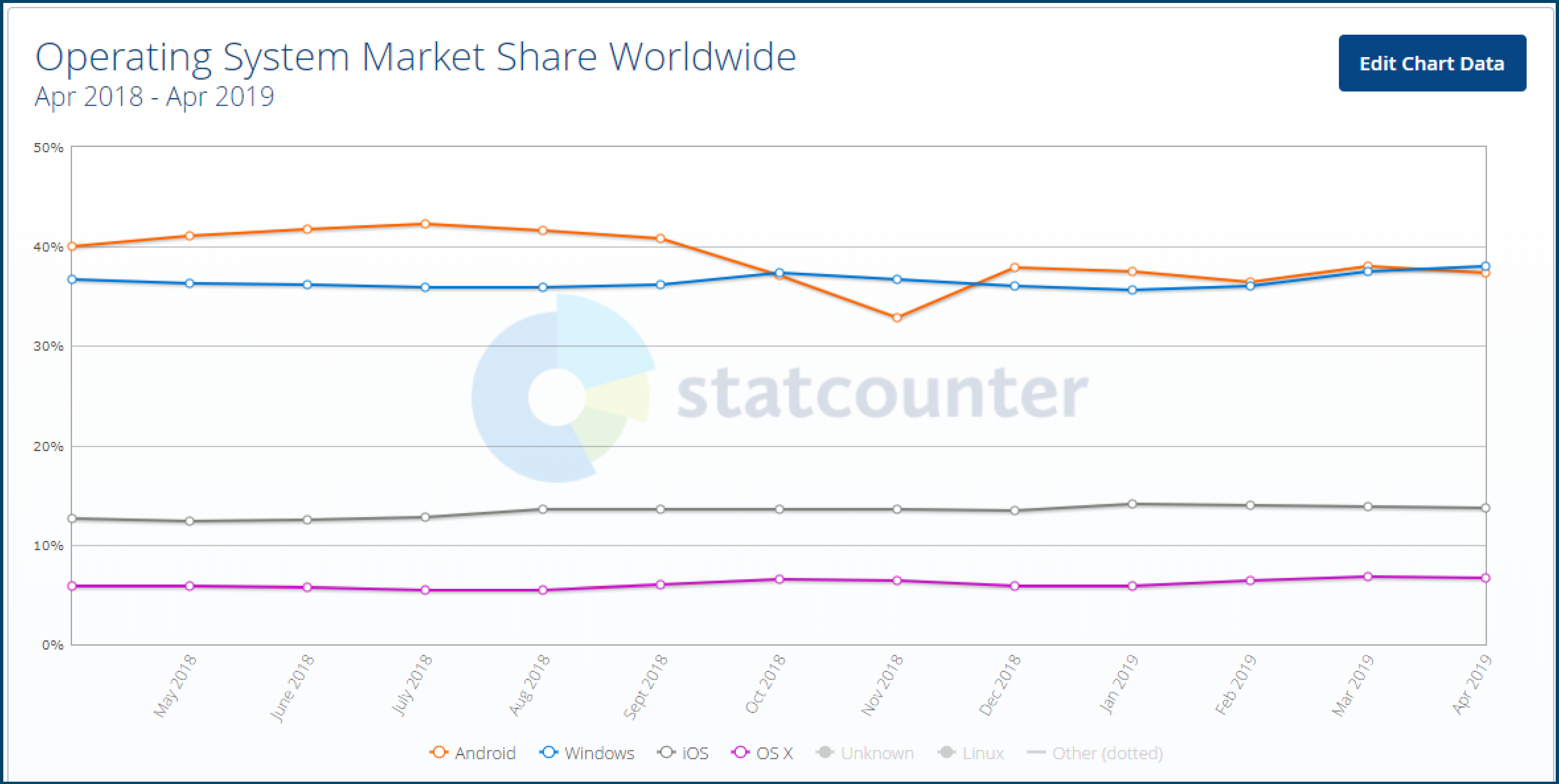
- “Logging and **monitoring of privileged activity**
- “**Discovery and visibility are key** because it’s increasingly important to know which data is where, and to get deep insight into how users and machines access various applications and data sources.”
- “From a process perspective, **undertake ongoing Incident Response planning activities**.
- “Security teams are aware that they need to **act as business enablers**, but still often remain excluded from the start of a project.”

2019 by Gartner

- Log and Monitor Admins
- Correct Categorization of Data
- Train Response
- Include Security into Every Project from the start

2019 will be another year of giant breaches

2019 will be a year of Malware on Mobiles



Operating System Market Share Worldwide

Apr 2018 - Apr 2019

Malicious Actors aim for Quick Monetization

RansomWare and CryptoMiners

Security Basics

Basics are the same

- Every device needs BitLocker or other Full Volume Encryption (or equal physical security)
- Principle of Least Privilege is required to have security at all

No BitLocker?

No more Sticky Keys demo???!!!

