

IT SECURITY

“DAS KLEINE 1X1”



Ihre heutigen IT-Security Vortragenden



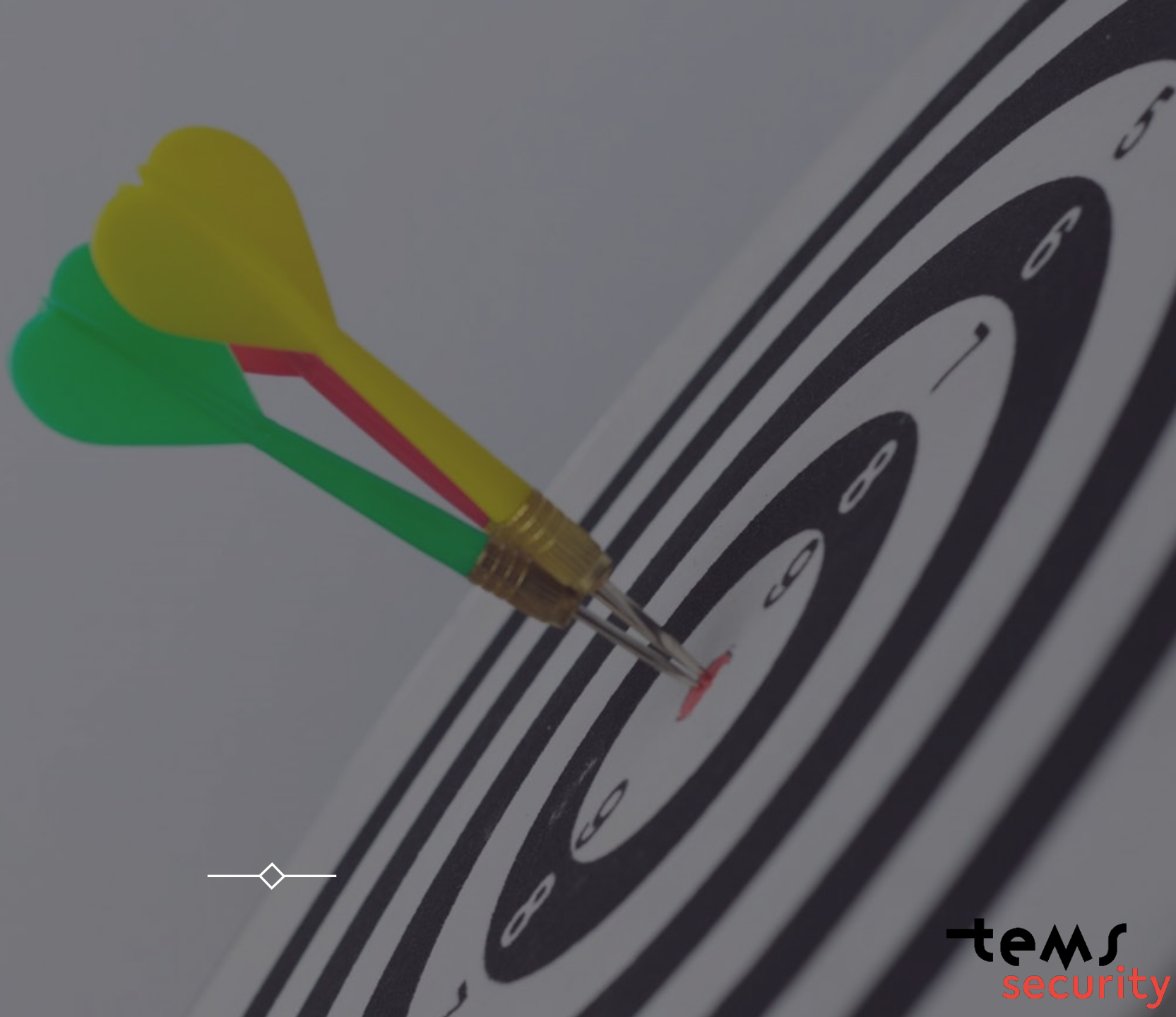
Alexander Kuchelbacher
CEO TEMS GMBH



Michael Meixner, CISSP
Managing Director

Agenda

- Rules of the Game
- Hackers Workflow
- Another side of Google
- Practice tips





The one and only Rules in IT-Security

Rules of the game



- The hacker need **only one Vulnerability or misconfiguration** and the hacker has access to an company network.
- A company can catch the hacker with **only through command or lateral movement** within the network and we are able to detect the hacker.

Training and knowledge are the key factor for success

Hacking workflow



WEAPONIZATION

EXPLOITATION

COMMAND & CONTROL (C2)



RECONNAISSANCE

DELIVERY

INSTALLATION

ACTIONS ON OBJECTIVES (*what`s next?*)

