SIE WURDEN GEHACKT?

Notfall-Nummer:
+43(1) 3914001 600

WEIHNACHTS-AUSGABE

WEBINAR

21. DEZEMBER 22

IT-Hardening 101

mit

tems security

Ihr heutiges Cyber Incident & IT-Security Team

Philip Berger
Managing Director

Alexander Kuchelbacher
CEO TEMS GMBH

Michael Meixner, CISSP
Managing Director

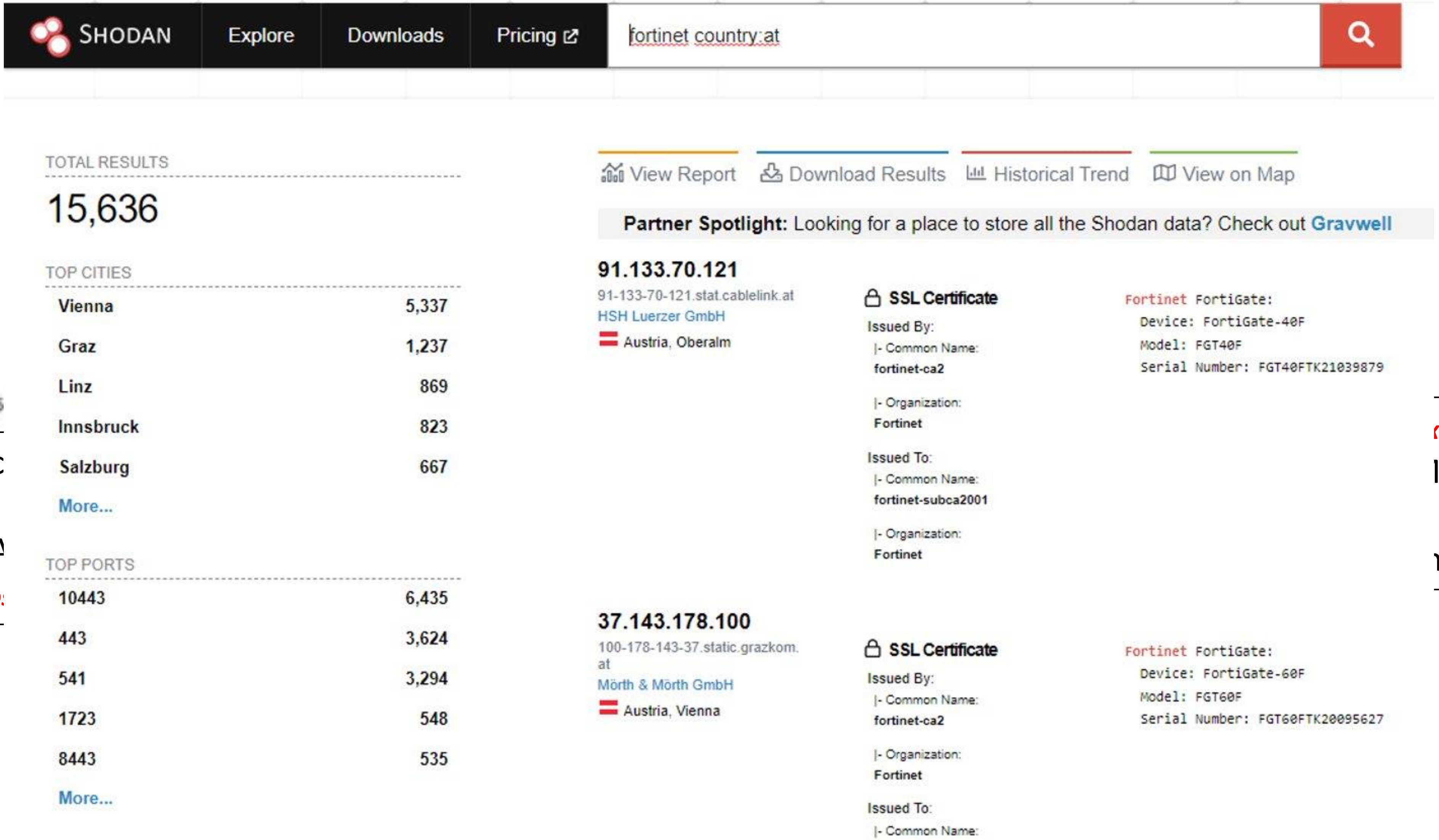
André Reinhold
Head of IT-Security

Stephan Emich
Senior Security Consultant

tems security

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI



fortinet country:at

TOTAL RESULTS

15,636

TOP CITIES

Vienna	5,337
Graz	1,237
Linz	869
Innsbruck	823
Salzburg	667
More...	