Excessive Privileges - DEMO

Threats and Mitigations

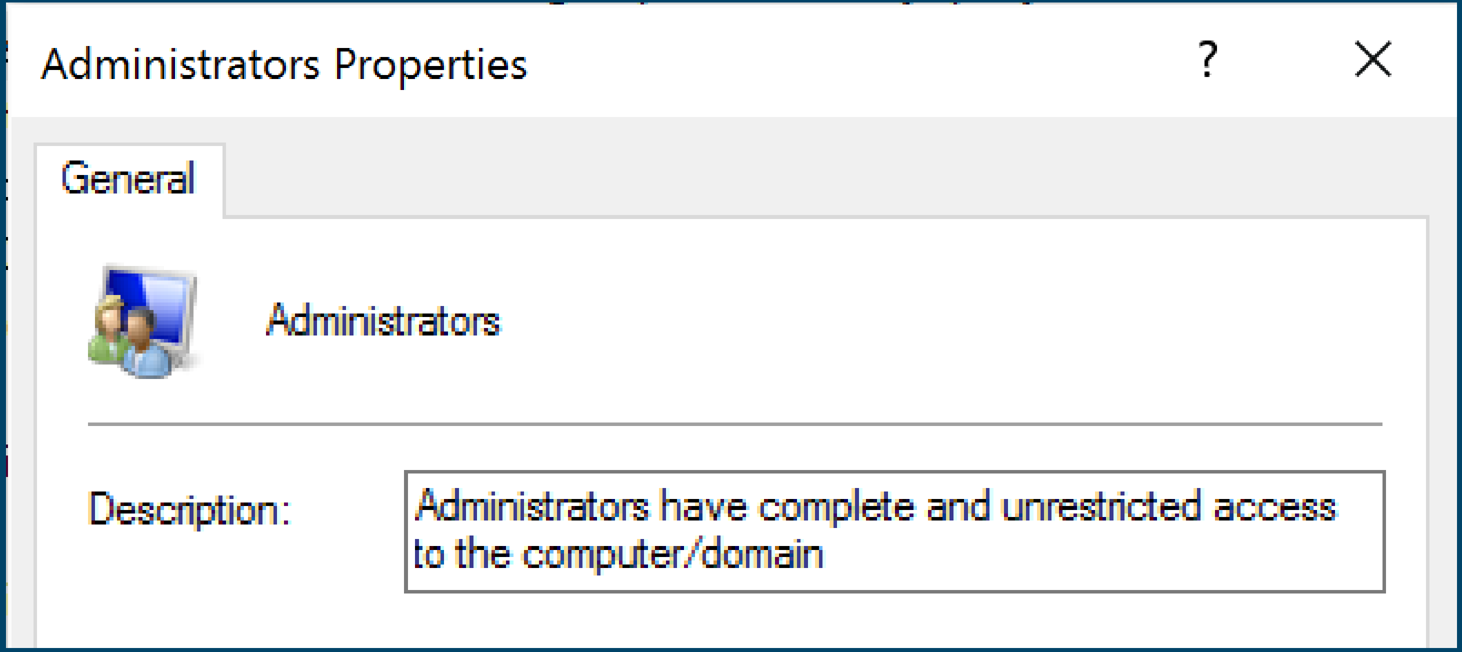
Traditional Viruses/Worms/Malware

Numbers not growing anymore like for some years

Mitigating Traditional Malware →Principle of Least Privilege (and Whitelisting)

NT 3.1 Security Guide

- States that local admins have full access to computer.
- It also says: ”in Windows there is no security if you run as admin”



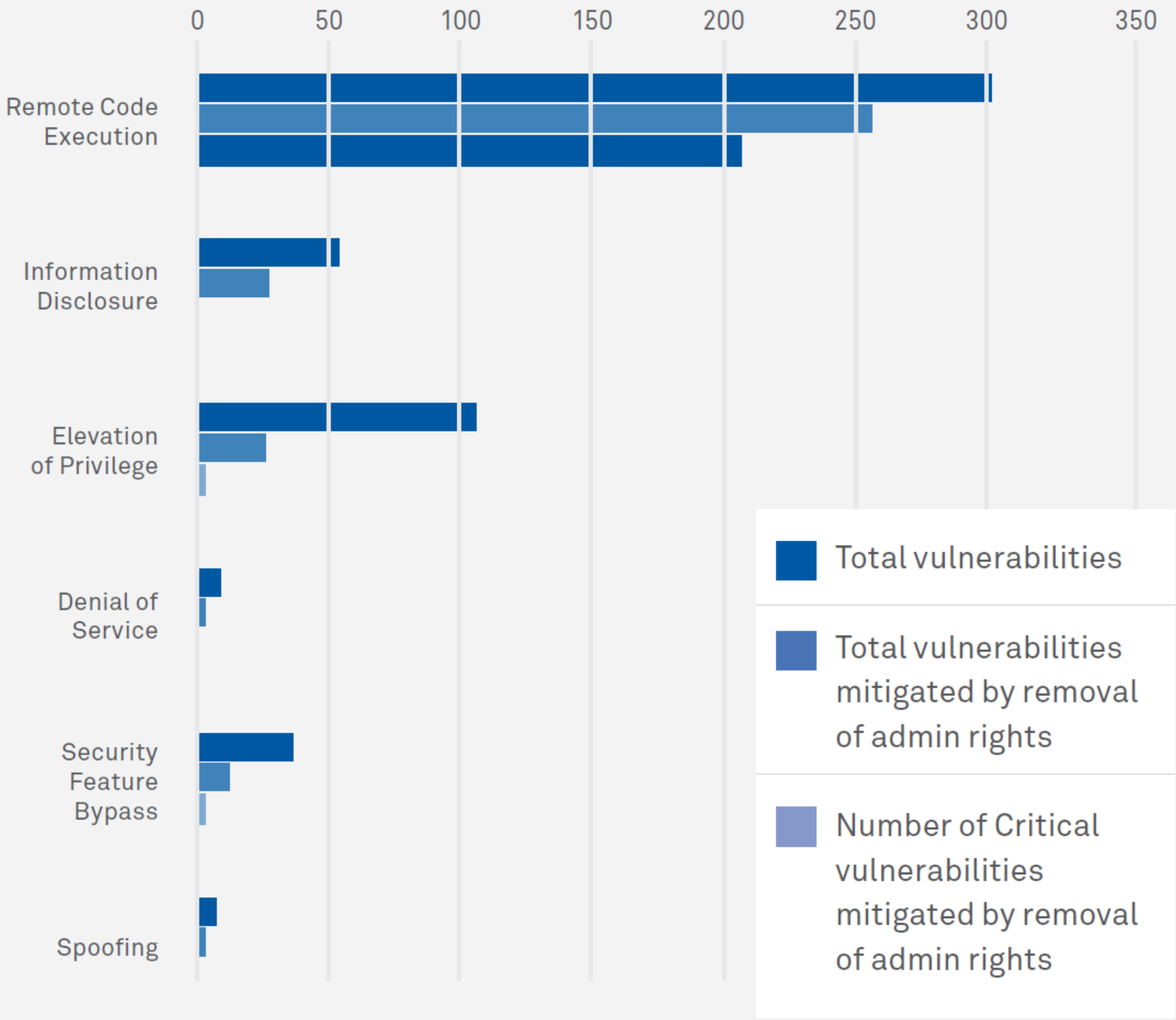
Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