Unsere große Fehleinschätzung mit IT



achrichtendienst



2nd Level Support

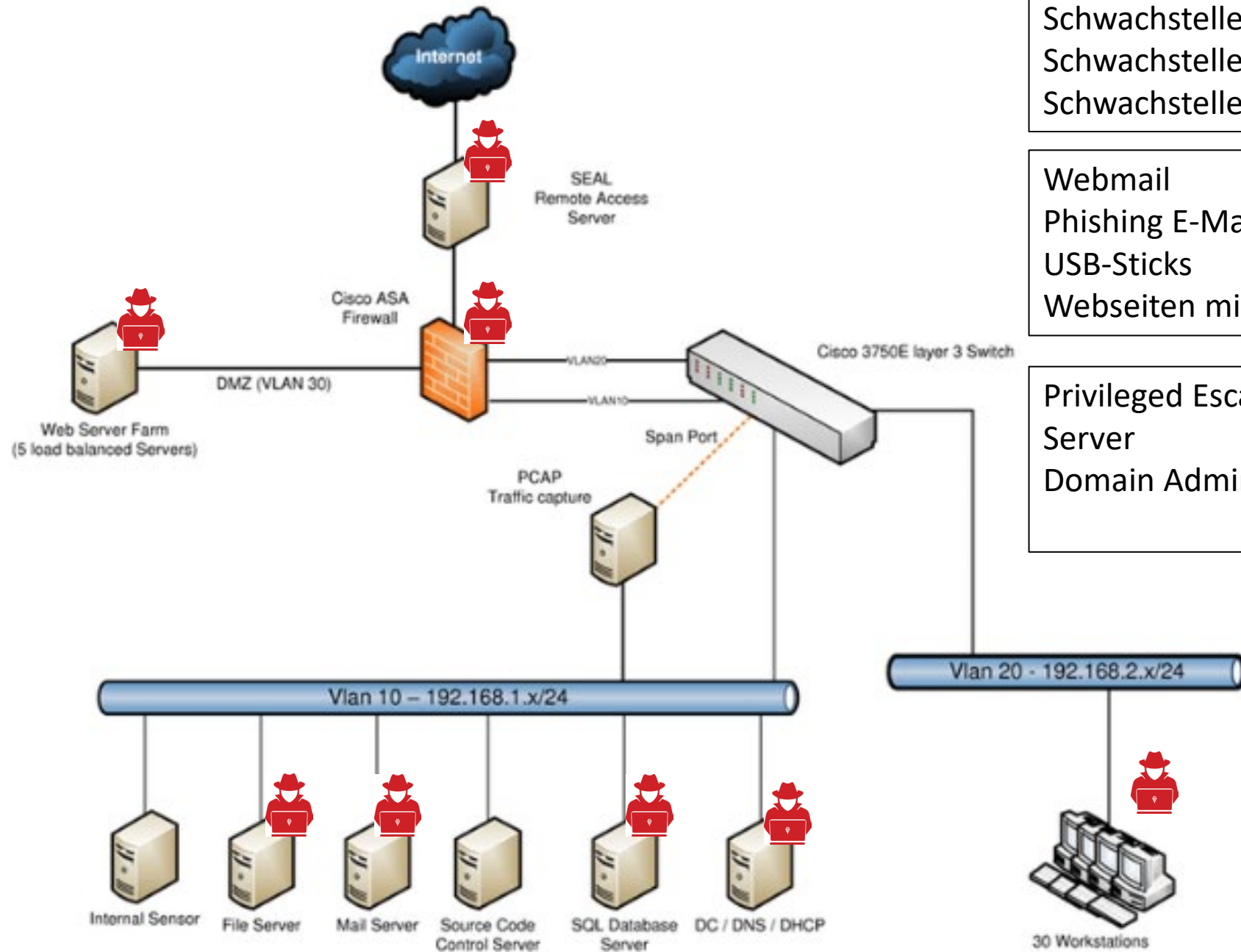


TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Pa

xität



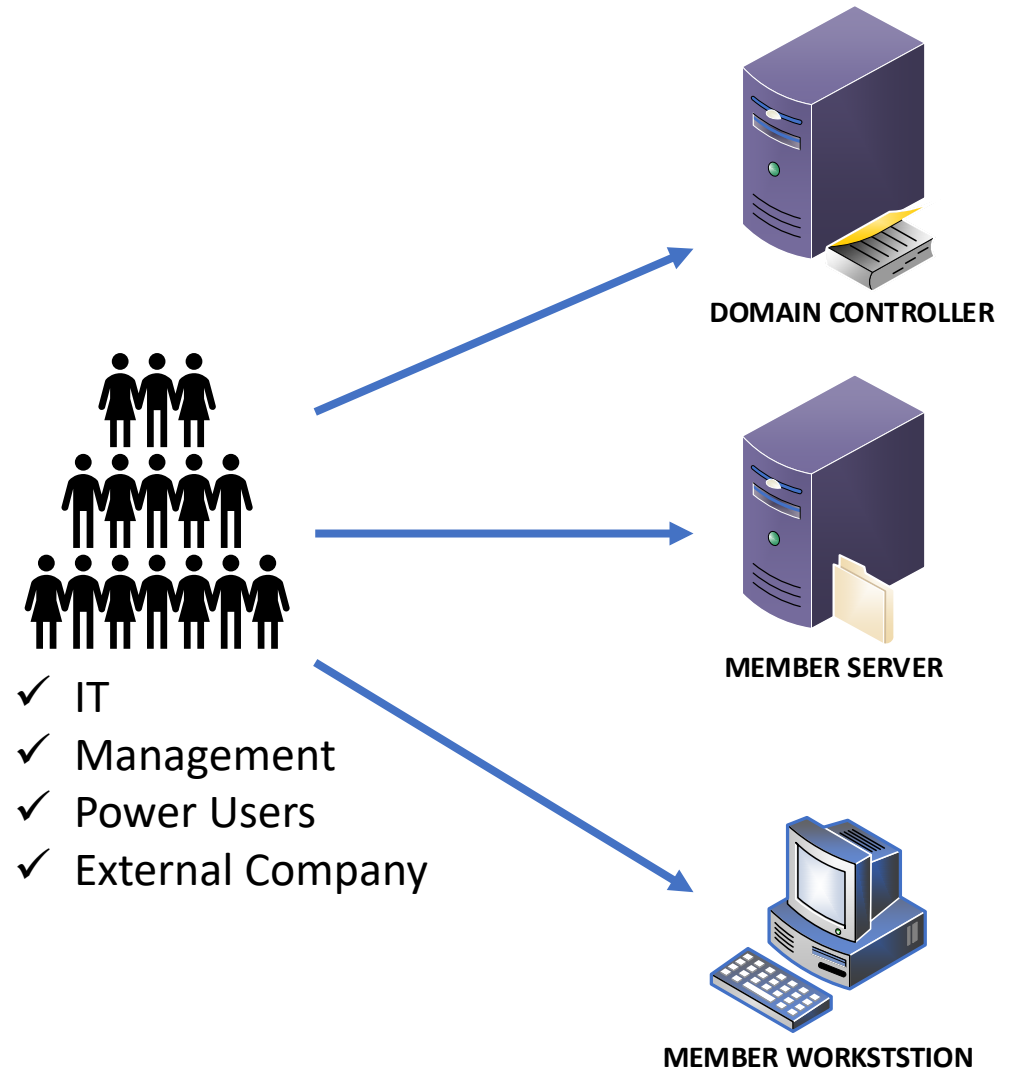
Schwachstellen im Remote Server
 Schwachstellen der Firewall
 Schwachstellen in der Webfarm

