

Bitte beschriften Sie die Cyber Defense Prüfung mit Ihrem Namen und Vornamen. Ich wünsche Ihnen viel Erfolg!

Name

Vorname

# Cyber Defense HS2021

## Hauptprüfung

### 18. Januar 2022

Document Name: 2021\_HS21\_Cyber\_Defense\_Hauptprüfung\_mit\_der\_Musterlösung\_V1.0.docx

Version: V1.0

Author: Ivan Buetler

Classification: EXAM

## Inhaltsverzeichnis

<b>1 CYBER DEFENSE HAUPTPRÜFUNG</b>	<b>4</b>
1.1 MITRE ATT&CK FRAMEWORK (6 PUNKTE)	4
1.2 YARA (6 PUNKTE)	6
1.3 VELOCIRAPTOR (8 PUNKTE)	8
1.4 MEMORY FORENSICS (7 PUNKTE)	10
1.5 RED TEAMING (4 PUNKTE)	12
1.6 MUTUAL AUTH (3 PUNKTE)	13
1.7 WEBAPP IN DMZ (12 PUNKTE)	14
1.8 INFORMATIKER STREIT (2 PUNKTE)	16
1.9 DNS OVER HTTP (DOH) (12 PUNKTE)	17
1.10 RANSOMWARE (8 PUNKTE)	20
1.11 RDP BRUTE FORCE ATTACK (2 PUNKTE)	21
1.12 IP BLOCKLIST (3 PUNKTE)	22
1.13 FORENSIK (6 PUNKTE)	23
1.14 GPO (6 PUNKTE)	24
1.15 SIGMA RULES (5 PUNKTE)	25
1.16	26
1.17 ADVISORY (6 PUNKTE)	27
1.18 SSH AUDIT (6 PUNKTE)	29
1.19 NLA (6 PUNKTE)	30
1.20 LARGE SCALE (6 PUNKTE)	31
1.21 SPF/DKIM/DMARC (6 PUNKTE)	32
<b>2 ANHANG</b>	<b>33</b>
2.1 LOG4J ADVISORY	33

## Punkteverteilung

Aufgabe	1	MITRE	6	Punkte
Aufgabe	2	Yara	6	Punkte
Aufgabe	3	Velociraptor	8	Punkte
Aufgabe	4	Memory Forensics	7	Punkte
Aufgabe	5	Red Teaming	4	Punkte
Aufgabe	6	Mutual Auth	3	Punkte
Aufgabe	7	Web App in DMZ	12	Punkte
Aufgabe	8	Informatiker Streit	2	Punkte
Aufgabe	9	DNS over HTTP	12	Punkte
Aufgabe	10	Ransomware	8	Punkte
Aufgabe	11	RDP Brute Force	2	Punkte
Aufgabe	12	IP Blocklist	3	Punkte
Aufgabe	13	Forensik	6	Punkte
Aufgabe	14	GPO	6	Punkte
Aufgabe	15	SIGMA Rules	5	Punkte
Aufgabe	16	Advisory	6	Punkte
Aufgabe	17	SSH Audit	6	Punkte
Aufgabe	18	NLA	6	Punkte
Aufgabe	19	Large Scale	6	Punkte
Aufgabe	20	SPF/DKIM/DMARC	6	Punkte
<b>TOTAL</b>			<b>120</b>	<b>Punkte</b>

## Sprache

Ihre Lösungen müssen in Blockschrift geschrieben werden (lesbar). Die Verwendung von Englischen Begriffen (aus den Folien, Vorlesung) ist absolut ok und erlaubt.

## Abändern der Fragestellung

Bitte ändern Sie die Fragestellung der Fragen nicht ab. Belassen Sie die Fragen wie sie sind. Wenn es für Sie Unklarheiten gibt, dann treffen Sie Annahmen. Kennzeichnen Sie ihre Annahmen deutlich.

## Zuwenig Platz für Ihre Antworten

Falls Sie zu wenig Platz für Ihre Lösung/Antwort haben, dann nutzen Sie bitte die Rückseite des vorherigen Blattes und machen eine deutlich und klar ersichtliche Referenz darauf (Pfeil, Buchstabe)

## Kugelschreiber / Filzstift

Bitte beantworten Sie die Fragen mit einem Kugelschreiber, Füllfederhalter oder Filzstift.

**\*NICHT\* mit Bleistift.**

## 1 Cyber Defense Hauptprüfung

### 1.1 MITRE ATT&CK Framework (6 Punkte)

Frage	Antwort	Punkte
Was ist eine Cyber Kill Chain?	<p>Die Cyber Kill Chain ist eine schematische Darstellung eines Angriffs. Dabei wird das Vorgehen während einem Angriff in einzelne Phasen unterteilt.</p> <p>Das MITRE ATT&amp;CK Framework nennt diese Phasen "Tactics".</p> <p>Die Kill Chain wird verwendet um die Abläufe von Angriffen geordnet zu kategorisieren und dokumentieren.</p>	1
Erklären Sie was der Begriff "Technique" im MITRE ATT&CK Framework bedeutet.	<p>Techniken sind Elemente von einer oder mehreren Taktiken. Grundsätzlich beschreibt die Technik die effektive Umsetzung einer Taktik. Das Framework listet für Techniken deshalb die technischen Details wie bspw. Kommandos oder Event IDs für die Detektion.</p>	1