2015

- Analysis of Microsoft "Patch Tuesday" Security Bulletins from 2015
  - 85% of Critical Microsoft vulnerabilities would be mitigated by removing admin rights
  - 52% increase in the total volume of vulnerabilities compared to 2014
- Windows Server vulnerabilities
  - 429 vulnerabilities (304 in 2014)
  - 85% were found to be mitigated by the removal of admin rights

Breakdown of Microsoft Vulnerability Categories in 2015



2016 Microsoft Vulnerabilities Study

Key findings

- Of the 189 vulnerabilities in 2016 with a Critical rating, 94% were concluded to be mitigated by removing administrator rights
- 100% of vulnerabilities impacting Microsoft's latest browser Edge could be mitigated
- 100% of vulnerabilities in IE and Chrome could be mitigated by removing admin rights
- 99% of vulnerabilities affecting Microsoft Office could be mitigated by removing admin rights

Microsoft Vulnerabilities Report 2017

The 2017 report highlights the following key findings:

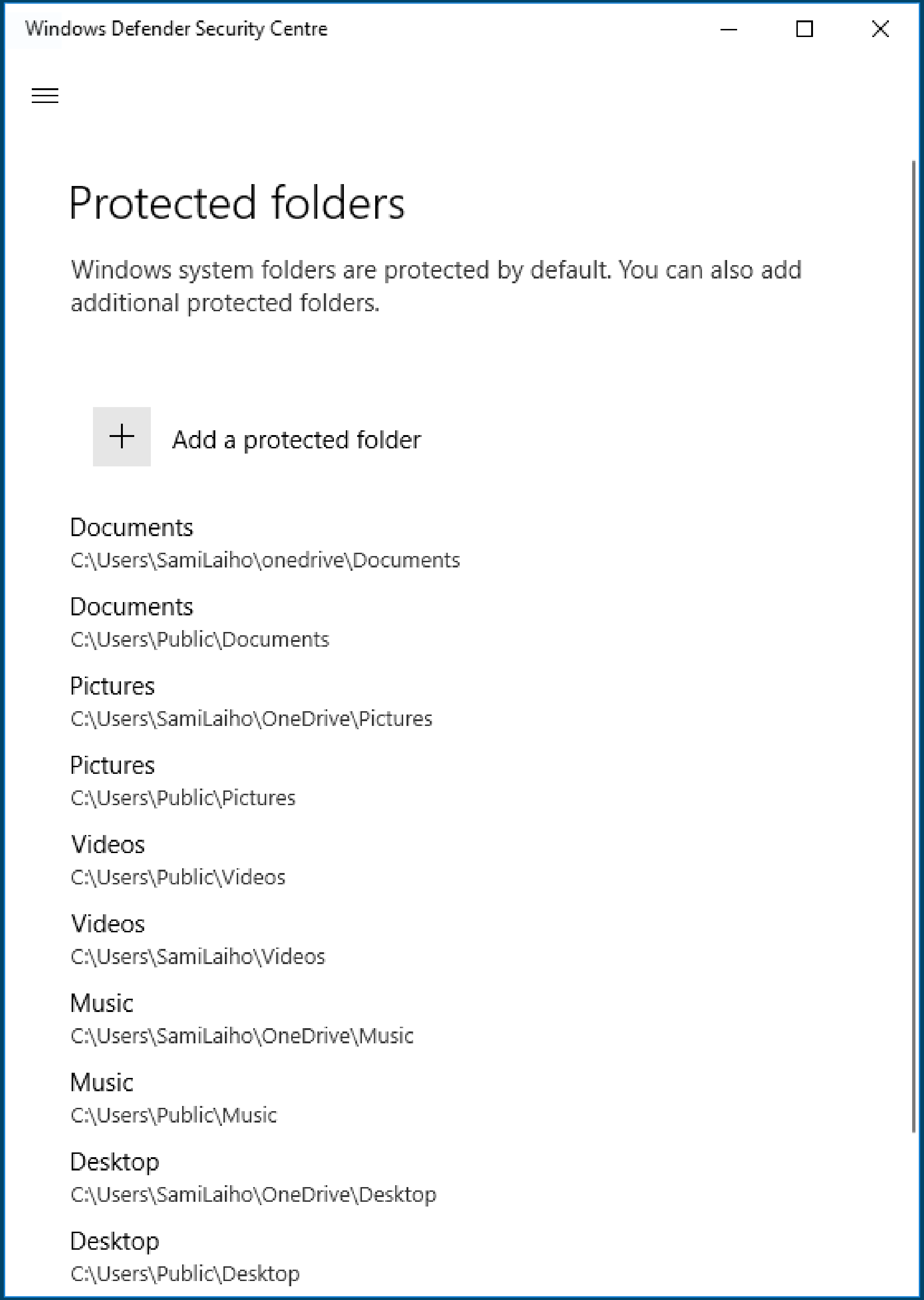
- Removing admin rights would mitigate 80% of all Critical Microsoft vulnerabilities in 2017.
- 95% of Critical vulnerabilities in Microsoft browsers can be mitigated by removing administrator rights.
- **88% of all Critical vulnerabilities reported by Microsoft over the last five years would have been mitigated by removing admin rights.**

Demo: Shit-O-Meter

RansomWare

People need access to their data…

Mitigating RansomWare →Whitelisting and Protected Folders



Protected folders

Windows system folders are protected by default. You can also add additional protected folders.