Webmail
 Phishing E-Mails (3 Typen)
 USB-Sticks
 Webseiten mit Malware

Privileged Escalation
 Server
 Domain Administrator

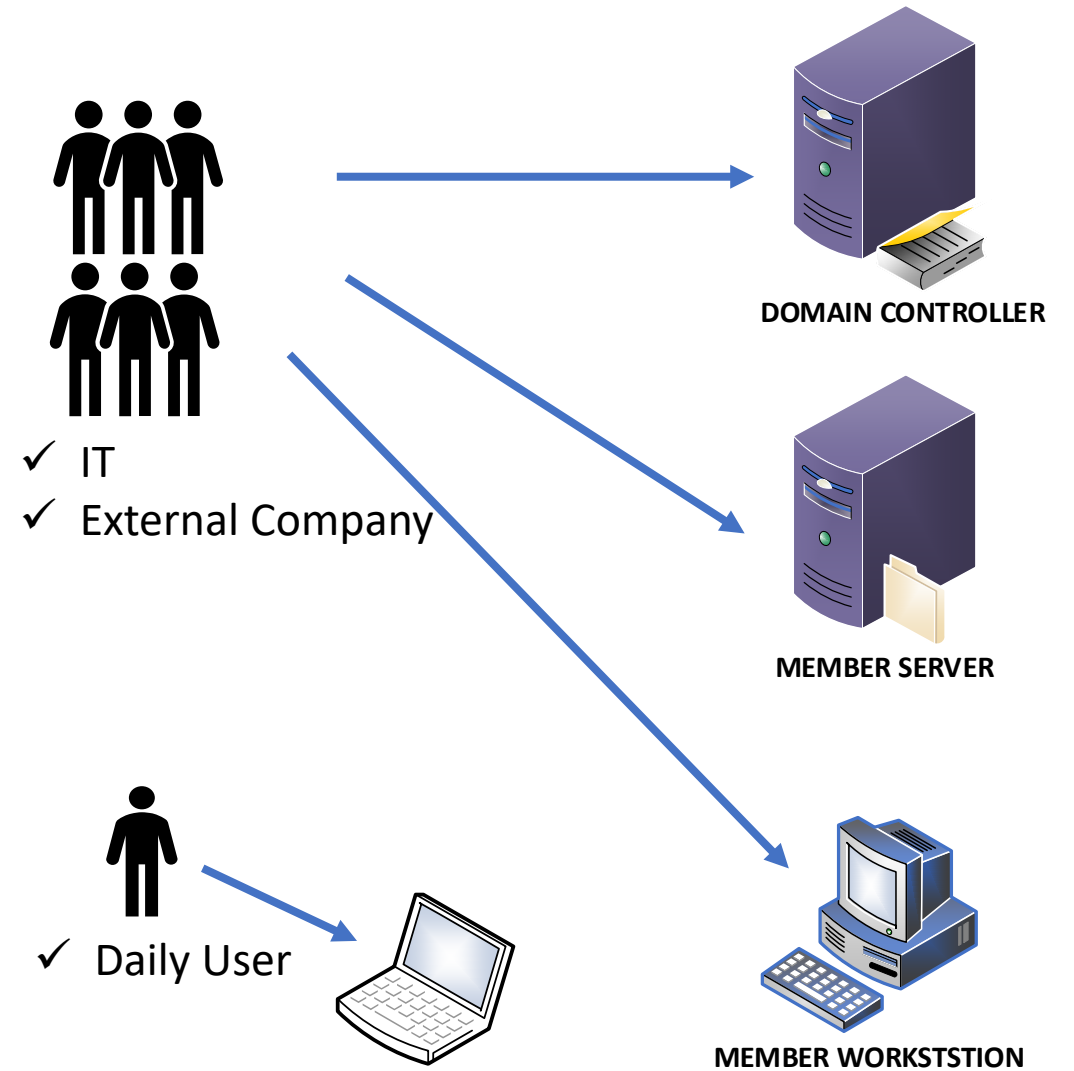
Single User concept

- ❑ Old by good and still exists in 2022
- ❑ Very simple to setup
- ❑ Very simple for administration
- ❑ **Very easy to get hacked within a minute**