Frage	Antwort	Punkte
Welchen Zweck verfolgen Angreifer, wenn wie " T1053 Scheduled Task/Job" anwenden?	"T1053 Scheduled Task/Job" ist eine Technik  Angreifer können die Funktion zur Aufgabenplanung missbrauchen, um die erstmalige oder wiederholte Ausführung von böartigem Code zu erleichtern. Zudem kann damit sichergestellt werden, dass ein Code über längere Zeit auf dem System verbleibt und läuft => Persistenz.	1
Erklären Sie was der Begriff "Tactic" im MITRE ATT&CK Framwork bedeutet.	Die Tactics sind die einzelnen Phasen eines Angriffs. Die MITRE ATT&CK Matrix stellt dabei diese Phasen als Spalten dar.	1
Nennen Sie eine "Tactic" und erklären Sie, was damit gemeint ist.	Bspw. Initial Access  Dies ist der Erstzugriff auf ein Opfer. Es werden verschiedene Zugangsvektoren nutzen, um zunächst in einem Netzwerk Fuß zu fassen. Zu den Techniken, die eingesetzt werden, um Fuß zu fassen, gehören gezieltes Spearphishing und das Ausnutzen von Schwachstellen auf öffentlich zugänglichen Servern. Die durch den Erstzugang erlangte Position kann einen kontinuierlichen Zugang ermöglichen, wie z. B. gültige Konten oder die Nutzung externer Remote-Dienste.	2

## 1.2 YARA (6 Punkte)

Frage	Antwort	Punkte
<p>Erklären Sie, inwiefern sich ein Scan mittels YARA Rules von einem Virens Scanner unterscheidet.</p> <p>Nennen Sie dabei je einen <b>Vorteil</b> und einen <b>Nachteil</b>.</p>	<p>Bsp. Nachteil</p> <ul style="list-style-type: none"> <li>- YARA wird nicht präventiv eingesetzt</li> <li>- YARA verwendet keine Hooks (On File Access) oder AV APIs</li> </ul> <p>Bsp. Vorteil</p> <ul style="list-style-type: none"> <li>- YARA erlaubt die Suche von Files nach selbst kreierten Regeln</li> </ul> <p>YARA erlaubt die Suche von spezifischen Zeichenketten</p>	2
<p>Sie untersuchen einen Vorfall.</p> <p>Ihr Kollege hat endlich die Malware entdeckt und davon gleich einen SHA256 Hash erstellt.</p> <p>Er will nun alle 5000 Server und Clients in der Infrastruktur auf den Hash durchsuchen.</p> <p>Erklären Sie, warum dies eine gute oder schlechte Idee ist.</p>	<p>Es ist eine schlechte Idee, weil es macht keinen Sinn einen Hash ohne weitere Metainformation zu suchen, da die Zielsysteme einer enormen Last ausgesetzt werden, um Hashes von allen möglichen Files zu erstellen.</p>	2

Frage	Antwort	Punkte
<p>Wir wollen das Memory eines aktuellen Windows 10 nach einem String durchsuchen und verwenden die YARA Regel nebenan.</p> <p>Leider verläuft die Suche erfolglos. Nennen Sie Gründe, warum die Suche gescheitert ist, und korrigieren Sie die Regel.</p>	<pre>rule Gotham {     strings:         \$a = "Batman"         \$b = "Robin"      condition:         \$a or \$b }</pre> <p><b>LÖSUNG</b></p> <p>Strings werden in der Regel in 16-byte Darstellung abgelegt und durch den Zusatz "wide" "ascii" in beliebiger Reihenfolge werden die Strings dann gefunden.</p> <pre>rule Gotham {     strings:         \$a = "Batman" wide ascii         \$b = "Robin" wide ascii      condition:         \$a or \$b }</pre>	2

### 1.3 Velociraptor (8 Punkte)

Frage	Antwort	Punkte
<p>Sie sind Incident Handler und werden zu einem Notfall gerufen. Die infizierte Firma betreibt über hundert Server und rund tausend Workstations darunter viele Laptops. Für die Analyse deployen Sie einen Velociraptor Server und via GPO die Velociraptor Agents auf die jeweiligen Server und Workstations. Nach rund 30min haben sich aber erst wenige Agents beim zentralen Server gemeldet.</p> <p><b>Nennen Sie 3 mögliche Ursachen.</b></p>	<ul style="list-style-type: none"> <li>- Aktuell ist keine Bürozeit und die Workstations sind nicht eingeschaltet</li> <li>- Die Systeme können Netzwerkässig nicht zum Server kommunizieren (Firewall)</li> <li>- Die Systeme haben die GPOs noch nicht aktualisiert und der Agent wurde nicht ausgeführt</li> <li>- Der Agent ist nicht mit einer korrekten Softwaresignatur versehen</li> <li>- Es handelt sich um Linux und Macs, die keine GPO unterstützen</li> </ul>	3
<p>Sie analysieren ein Fall und haben herausgefunden, dass sich die Angreifer mittels PSEXEC von System zu System bewegen.</p> <p>Sie möchten nun mit Hilfe von Velociraptor herausfinden, welche Systeme betroffen sind.</p> <p>Zählen Sie vier Aktionen auf, die Sie dafür im GUI des Velociraptors ausführen müssen?</p>	<ol style="list-style-type: none"> <li>1. Wechsel auf die Ansicht Hunt</li> <li>2. Neuen Hunt erstellen</li> <li>3. Wählen des Sysinternals EULA Artefakt</li> <li>4. Hunt starten</li> </ol>	2