Documents
C:\Users\SamiLaiho\onedrive\Documents

Documents
C:\Users\Public\Documents

Pictures
C:\Users\SamiLaiho\OneDrive\Pictures

Pictures
C:\Users\Public\Pictures

Videos
C:\Users\Public\Videos

Videos
C:\Users\SamiLaiho\Videos

Music
C:\Users\SamiLaiho\OneDrive\Music

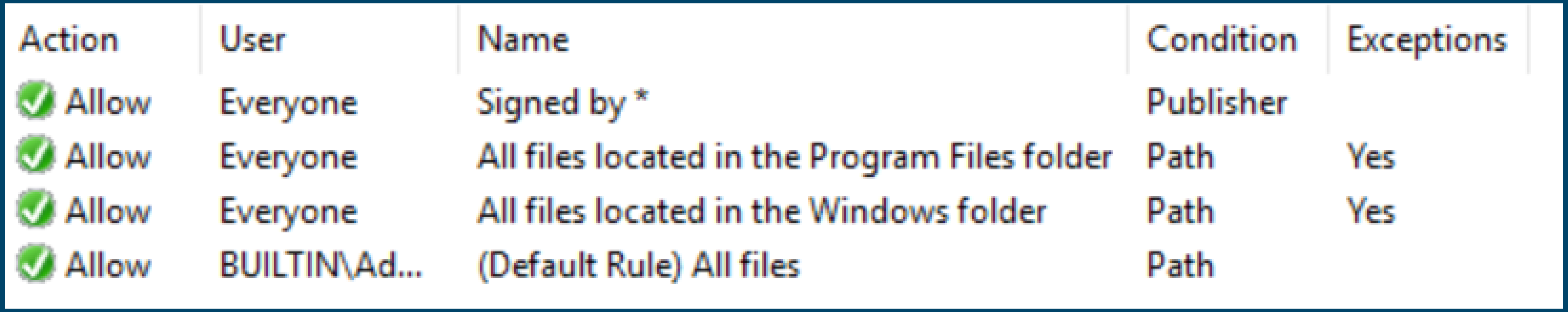
Music
C:\Users\Public\Music

Desktop
C:\Users\SamiLaiho\OneDrive\Desktop

Desktop
C:\Users\Public\Desktop

AppLocker can be simple

- As long as you don’t have admin-rights



Action	User	Name	Condition	Exceptions
✓ Allow	Everyone	Signed by *	Publisher	
✓ Allow	Everyone	All files located in the Program Files folder	Path	Yes
✓ Allow	Everyone	All files located in the Windows folder	Path	Yes
✓ Allow	BUILTIN\Ad...	(Default Rule) All files	Path	

Signing

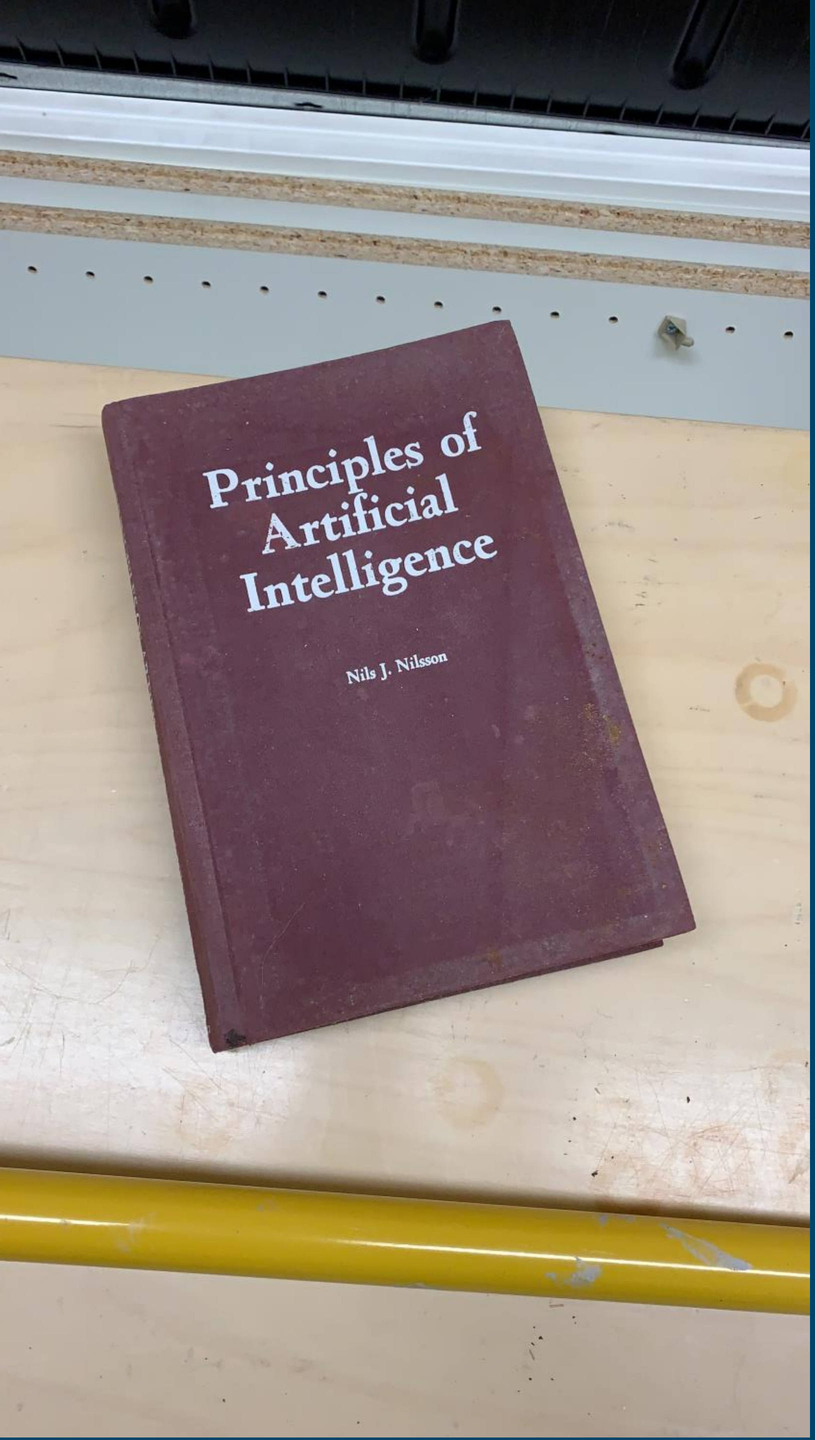
- Require signing for everything
  - Code
  - Scripts

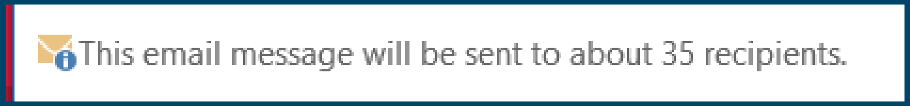
Developers - RTFM

https://docs.microsoft.com/fi-fi/windows/desktop/win_cert/certification-requirements-for-windows-desktop-apps