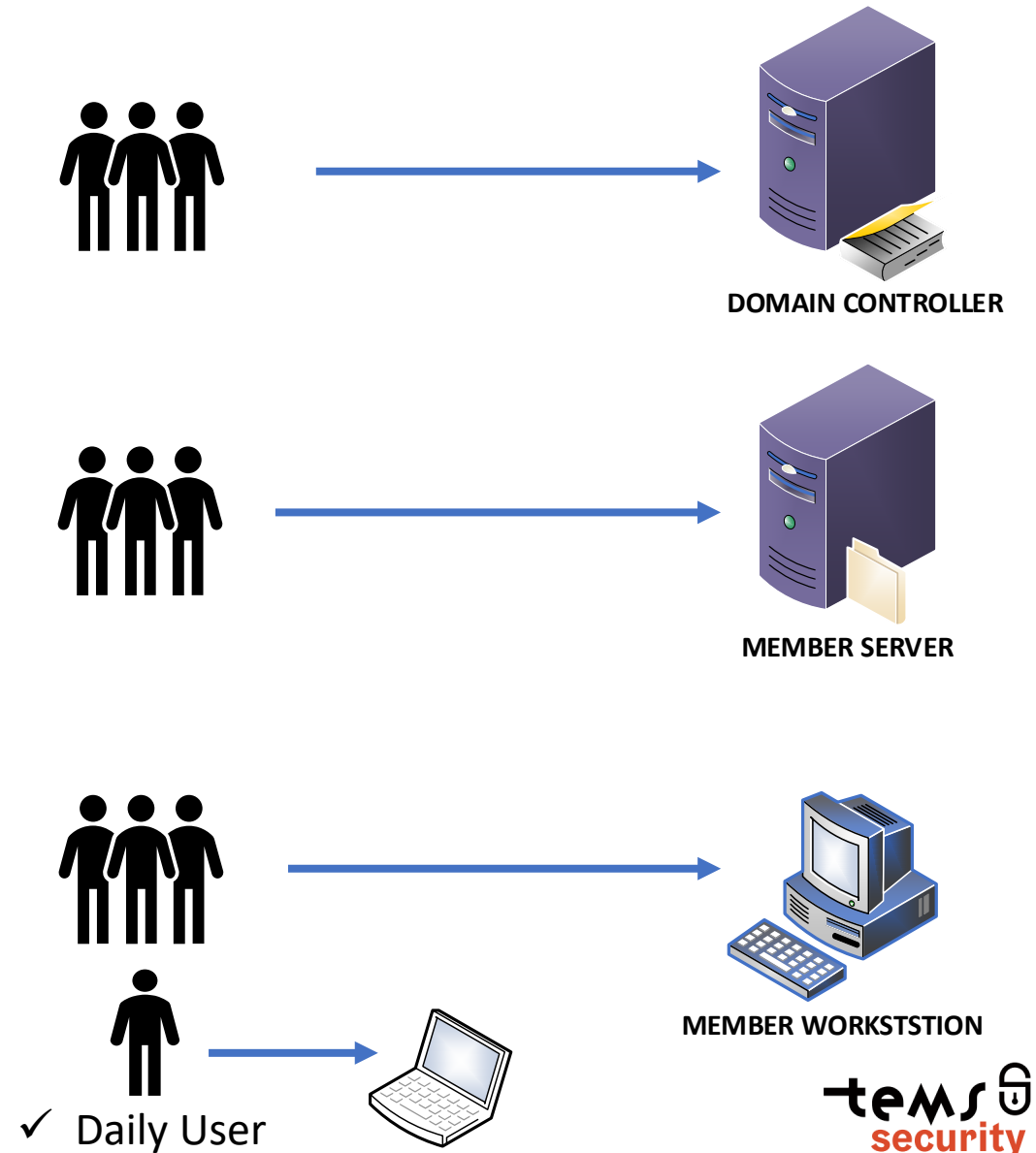
Two User concept

- ❑ One user account for administration
- ❑ One normal daily user account
- ❑ Old by good and still exists in 2022
- ❑ Very simple to setup
- ❑ Very simple for administration
- ❑ Easy to get hacked within two minutes