Frage	Antwort	Punkte
<p>Leider passt keines der vorgefertigten Artefakte für Ihre aktuelle Untersuchung.</p> <p>Sie verwenden das Velociraptor Notebook, um eine neue Query zu programmieren und es werden auch gleich erste Ergebnisse dargestellt.</p> <p>Von welchem System stammen die Ergebnisse des Notebook Output, welche bei der ausgeführten Query angezeigt werden?</p>	<p>Die Resultate stammen vom System, wo der Velociraptor Server installiert ist.</p>	1
<p>Wenn ein Benutzer nicht interaktiv am System angemeldet ist, dann ist sein Registry Hive bzw. dann sind seine User spezifischen Registry Einträge nicht in der Registry ersichtlich.</p> <p>Nennen Sie eine Methode, wie man mit Velociraptor trotzdem auf die Registry-Einträge von nicht angemeldeten Benutzern zugreifen kann.</p>	<p>Man kann der RAW Reg Accessor verwenden um damit auf das ntuser.dat im Benutzerprofil zuzugreifen und die benutzerspezifischen Registry Einträge direkt aus dem File lesen.</p>	2

## 1.4 Memory Forensics (7 Punkte)

Frage	Antwort	Punkte
<p>Die Akquisition von flüchtigem Speicher (RAM) braucht Zeit und Platz und macht deshalb nicht für jede Untersuchung Sinn.</p> <p>Nennen Sie 2 Situationen, Verdächtige bzw. Vorfälle wo die Akquisition von RAM zwingend notwendig ist.</p>	<p>Situationen, wo folgende Artefakte benötigt werden</p> <ul style="list-style-type: none"> <li>- Prozesse</li> <li>- Netzwerkverbindungen</li> <li>- Geladene Treiber</li> <li>- Konsolen Historie</li> <li>- Zeichenkette im Speicher</li> <li>- Credentials und Schlüssel</li> <li>- Laufende Programme</li> <li>- Rootkit</li> </ul>	2
<p>Erklären Sie den Begriff "Memory Smear" und was dies für die forensische Analyse von flüchtigem Speicher (RAM) bedeutet.</p>	<p>In der Zeit, wo das Memory collected wird, passieren weitere Änderungen am System, so dass allenfalls im Nachgang durch Inkonsistenzen keine gute Analyse gemacht werden kann.</p> <p>Durch die Akquisition von Memory verändert der Forensiker den Zustand des Systems.</p>	1
<p>Nennen Sie zwei Beispiele, wie bzw. wo Sie beim Sammeln von flüchtigem Speicher den "Memory Smear" verhindern können.</p>	<p>Virtuelle Maschine =&gt; pausieren</p> <p>OS =&gt; Evt. User Prozess pausieren</p>	2

Frage	Antwort	Punkte
Nennen Sie den Unterschied zwischen den Volatility commands pslist und psscan.	<p>Pslist =&gt; folgt der EProcess Struktur der PSActiveProcessList (double linked list) und gibt die Prozesse aus.</p> <p>Psscan =&gt; sucht den Speicher nach den einzelnen Elementen ab und kann somit auch Elemente erkennen, die mutwillig aus der Liste detached/unliked wurden (hidden processes).</p>	2

### 1.5 Red Teaming (4 Punkte)

Frage	Antwort	Punkte
Erklären Sie den Begriff "Lateral Movement"	Angreifer hüpfen von System zu System.	1
Geben Sie 3 Unterschieden zwischen "Penetration Test" und "Red Teamings" an.	<p>1 Penetration Test sucht nach Schwachstellen und gibt diese dem Kunden weiter (für die Behebung)</p> <p>2 Penetration Test sind die IT Verantwortlichen der Kunden meist informiert über den Test</p> <p>3 Red Teaming beübt die Organisation und schaut, ob das Monitoring Team die Attacke erkennt</p> <p>4 Red Teaming prüft das Verhalten der User und tested, zum Beispiel die Wirksamkeit einer Awareness Kampagne (Phishing, E-Mail Fraud)</p>	3

## 1.6 Mutual Auth (3 Punkte)

Frage	Antwort	Punkte
Erklären Sie wie Mutual Auth mit Zertifikaten funktioniert und begründen Sie, warum damit <b>kein</b> MitM möglich ist. Argumentieren Sie mittels Krypto Knowhow.	<p><b>Erklärung</b></p> <p>Bei Mutual Auth verifiziert der Client die Signatur des Server Zertifikats mit dem PubKey des Server Zertifikates respektive der CA Signatur und der Server prüft die Signatur des Client Zertifikates mit dem PubKey des Client Zertifikates, respektive der CA.</p> <p><b>Begründung</b></p> <p>Somit ist sowohl die Identität des Servers als auch des Clients über die korrekte Signature (via PubKey, CA Key) geprüft.</p> <p><b>Krypto Know-How</b></p> <p>Falls der MitM kein gültiges Client Certificate mit Private Key hat, ist somit eine MitM verhindert.</p>	3



Der CEO der Firma möchte den verwundbaren Log4j Service auf keinen Fall ausser Betrieb nehmen. Um einen Code Change in der Produktion einzuspielen, dauert es sicher 10 Tage. Welche Schritte machen Sie mit dieser Rahmenbedingung in welcher Reihenfolge, damit niemand die Sicherheitslücke ausnützen kann?