TOP PORTS

10443	6,435
443	3,624
541	3,294
1723	548
8443	535
More...	

Partner Spotlight: Looking for a place to store all the Shodan data? Check out Gravwell

91.133.70.121
91-133-70-121.stat.cablelink.at
HSH Luerzer GmbH
Austria, Oberalm

SSL Certificate
Issued By:
|- Common Name:
fortinet-ca2
|- Organization:
Fortinet
Issued To:
|- Common Name:
fortinet-subca2001
|- Organization:
Fortinet

```
Fortinet FortiGate:
  Device: FortiGate-40F
  Model: FGT40F
  Serial Number: FGT40FTK21039879
```

37.143.178.100
100-178-143-37.static.grazkom.at
Mörth & Mörth GmbH
Austria, Vienna

SSL Certificate
Issued By:
|- Common Name:
fortinet-ca2
|- Organization:
Fortinet
Issued To:
|- Common Name:

```
Fortinet FortiGate:
  Device: FortiGate-60F
  Model: FGT60F
  Serial Number: FGT60FTK20095627
```

(5

Privileged Esc
Server Attack
Get Domain A
„Golden Kerbero

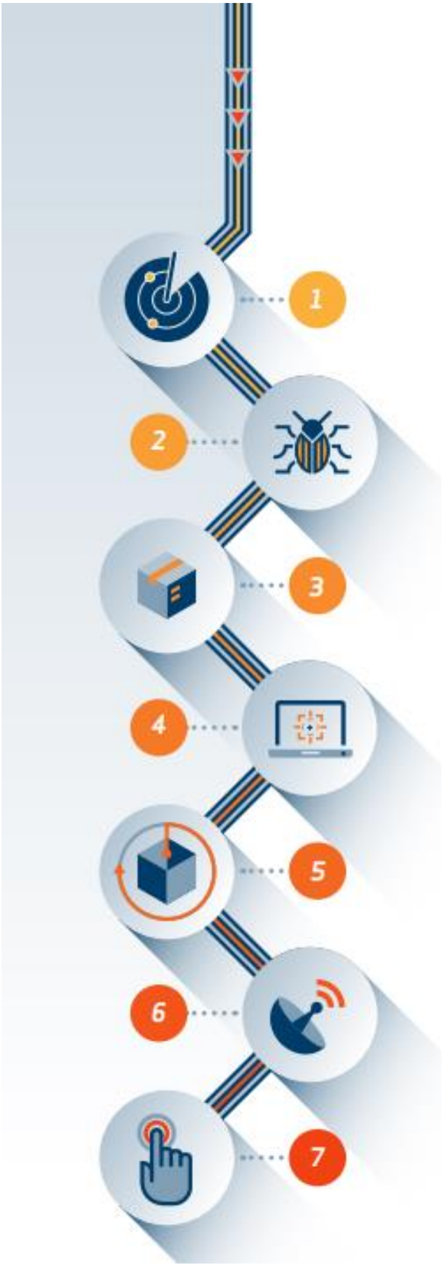
xchange)
lails *(3 Types)*
ı Malware

ermöglicht es unautorisierten Angreifenden, Schadcode auf dem System oder Befehle über speziell geformte Anfragen auszuführen.

Die Schwachstelle wird vom Hersteller nach Common Vulnerability Scoring System (CVSS) v3.1 mit einem gesamt CVSS-Wert von 9.3 als „kritisch" bewertet. Für die Schwachstelle wurde die CVE-2022-42475 vergeben (siehe [FORT2022a], [MITR2022]).

tems security

Hacking workflow



RECONNAISSANCE

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND & CONTROL (C2)

ACTIONS ON OBJECTIVES (what`s next?)

Source: https://www.lockheedmartin.com/

THE LOCKHEED MARTIN CYBER KILL CHAIN ®

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

How to make it easy for Hackers
Easy administration

1	Backup run with Domain admin user	local admin rights for anything who request it	Tier Model is to much work	Perform admin tasks from user workstations
2	Admin shares with everyone rights	Full unlimited Internet access for all Server without logging	Default passwords are easy to remember	MFA is too boring
3	Use standard password for service accounts	Password in clear text in txt or excel without PW	No Firewall Logging and a lot “Any to Any” Rules	Password policy OK but password expire set to “Never”

tems security

Webinar Series

17. Jänner 2023
09:00 Uhr – 10:00 Uhr (online)

Tech talk Deluxe with TEMS(Security) Professionals

THEMA: “SIEM with Tems Security”

INHALT:

- ✓ SIEM Überblick
- ✓ SIEM Einblicke
- ✓ Integrationen
- ✓ Alerting

SIE WURDEN GEHACKT?
Notfall-Nummer:
+43(1) 3914001 600