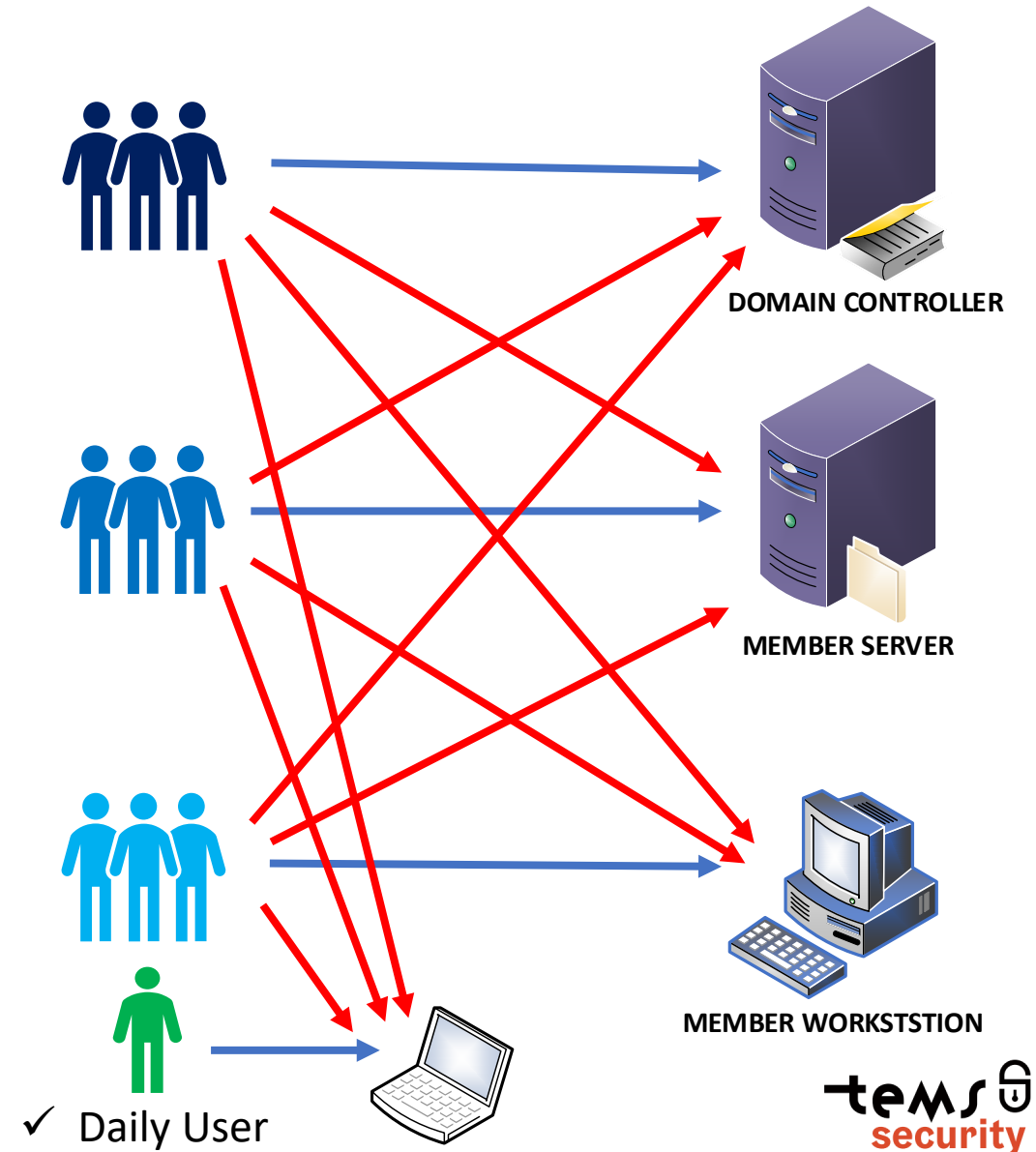
Tier Level Modell (Basic implementation)

- ❑ Four user accounts for Domain admins
- ❑ Three user accounts for Server admins
- ❑ Two user accounts for Desktop admins
- ❑ Easy with IT-Security focus to implement
- ❑ Challenge for hacker to gain access to Servers or Domain controllers



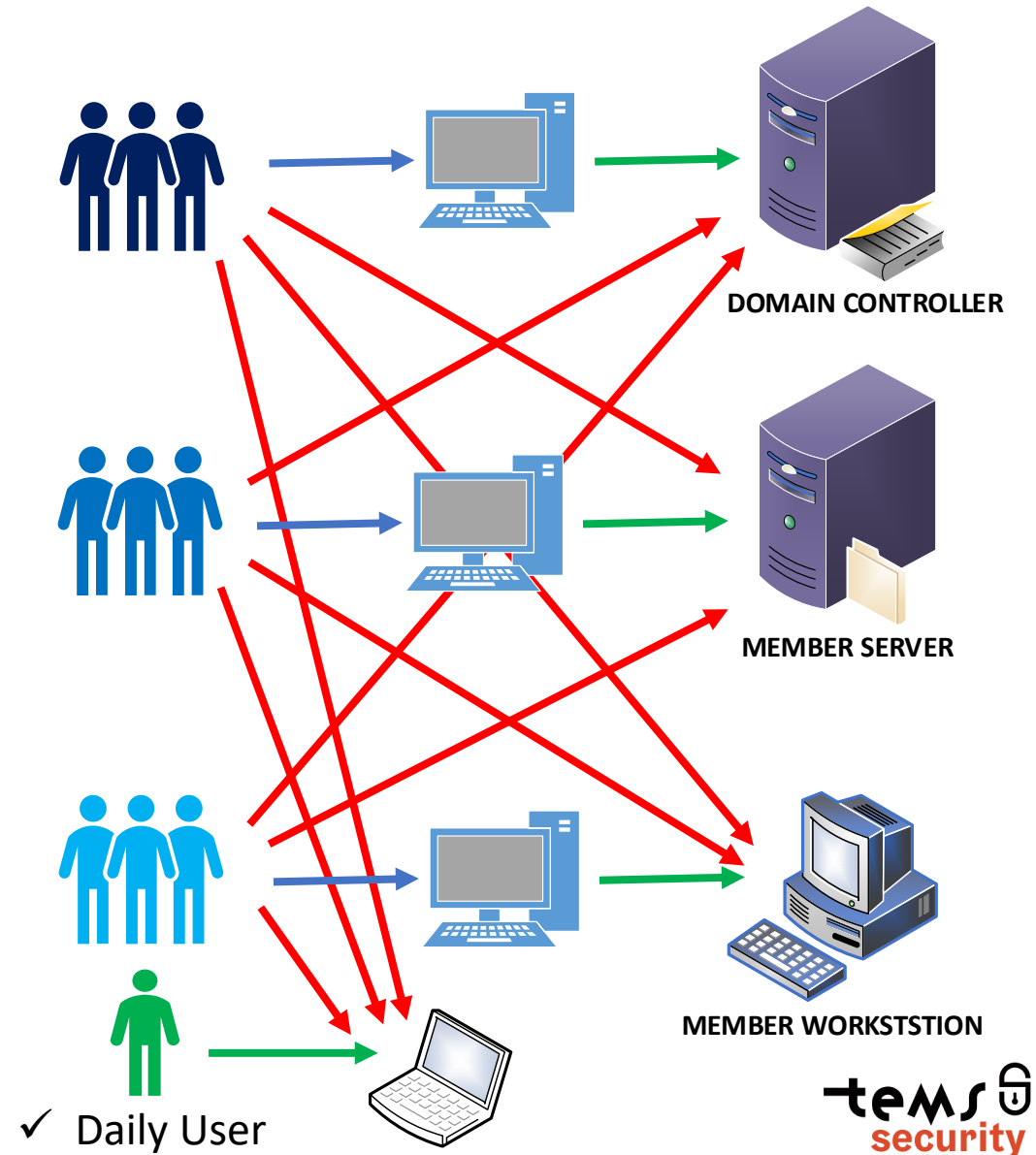
Tier Level Modell (with enforcement)