Reihenfolge	Antwort	Punkte
Sofortmassnahme (gleicher Tag)	<ol style="list-style-type: none"> <li>1 Sicherstellen, dass verwundbares System keinen Outgoing Traffic initialisieren kann.</li> <li>2 Falls eine WAF im Einsatz ist, eine WAF Rule definieren</li> <li>3 Überwachung des Systems, ob jemand versucht, den Log4j Exploit anzuwenden.</li> </ol>	3
Mittelfristige Massnahme (innerhalb 1 Woche)	<ol style="list-style-type: none"> <li>1 Auftrag für Code Fixing geben. Entwicklerteam soll Gegenmassnahme sofort umsetzen und Testing Fix auf DEV System priorisieren</li> <li>2 Roll-out Fix auf dem verwundbaren System</li> </ol>	2
Längerfristige Massnahme (innerhalb nächstem Monat)	<ol style="list-style-type: none"> <li>1 Monitoring von Verwundbarkeiten von eingesetzten Libraries</li> <li>2 Update Prozess überdenken, so dass HotFixes schneller in die PROD kommen können</li> <li>3 Monitoring Web App verbessern</li> </ol>	3

## 1.8 Informatiker Streit (2 Punkte)

Zwei SOC Mitarbeiter streiten sich in der Kaffee Pause über den Nutzen von Yara. Einer der Kollegen, der primär Windows Event Logs analysiert (EVT) argumentiert, dass er mit Yara überhaupt keinen Erfolg hatte und das Projekt «Yara» überbewertet wird.

Fragen	Antwort	Punkte
<p>Beurteilen Sie die obige Aussage.</p> <p>Begründen Sie Ihre Antwort.</p>	<p>Yara ist ein Tool für das Suchen von Mustern Binary Daten. Wenn die Binary Daten aber eine bekannte Struktur aufweisen (ZIP, EVT) dann sollte man mit einem Tool arbeiten, das dieses Format versteht und Exports erstellen, die man dann allenfalls mit Yara weiter untersuchen kann. Die exportierten Daten von EVT sind aber Text-Dateien, so dass YARA ungeeignet ist. Bei ZIP ist es anders, weil im ZIP auch Binäre Dateien enthalten sein können.</p> <p>Anders ausgedrückt, Yara ist für das Analysieren von EVT Files ungeeignet.</p>	2



## 1.9 DNS over HTTP (DoH) (12 Punkte)

Ein neuartiger Trojaner soll im Rahmen eines Red-Teaming Engagement über HTTPS DoH Kontakt zu seinem C2 Server (Command & Control) aufnehmen.

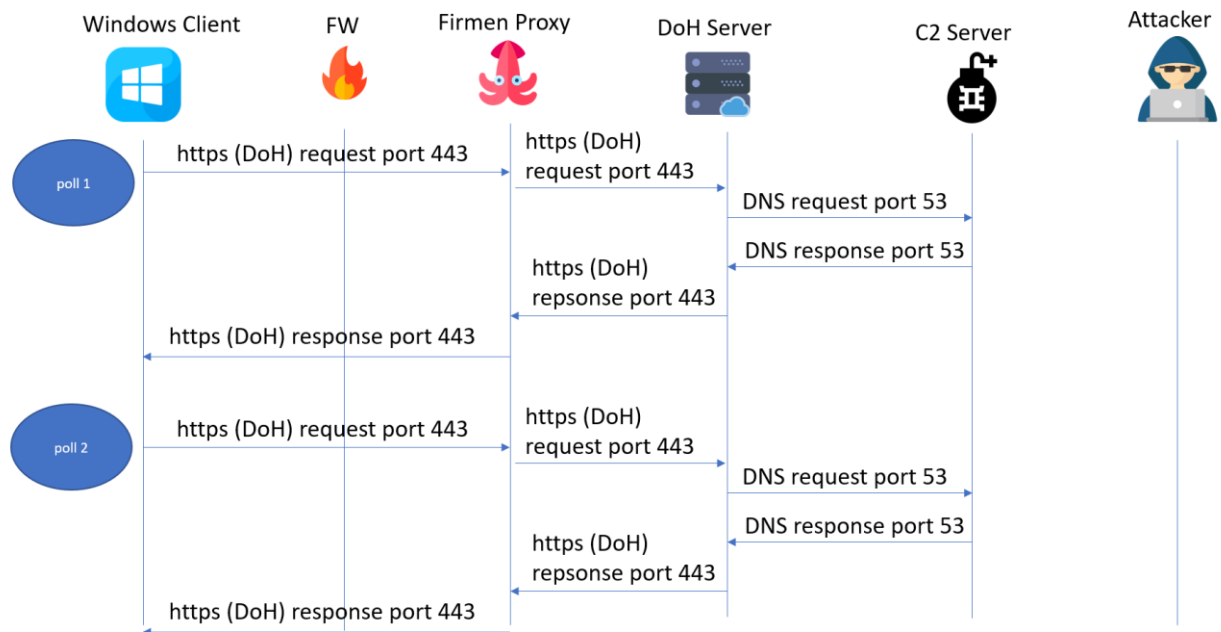
### Kriterien für Bewertung (Zeichnung)

- Richtung der Pfeile
- Angabe des Protokolls und Port
- Beschriftung pro Pfeil (Bedeutung)