CryptoMiners

Mitigating CryptoMiners → Whitelisting and maybe some AI…

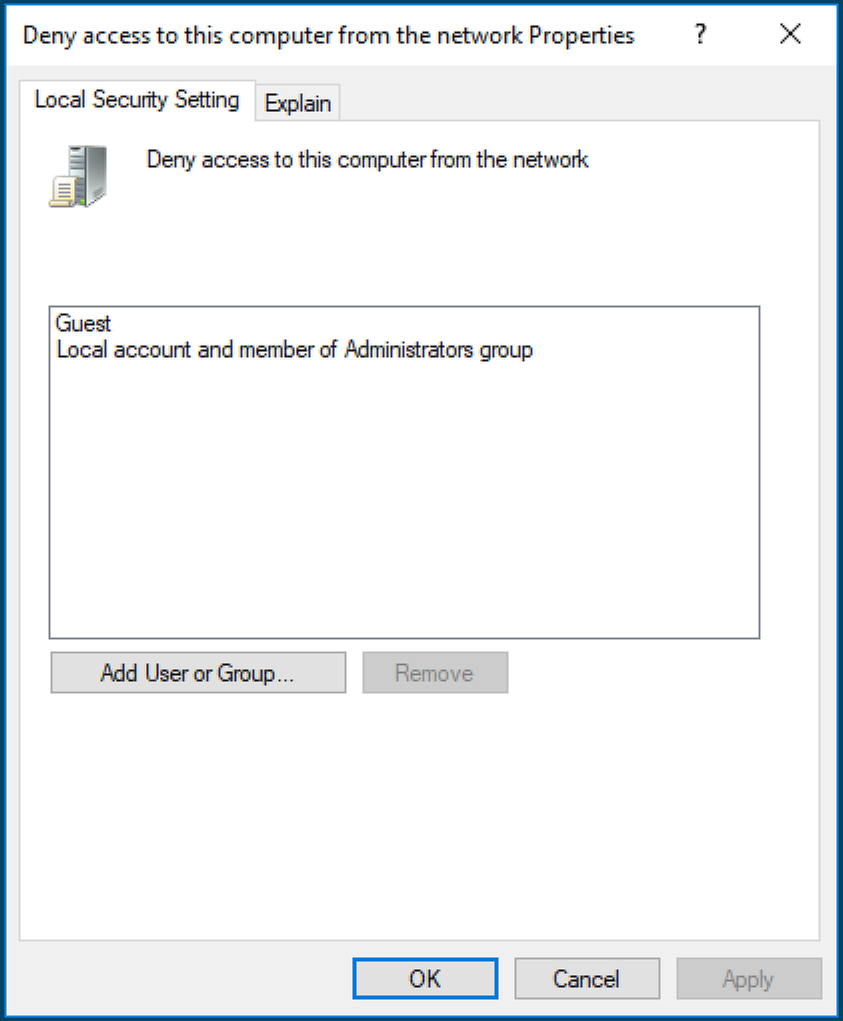



This email message will be sent to about 35 recipients.

Lateral Movement

Pass the Hash, Poisoned Endpoints etc.

Quickfix



Deny access to this computer from the network Properties

Deny access to this computer from the network

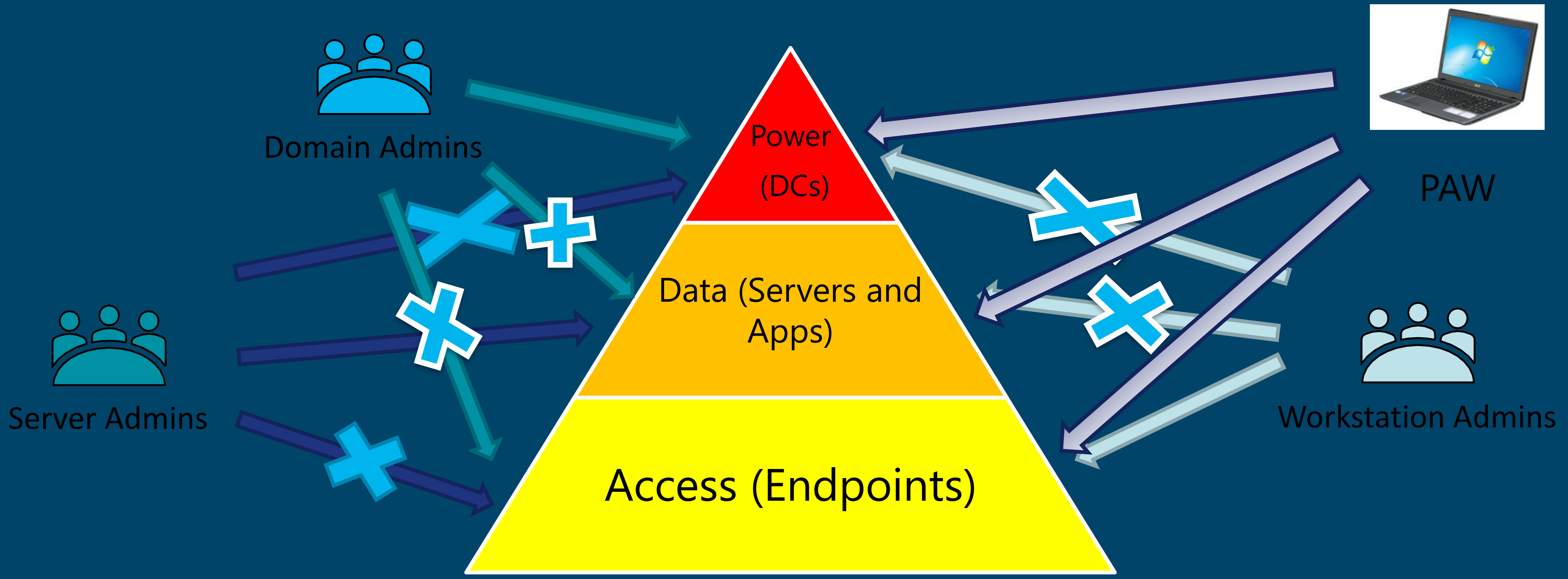
Guest
Local account and member of Administrators group