- ❑ Four user accounts for Domain admins
- ❑ Three user accounts for Server admins
- ❑ Two user accounts for Desktop admins
- ❑ Easy with IT-Security focus to implement
- ❑ Difficult for hacker to gain access to Servers or Domain controllers

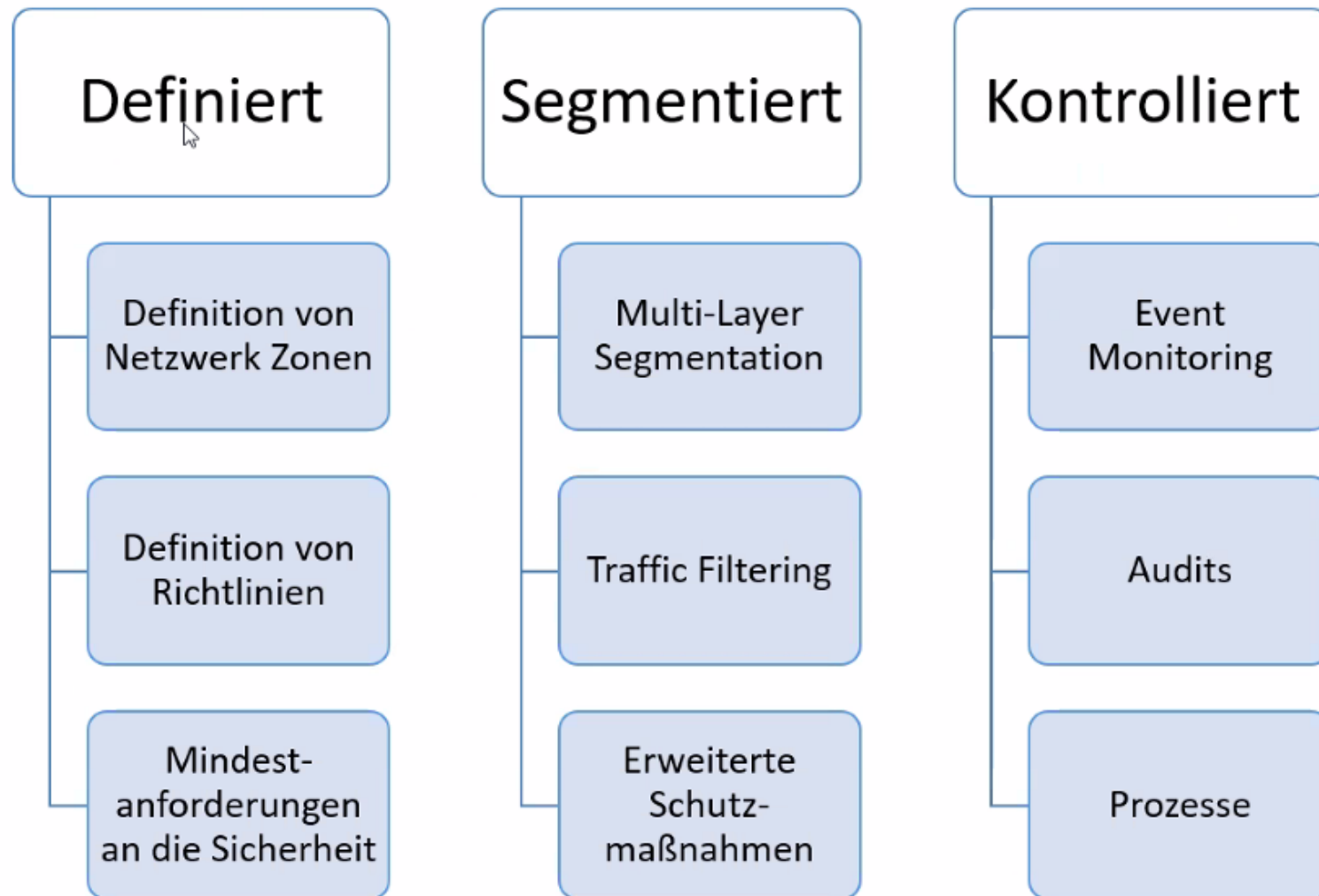


Tier Level Modell (state of the Art)

- ❑ Administration only with Privileged Access Workstation (aka PAW)
- ❑ Four user accounts for Domain admins
- ❑ Three user accounts for Server admins
- ❑ Two user accounts for Desktop admins
- ❑ Easy with IT-Security focus to implement
- ❑ Very difficult for hacker to lateral movement within the network



Eckpfeiler für ein sicheres Netzwerk



Google but not Google

Vulnerability from December 2022 for Fortinet Firewalls

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

PSIRT Advisories

VPN

FortiOS / FortiProxy - Heap buffer underflow in administrative interface

Summary

A buffer underwrite ("buffer underflow") vulnerability in FortiOS & FortiProxy administrative interface may allow a remote unauthenticated attacker to execute arbitrary code on the device and/or perform a DoS on the GUI, via specifically crafted requests.