### Polling des Trojaner zum C2 (polling for commands)

Zeichnen Sie nur das «Polling» des Windows Client zum C2 Server ein

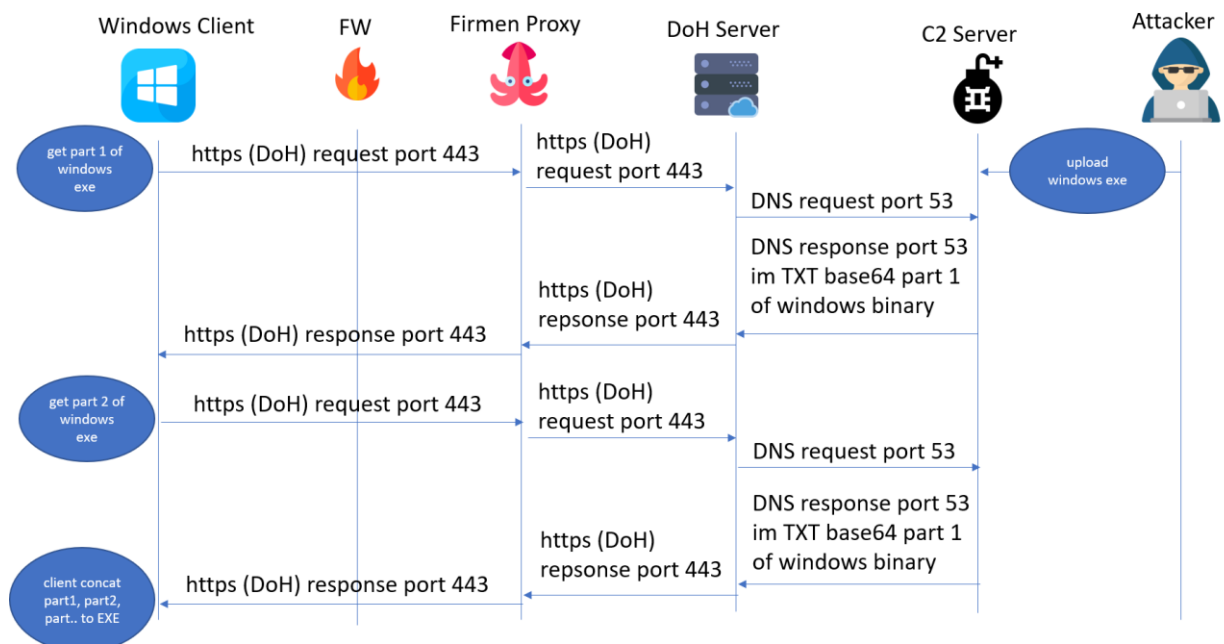
Zeichnung: 4 Punkte



### Download EXE vom C2 zum Windows Client

Zeichnen Sie ein, wie das trojanische Pferd auf dem Windows Client vom C2 Server ein weiteres EXE downloaded.

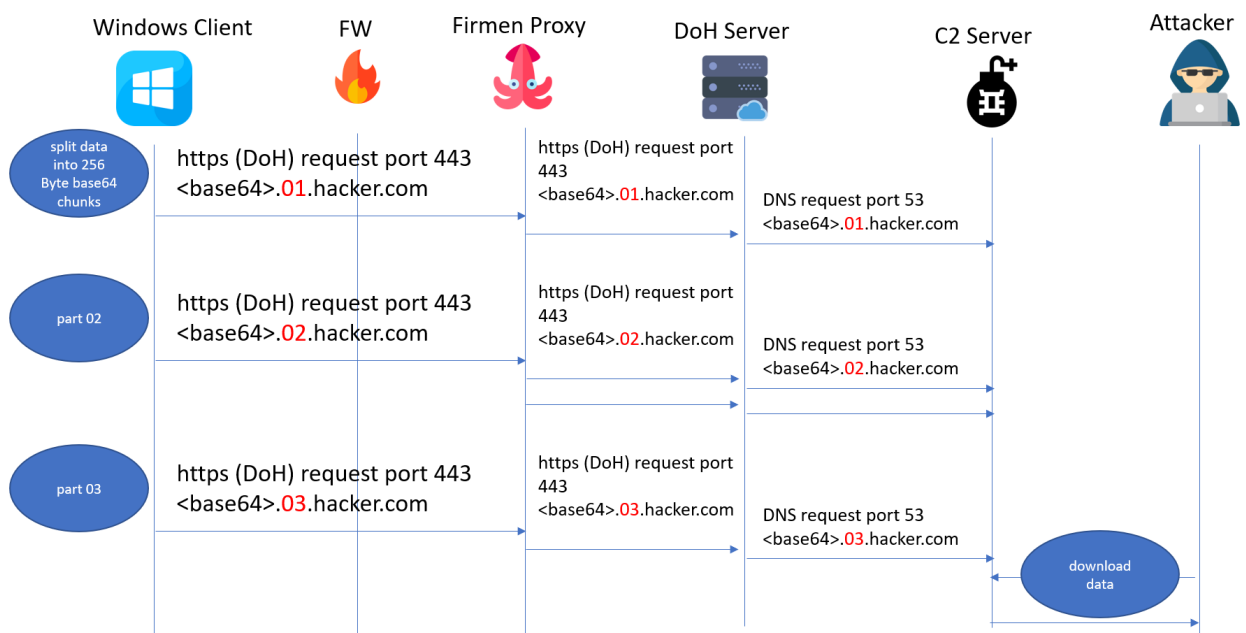
Zeichnung: 4 Punkte



### Datei-Upload vom Windows Client zum C2 Server

Zeichnen Sie den Ablauf, wie das trojanische Pferd auf dem Windows Client eine Datei (z.B. C:\geheim\passworte.txt) vom Windows Client zum C2 Server uploaded.