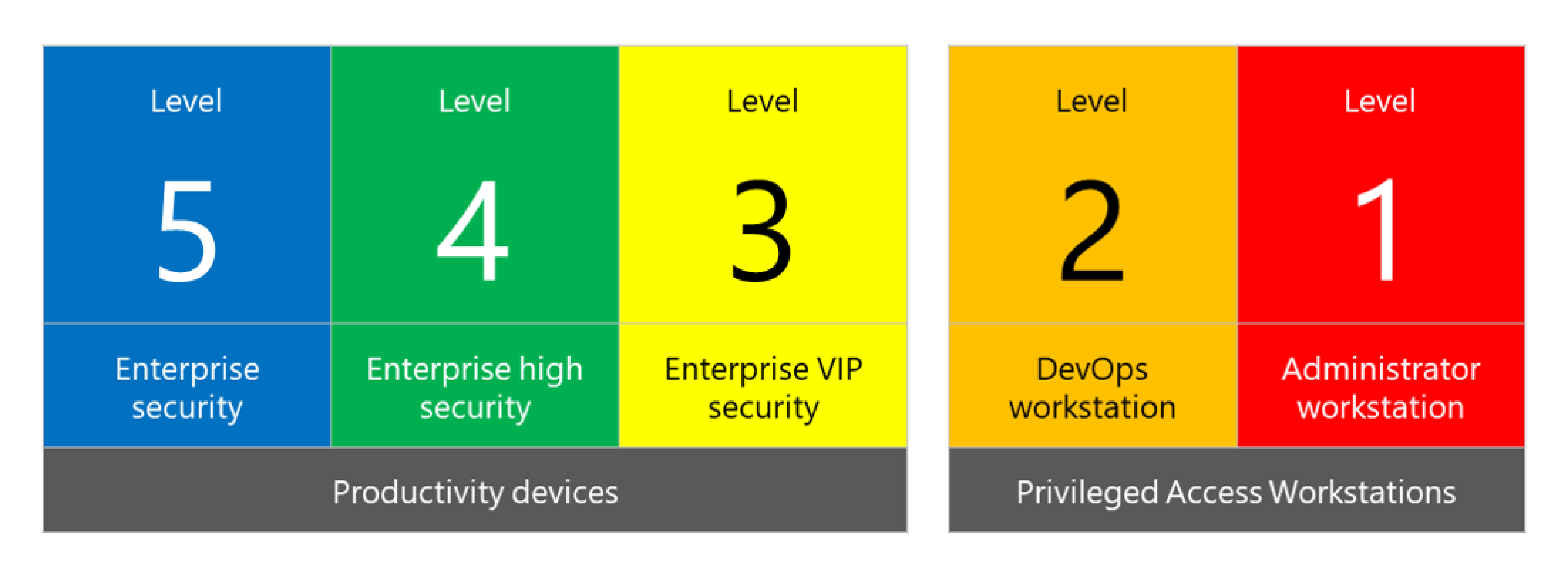
Better

- Deploy LAPS
- Deploy Credential Guard
  - Requires Enterprise

PtH mitigation – CONCEPT!

- Divide the environment to at least three layers/tiers (Azure minimum two)
- Don’t allow upper layer admins to log on to lower layers





Level 5	Level 4	Level 3	Level 2	Level 1
Enterprise security	Enterprise high security	Enterprise VIP security	DevOps workstation	Administrator workstation
Productivity devices			Privileged Access Workstations	

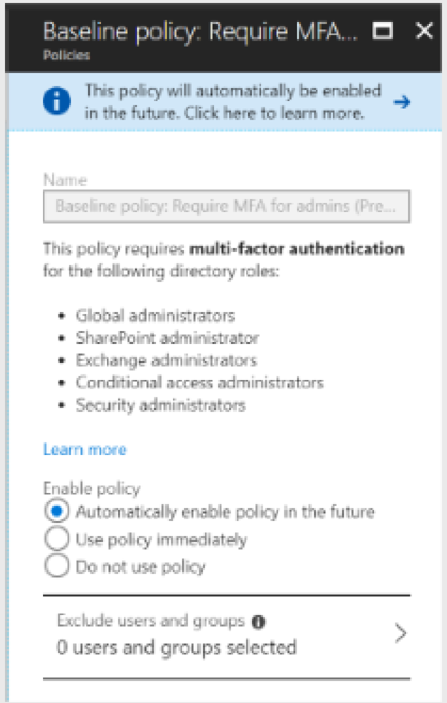
https://www.microsoft.com/security/blog/2019/04/11/introducing-the-security-configuration-framework-a-prioritized-guide-to-hardening-windows-10/

Phishing

Mitigating Phishing → MFA and Training

Microsoft Forcing Multi-Factor Authentication on Azure AD Admin Accounts

By **Catalin Cimpanu** June 25, 2018 02:07 PM 0



Baseline policy: Require MFA...

Policies

This policy will automatically be enabled in the future. Click here to learn more.

Name

Baseline policy: Require MFA for admins (Pre...

This policy requires **multi-factor authentication** for the following directory roles:

- Global administrators
- SharePoint administrator
- Exchange administrators
- Conditional access administrators
- Security administrators