Exploitation status:

Fortinet is not aware of any instance where this vulnerability was exploited in the wild. We continuously review and test the security of our products, and this vulnerability was internally discovered within that frame.

Affected Products

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.9
- FortiOS version 6.4.0 through 6.4.11
- FortiOS version 6.2.0 through 6.2.12
- FortiOS 6.0 all versions
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.8
- FortiProxy version 2.0.0 through 2.0.12
- FortiProxy 1.2 all versions
- FortiProxy 1.1 all versions

CVSS Score



TOTAL RES

15,61

TOP CITIES

Vienna

Graz

Linz

Innsbruck

Salzburg

More...

TOP PORTS

10443

443

541

1723

8443

More...

IR Number	FG-IR-23-001
Date	Mar 7, 2023
Severity	●●●●● Critical
CVSSv3 Score	9.3
Impact	Execute unauthorized code or commands
CVE ID	CVE-2023-25610
Affected Products	FortiOS : 7.2.3, 7.2.2, 7.2.1, 7.2.0, 7.0.9, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 6.4.9, 6.4.8, 6.4.7, 6.4.6, 6.4.5, 6.4.4, 6.4.3, 6.4.2, 6.4.11, 6.4.10, 6.4.1, 6.4.0, 6.2.9, 6.2.8, 6.2.7, 6.2.6, 6.2.5, 6.2.4, 6.2.3, 6.2.2, 6.2.12, 6.2.11, 6.2.10, 6.2.1, 6.2.0, 6.0.9, 6.0.8, 6.0.7, 6.0.6, 6.0.5, 6.0.4, 6.0.3, 6.0.2, 6.0.16, 6.0.15, 6.0.14, 6.0.13, 6.0.12, 6.0.11, 6.0.10, 6.0.1, 6.0.0
	FortiProxy : 7.2.2, 7.2.1, 7.2.0, 7.0.8, 7.0.7, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0, 2.0.9, 2.0.8, 2.0.7, 2.0.6, 2.0.5, 2.0.4, 2.0.3, 2.0.2, 2.0.12, 2.0.11, 2.0.10, 2.0.1, 2.0.0, 1.2.9, 1.2.8, 1.2.7, 1.2.6, 1.2.5

Informationen gelten

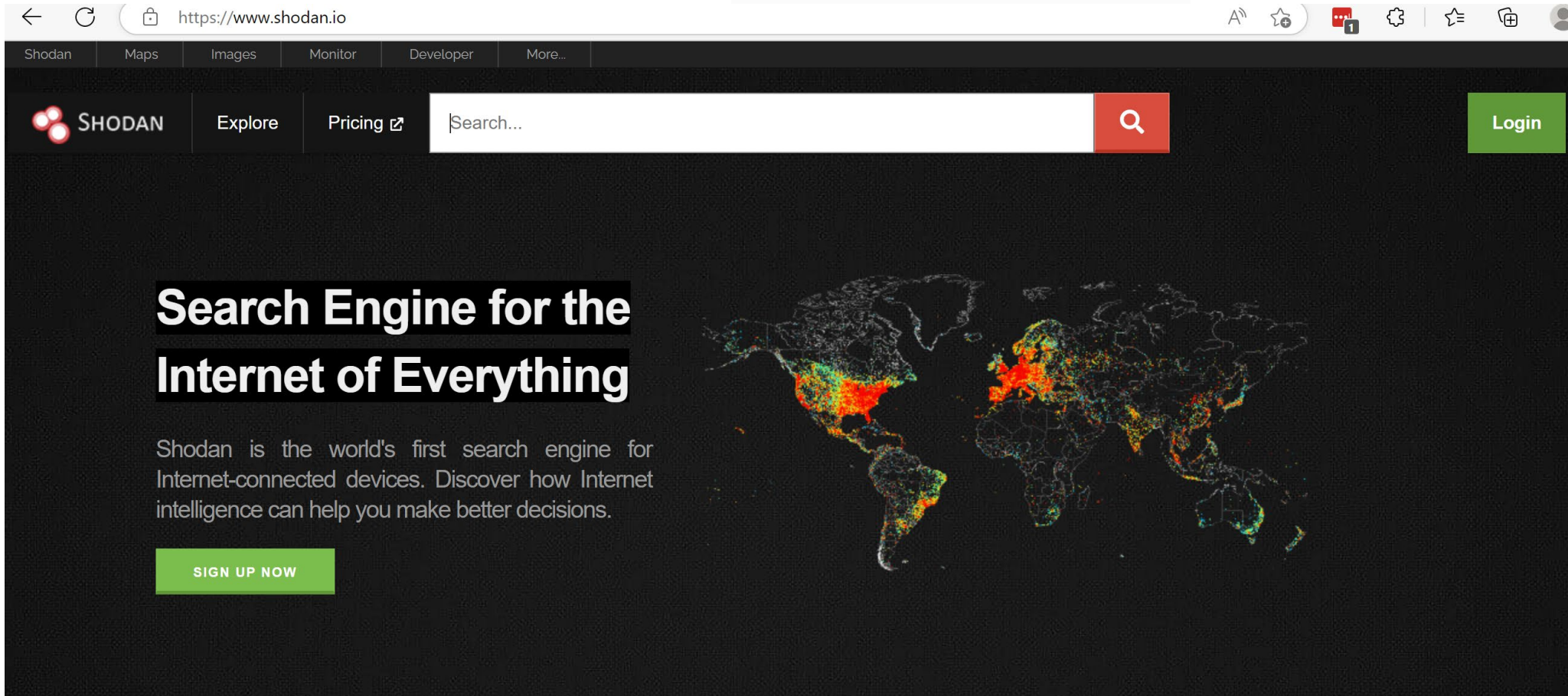
Informationen frei weitergegeben

Informationen zum TLP

Informationen zu einer Angabe des Fortinet – siehe [CWE2022] Diese Schwachstelle über speziell geformte