Zeichnung: 4 Punkte



## 1.10 Ransomware (8 Punkte)

Eine Firma wird Opfer einer Ransomware Attacke. Niemand hat den Angriff bemerkt und alle Daten sind übers Wochenende verschlüsselt worden. Der erste Mitarbeiter am Montag in der früh konnte sich nicht mehr am PC anmelden. Alle Files sind verschlüsselt, auf allen Clients und Server (Active Directory). Das Backup ist jedoch Gott sei Dank noch in Ordnung und die Netzwerk-Geräte und Firewalls sind nicht betroffen. Sie werden als Cyber Security Spezialist angefragt, was man nun der Reihe nach tun soll.

Geben Sie in untenstehende Tabelle 4 Schritte an, was der Kunde der Reihenfolge (Priorität) nach tun muss und was man besonders achten muss, um wieder in den «Normalbetrieb zu kommen». Verzichten Sie auf organisatorische Massnahmen und fokussieren Sie sich auf technische Massnahmen.

Reihenfolge	Antwort	Punkte
1	Backups in Sicherheit bringen  Zuerst rausfinden, über welche Attacke die Ransomware reingekommen ist. Es nützt nichts mit dem Backup Recovery zu beginnen, bevor man das Eintrittsfenster nicht geschlossen hat	2
2	Wiederherstellung Active Directory auf Basis des funktionierenden Backups	2
3	Wiederherstellung der Windows Clients auf Basis des funktionierenden Backups. Dabei die wichtigsten Clients priorisieren.	2
4	Verbesserung Monitoring, um bei einem erneuten Ransomware Angriff nicht erst am Montag in der Früh davon zu erfahren.	2

### 1.11 RDP Brute Force Attacke (2 Punkte)

Während der Wazuh-Übung im Hacking-Lab war es etwas frustrierend zu sehen, dass man im Wazuh die RDP Brute Forcing Attacken nicht finden konnte.

Frage	Antwort	Punkte
<p>Beschreiben Sie die Lösung für das Problem, so dass sämtliche RDP Brute Forcing Attacken auf allen Systemen in Wazuh erkannt wird</p> <p>PS: Wir haben dies in der HL Übung gemacht.</p>	<p>Alle RDP Server müssen ihre Logs an Wazuh weiterleiten. Ohne diese Info ist es Wazuh nicht möglich, den Angriff zu erkennen.</p> <p>In der HL Übung wurde das RDP Log einiger Server noch nicht an Wazuh weiter geleitet.</p>	2

## 1.12 IP Blocklist (3 Punkte)

Der Spezialist von Wazuh und der Spezialist von MISP treffen sich in der Kaffee Pause. Sie tauschen sich aus. Dabei erzählen beide Spezialisten, dass Sie externe Quellen für ihr Tool einsetzen (IP Blacklist, IP-Reputation, Tor Exit Nodes, C2 Server Listen, Spam Listen, etc.)

Beide Spezialisten benutzten zum Teil die gleichen Feeds in MISP und Wazuh und zahlen natürlich auch doppelt (für die kostenpflichtigen Feeds)

Frage	Antwort	Punkte
Wofür zieht man in Wazuh oder MISP externe Quellen an?	<p><b>Grund 1</b> Externe Quellen helfen Unternehmen Erfahrungen von Dritten in ihre Analysen zu integrieren. So kann man beispielsweise über die TOR Exit Node Liste vergleichen, ob diese IP im eigenen Firmennetz in irgendeiner Form vorgekommen ist. Sei es in der Auswertung von Wazuh oder auch MISP.</p> <p><b>Grund 2</b> Austausch von KnowHow mit Dritten</p>	2
Beschreiben Sie eine Methode, mit welcher die Feeds nur noch 1x bezahlt werden müssen.	Das einfachste wäre es, wenn nur ein Tool die Feeds bezieht und dem anderen Tool als API anbietet. Falls das nicht möglich ist, dann könnte man ein System entwickeln das gegenüber dem Internet alle Feeds pollt und als API für Wazuh oder MISP bereitstellt.	1

### 1.13 Forensik (6 Punkte)

Ein Forensiker erstellt ein Memory Abbild von einem «kompromittierten» Windows 10 Client, auf dem man vermutet, dass ein Trojaner aktuell läuft. Sie bekommen das Memory Abbild und sollen es analysieren.

Frage	Antwort	Punkte
Mit welchem Tool analysieren Sie das Memory Abbild?	Volatility	1
Welche 5 Schritte unternehmen Sie, um das Abbild zu untersuchen?	<p>0 Hash/Checksumme prüfen</p> <p>1 Analyse OS Version des Images. Sicherstellen, dass man mit dem richtigen Image arbeitet</p> <p>2 Analyse der Prozesse. Durchsuchen nach auffälligen Prozessen wie svchost.exe</p> <p>3 Dumping von potenziell seltsamen Prozessen. Analyse des Inhaltes oder der Kommando Argumente</p> <p>4 Vergleich der gedumpten Prozesse mit VirusTotal oder ähnlich. Identifikation einer bekannten Malware</p> <p>5 Erstellung Bericht zuhanden Auftraggeber</p>	5


## 1.14 GPO (6 Punkte)

Im Rahmen des Unterrichtes haben Sie das Active Directory und die GPO (Group Policy Object) kennen gelernt.