Learn more

Enable policy

● Automatically enable policy in the future

○ Use policy immediately

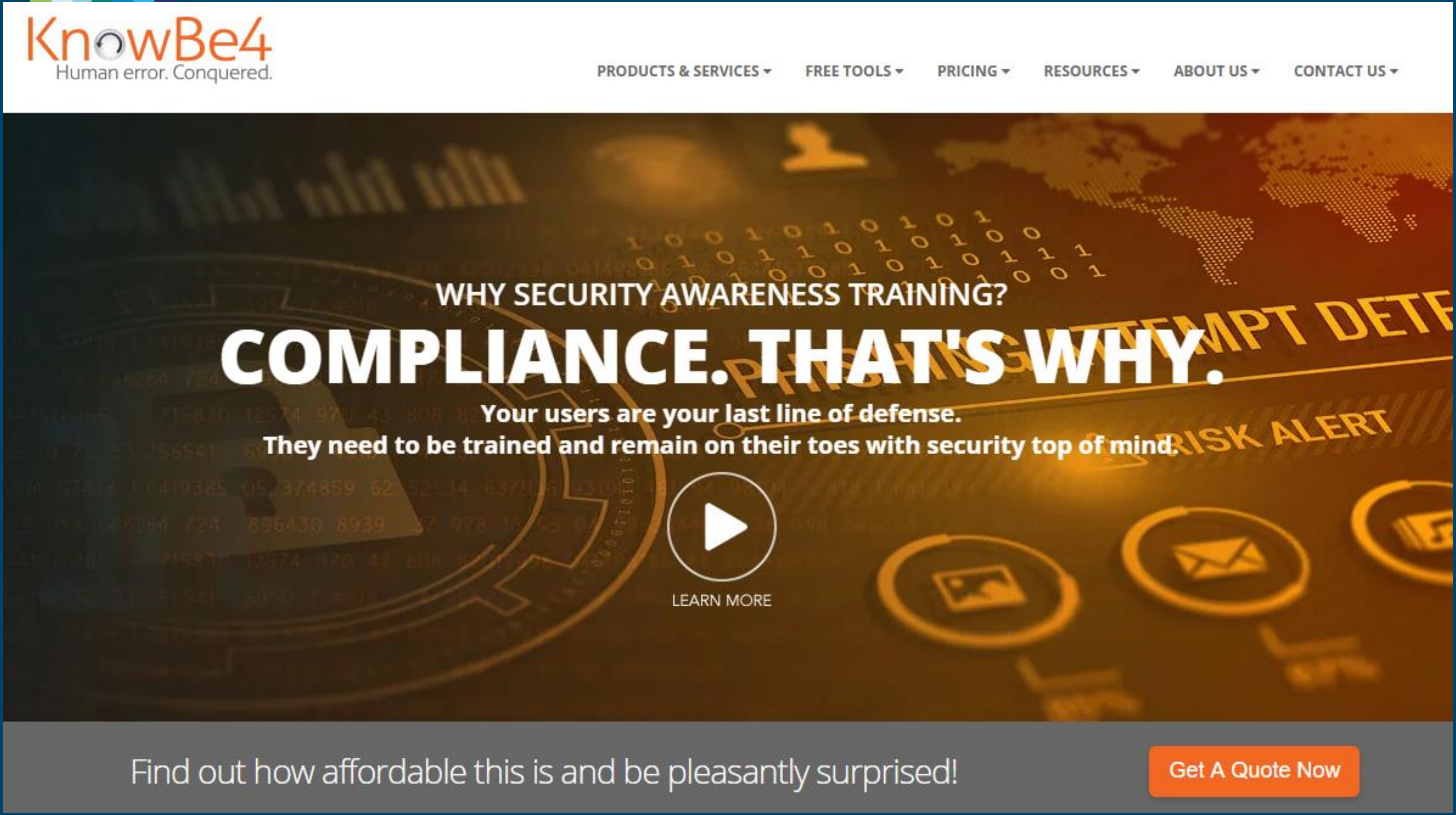
○ Do not use policy

Exclude users and groups

0 users and groups selected

Microsoft will soon enable multi-factor authentication (MFA) for all high-privileged Azure AD accounts, the company said on Friday.

The MFA feature will be part of Microsoft Azure AD's "baseline policy," a set of security features that are enabled for accounts to support a minimum of security measures.



WHY SECURITY AWARENESS TRAINING?

COMPLIANCE. THAT'S WHY.

Your users are your last line of defense.
They need to be trained and remain on their toes with security top of mind.

Find out how affordable this is and be pleasantly surprised!

Training

- Bank employee

Training

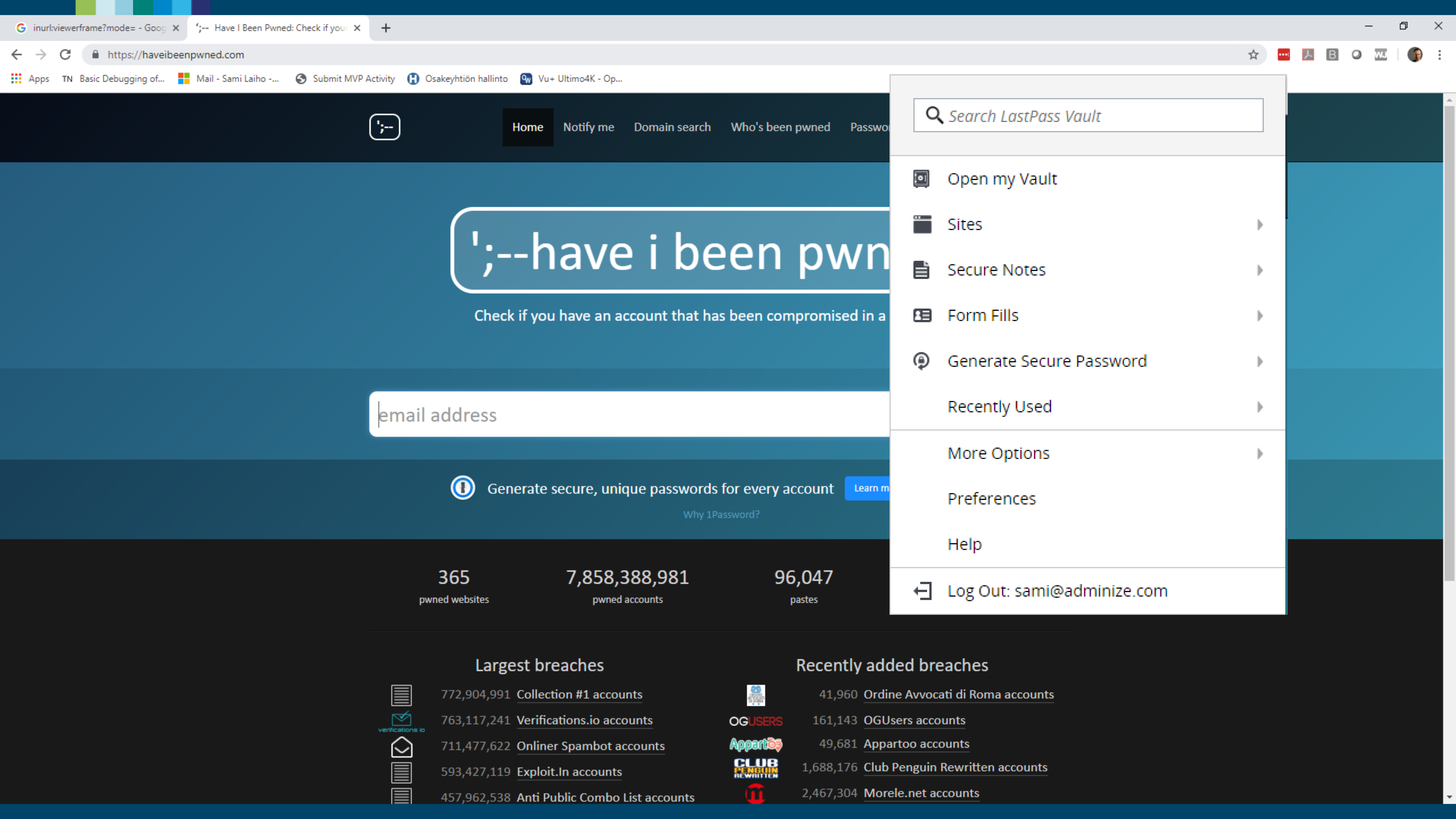
- CIO !!