Shodan.io



The screenshot shows the Shodan.io website interface. At the top, there is a navigation bar with links for Shodan, Maps, Images, Monitor, Developer, and More... Below this is a search bar with the placeholder text "Search..." and a red search button. To the right of the search bar is a green "Login" button. The main content area features a large heading "Search Engine for the Internet of Everything" and a subheading "Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions." Below the text is a green "SIGN UP NOW" button. On the right side of the main content area is a world map with a heatmap overlay, showing high concentrations of devices in North America and Europe.



LIVE DEMO

Shodan.io



N°	Notifier	Single def.	Mass def.	Total def.	Homepage def.	Subdir def.
1.	Hmei7	139830	154879	294709	85387	209322
2.	d3bvx	84239	76967	161206	21104	140102
3.	Index Php	78964	75820	154784	9796	144988
4.	iskorpitx	78018	393556	471574	268015	203559
5.	chinafans	59680	52410	112090	287	111803
6.	Sejeal	52296	53936	106232	9881	96351
7.	1923Turk	43760	229059	272819	108399	164420
8.	muhmademad	41141	41387	82528	10153	72375
9.	Team_CC	38544	78463	117007	19531	97476
10.	misafir	29192	52504	81696	11197	70499
11.	ZoRRoKiN	26882	47657	74539	43246	31293
12.	imam	26504	29385	55889	2268	53621
13.	panataran	24757	24772	49529	2832	46697
14.	GHoST61	24620	330797	355417	175498	179919
15.	Ashiyane Digital Security Team	23405	60365	83770	25221	58549
16.	Fatal Error	23319	50604	73923	67622	6301
17.	ErrOr SquaD	22723	44469	67192	3880	63312
18.	w4l3xzy3	22215	30743	52958	1909	51049
19.	BD GREY HAT HACKERS	21678	67547	89225	35831	53394
20.	SA3D HaCk3D	20357	68443	88800	17867	70933
21.	jok3r	20280	14090	34370	1630	32740
22.	HighTech	19130	35548	54678	29006	25672
23.	Mr.Kro0oz.305	16686	41474	58160	4706	53454
24.	TheWayEnd	16558	100000	116558	53434	63124
25.	LUN4T1C0	16521	23084	39605	1821	37784
26.	KaMtiEz	14877	16437	31314	10011	21303
27.	HolaKo	13865	7833	21698	1127	20571
28.	MiSh	13123	3214	16337	90	16247
29.	Mister Spy	11786	7168	18954	2369	16585
30.	Clash Hackers	11283	9521	20804	578	20226



LIVE DEMO

zohe-h.org





With and without Log Management

helpdecrypt@msgsafe.io



YOUR FILES ARE ENCRYPTED

Don't worry, you can return all your files!

If you want to restore them, follow this link: email helpdecrypt@msgsafe.io YOUR ID **C279F237**

If you have not been answered via the link within 12 hours, write to us by e-mail: helpdecrypt@msgsafe.io

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

System or network activity (packets, program execution, ...)

OR



Jedes Unternehmen welches über kein SIEM verfügt fährt hier 130 km/h

LIVE DEMO

KIBANA (SIEM)





Tems Security Service Offering

Managed Services

- Patchmanagement
- Firewalling
- Endpoint Security
- Monitoring (SIEM)

Cyber Security Assessments

Penetrationstest (intern, extern)

Netzwerk Security

Backup Konzepte

Incident Response (24x7 Hotline)

IT Forensik
Car Forensics
eDiscovery

IT Gutachten

Cyber-Security Schulungen

Linux Consultant

SIEM / XDR



Minimal requirements for IT Security

TOP 5 IT SECURITY RELATED POINTS

1. **Create a security policy:** A security policy outlines the principles and procedures for IT security within a company. It should define the responsibilities of employees and the strategies for preventing and addressing security breaches.
2. **Protect your networks and devices:** Protect your networks and devices with firewalls, antivirus software, and other security measures. Also, ensure that all devices are regularly updated with the latest security updates and patches.
3. **Protect your data:** Encrypt important data and conduct regular backups to restore essential data in case of loss or security breach.
4. **Train your employees:** Make your employees aware of the most critical security procedures and practices within the company and handling sensitive data.
5. **Regularly review your security measures:** Conduct regular security reviews to identify and address vulnerabilities in your security measures.

HANDS-ON BY TEMS SECURITY

1. Based on your Company size, a couple of pages of “Do's and Don'ts”
2. Key is Multifactor Authentication for everything from the Internet to any internal resources and patch, log and monitor all systems
3. Bitlocker with PIN and LAPS is a good baseline with state of the art backup concept
4. Phishing campaign is mentored for everyone
5. If you are done with all 4 perform an IT-Audit

Thank you

QUESTIONS?