Frage	Antwort	Punkte
Welche Voraussetzungen müssen auf einem Win10 Client erfüllt sein, damit man diesen über die GPO steuern kann? `	Win10 Client muss der AD Domäne hinzugefügt sein. Erst dann ist der Trust vorhanden, damit das AD mit dem System kommunizieren kann.	1
<p>Beschreiben Sie 5 notwendige Teilschritte die nötig sind, um via GPO den Wazuh Agent auf allen Windows Clients zu installieren.</p> <p>Das AD hat alle Clients in der Gruppe «ALL CLIENTS» gespeichert.</p>	<ol style="list-style-type: none"> <li>1) Copy Wazuh Agent auf SYSVOL</li> <li>2) Create GPO Scheduled Task für Installation Wazuh Agent. Der Scheduled Task nimmt den Wazuh Agent vom SYSVOL und installiert diesen lokal auf dem Win10 Client</li> <li>3) Link GPO Scheduled Task to Group "ALL CLIENTS"</li> <li>4) Run "gpupdate /force" on all Win Clients</li> <li>5) Testing, ob alle Clients als "registered device" in Wazuh ersichtlich sind</li> </ol>	5



### 1.15 SIGMA Rules (5 Punkte)

Frage	Antwort	Punkte
<p>Erklären Sie den Nutzen von SIGMA Rules</p> 	<p><b>Nutzen 1</b> SIGMA Rules beschreiben deklarativ Rules auf einer abstrakten Ebene. Diese kann man anschliessend in Kibana Rules, Splunk Rules oder auch andere ISMS System Rules konvertieren.</p> <p><b>Nutzen 2</b> Mit SIGMA umgeht man das Problem, dass jedes ISMS seine eigene Query Language hat und macht sozusagen abstrakte Rules.</p>	2

```

<{} win_susp_lsass_dump.yml x  win_susp_failed_logons_single_source.yml  win_susp_failed_logon_reas  🔍 📄 ⋮
1  title: Password Dumper Activity on LSASS
2  description: Detects process handle on LSASS process with certain access mask and object type SAM_DOMAIN
3  status: experimental
4  reference: https://twitter.com/jackcr/status/807385668833968128
5  logsource:
6    product: windows
7  detection:
8    selection:
9      EventLog: Security
10     EventID: 4656
11     ProcessName: 'C:\Windows\System32\lsass.exe'
12     AccessMask: '0x705'
13     ObjectType: 'SAM_DOMAIN'
14     condition: selection
15  falsepositives:
16    - Unkown
17  level: high
18

```

Frage	Antwort	Punkte
<p>Was kann der SOC Spezialist, der bei sich selbst Wazuh einsetzt mit obiger SIGMA Rule machen (Nutzen) und wofür ist die Rule?</p>	<p><b>Nutzen (1 Punkt)</b> Der SOC Spezialist kann die SIGMA Rule in eine Kibana Rule konvertieren und sie dann relativ einfach in Wazuh übernehmen.</p> <p><b>Erklärung Rule (2 Punkte)</b></p>	3

Frage	Antwort	Punkte
	Die Rule versucht zu erkennen, wenn jemand über den lsass.exe Prozess versucht Passwörter zu dumpen (z.B. Mimikatz)	

## 1.16 Advisory (6 Punkte)

Am 11.1.2022 wurde folgendes Advisory für WordPress veröffentlicht.

```
# Exploit Title: WordPress Core 5.8.2 - 'WP_Query' SQL Injection
# Date: 11/01/2022
# Exploit Author: Aryan Chehreghani
# Vendor Homepage: https://wordpress.org
# Software Link: https://wordpress.org/download/releases
# Version: < 5.8.3
# Tested on: Windows 10
# CVE : CVE-2022-21661

# [ VULNERABILITY DETAILS ] :

#This vulnerability allows remote attackers to disclose sensitive information on affected installations of WordPress Core,
#Authentication is not required to exploit this vulnerability, The specific flaw exists within the WP_Query class,
#The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries,
#An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise.

# [ References ] :

https://wordpress.org/news/category/releases
https://www.zerodayinitiative.com/advisories/ZDI-22-020
https://hackerone.com/reports/1378209

# [ Sample Request ] :

POST /wp-admin/admin-ajax.php HTTP/1.1
Host: localhost
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.99
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Cache-Control: max-age=0
Connection: close
Content-Type: application/x-www-form-urlencoded

action=<action_name>&nonce=a85a0c3bfa&query_vars={"tax_query":{"0":{"field":"term_taxonomy_id","terms":["<inject>"]}}}]
```

Frage	Antwort	Punkte
Was bedeutet CVE und was ist der Nutzen?	<p><b>Erklärung</b></p> <p>The mission of the CVE® Program is to identify, define, and catalogue publicly disclosed cybersecurity vulnerabilities.</p> <p>CVE = Common Vulnerabilities and Exposures.</p> <p><b>Nutzen</b></p> <p>Definierter Standard für die Diskussion und Austausch von Schwachstellen</p>	2