Credential Theft

Mitigating Credential Theft

→No reusing passwords

→Password Managers



';--have i been pwn

Check if you have an account that has been compromised in a

Generate secure, unique passwords for every account

Why 1Password?

365	7,858,388,981	96,047
pwned websites	pwned accounts	pastes

Largest breaches

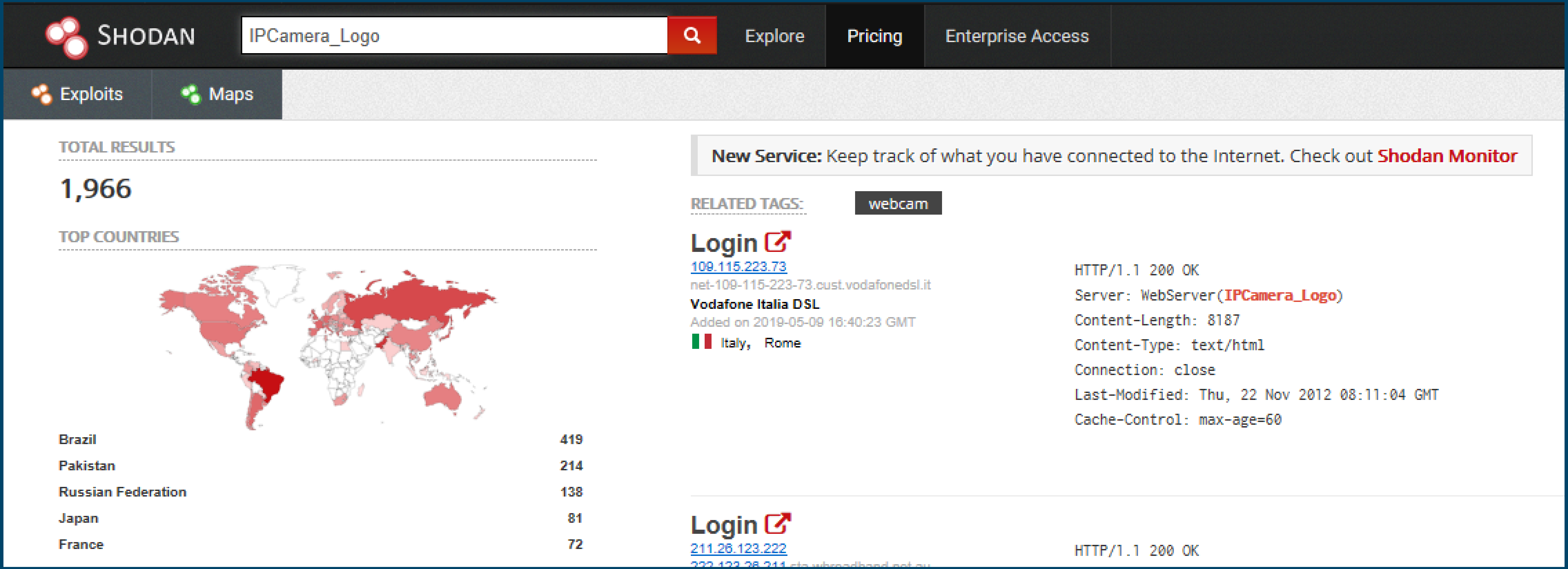
772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts

Recently added breaches

41,960	Ordine Avvocati di Roma accounts
161,143	OGUsers accounts
49,681	Appartoo accounts
1,688,176	Club Penguin Rewritten accounts
2,467,304	Morele.net accounts

IoT – Learn to protect devices

- https://www.shodan.io/explore/tag/webcam



TOTAL RESULTS

1,966

TOP COUNTRIES

Brazil	419
Pakistan	214
Russian Federation	138
Japan	81
France	72

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

RELATED TAGS: webcam

Login

109.115.223.73
net-109-115-223-73.cust.vodafonedsl.it
Vodafone Italia DSL
Added on 2019-05-09 16:40:23 GMT
Italy, Rome

```
HTTP/1.1 200 OK
Server: WebServer(IPCamera_Logo)
Content-Length: 8187
Content-Type: text/html
Connection: close
Last-Modified: Thu, 22 Nov 2012 08:11:04 GMT
Cache-Control: max-age=60
```

Login

211.26.123.222
222.123.26.211.sta.wbroadband.net.au

```
HTTP/1.1 200 OK
```

Google

- inurl:viewerframe?mode=

WANT MORE?

- Come to my courses
  - https://win-fu.com/ilt/!
- Check out my videos at PluralSight!
  - Send me an email for a free pass!
- Check out my personal video library at https://win-fu.com/dojo
  - Send me an email for a free pass!
- Follow me on Twitter: @samilaiho
- Consulting? Email me at sami@adminize.com

Thank You!

Platinum

Microsoft

Gold

audiocodes

Silver

au2mator

pexip

Jabra

logitech