Frage	Antwort	Punkte
<p>Das SOC Team möchte in Wazuh erkennen, falls jemand den Exploit des Advisory ausprobiert.</p> <p>Was müssen Sie wie tun, damit man in Wazuh einen Alert von einem Angriffsversuch bekommt?</p>	<p>Das Log des WordPress Server müsste zuerst in Wazuh enthalten sein. Dies geschieht über den Wazuh Agent.</p> <p>Anschliessend geht es darum einen Alert für POST Requests an /wp-admin/admin-ajax.php zu erstellen. Da POST Daten meist nicht geloggt werden, wird ein Alert auf die Daten im Post Request wohl nicht ohne weiteres möglich sein.</p>	2
<p>Um welche Art von Angriff handelt es sich und wie kann sich das Unternehmen davor schützen?</p> <p>Begründen Sie Ihre Antwort. Abschalten des Systems gilt nicht als Lösung.</p>	<p><b>Art des Angriff</b> SQL Injection via POST</p> <ol style="list-style-type: none"> <li>1) Patching</li> <li>2) WAF Rule</li> </ol> <p><b>Begründung</b></p> <p>Könnte schwierig werden, weil POST Daten üblicherweise nicht geloggt werden. WAF können dies aber. Das Problem im Source Code beheben ist empfohlen.</p>	2

### 1.17 SSH Audit (6 Punkte)

Eine Firma hat viele SSH Services in der DMZ. Der Login ist nur mit SSH PubKey Auth erlaubt. Username/Passwort Auth ist überall deaktiviert. Die SSH Dienste werden auch von einer externen Firma für die IT-Support Unterstützung benutzt. Sie vertrauen aber dem externen Dienstleister nicht 100% und möchten die Aktivitäten des externen Dienstleisters überwachen. Sie wollen jeden Befehl sehen und protokollieren, welcher der externe Dienstleister via SSH auf ihren Systemen eingibt.

Frage	Antwort	Punkte
<p>Ein Mitarbeiter aus dem eigenen Unternehmen schlägt vor, hierfür den SSH MitM Docker zu verwenden, den Sie in der Übung kennen gelernt haben. Bewerten Sie diesen Lösungsansatz.</p> <p>Erklären Sie den Sachverhalt. Begründen Sie ihre Gedanken. Denken Sie auch an SSH Tunneling.</p>	<p><b>Erklärung Sachverhalt</b> SSH MitM nicht möglich, weil Mutual Auth dies nicht unterstützt. Ausser man würde beim SSH MitM den echten private Key des externen MA hinterlegen, damit er auf die anderen Systeme der DMZ jumpen kann. Dann würde der SSH MitM Host alle Befehle loggen.</p> <p><b>Begründung</b>  Dies könnte allenfalls durch den externen MA mittels SSH Tunneling umgangen werden.</p>	3
<p>Das Konzept mit dem SSH MitM ist in der Firma sehr umstritten. Man will das letztlich nicht.</p> <p>Erklären Sie ein Konzept, mit welchem Sie sämtliche SSH Befehle des externen Dienstleisters auf allen Systemen überwachen können (ohne SSH MitM Proxy)</p> <p>Ist sowas möglich? Begründen Sie Ihre Antwort.</p>	<p><b>Konzept</b>  Alle SSH Systeme, auf die der externe Mitarbeiter Zugriff hat, benötigt ein Logging der Kommandos. Ein Jumphost reicht nicht mehr aus</p> <p><b>Begründung</b>  Um die Strong Auth nicht aufzugeben</p>	3

### 1.18 NLA (6 Punkte)

Bei der RDP MitM Übung haben wir gesehen, dass RDP MitM mit aktiviertem NLA verhindert wird.

Frage	Antwort	Punkte
Erklären Sie auf Basis von kryptografischen Argumenten, warum NLA vor MitM schützt	<p><b>Erklärung</b></p> <p>RDP ist ein Challenge/Response Protokoll. Das Passwort wird nie übers Netz gesendet.</p> <p>Der Server schickt sein Server Zertifikat zum RDP Client, wo dieses mit dem Hash (User Passwort) verschlüsselt retourniert wird.</p> <p>Da der MitM den Hash des Passwortes nicht kennt (wegen Challenge Response), kann der MitM diese Response nicht berechnen und MitM wird erkannt.</p>	3
<p>Könnte die Methode von NLA nicht auch auf Form-based Authentisierungssysteme bei Web-Apps genutzt werden?</p> <p>Begründen Sie Ihre Antwort.</p>	<p>Nein, diese Prüfung müsste auf Stufe https Aufbau passieren, wo der Hash des Passwortes nicht bekannt ist.</p> <p>Mit <b>FIDO2</b> geht man aber in diese Richtung und dort ist es möglich.</p>	3

## 1.19 Large Scale (6 Punkte)

In einem Unternehmen mit 20'000 Windows Clients will man herausfinden, wer alles ein Tool gestartet hat, das einen bestimmten Registry Key schreibt (wie in der Übung SysInternals in die Registry)

Man könnte dies via GPO über ein PowerShell Script lösen. Das SOC Team nutzt jedoch eine SOAR Lösung für diesen Zweck.

Frage	Antwort	Punkte
Worin liegt der Unterschied zwischen einem SIEM und SOAR?	<p>1 SIEM ist basierend auf einem zentralen Logging. Ein Incident erscheint als Alert. Der Incident Reporter erhält ein Ticket und muss dann selbst schauen, wie er die weiterführenden Analysen macht</p> <p>2 SOAR ist eine Erweiterung von SIEM. Hier wird der Incident Responder dabei unterstützt Analysen zu machen, beispielsweise mittels Velociraptor.</p> <p>3 SIEM Systeme sind einfacher und kostengünstiger als SOAR – oft werden auf den Maschinene der End-User keine Agents installiert, was bei SOAR praktisch immer zum Einsatz kommt</p>	3
Welches SOAR System haben Sie während den HL Übungen kennen gelernt?	Velociraptor	1
Wie muss man mit SOAR Methoden vorgehen, um die Antwort auf die Frage zu erhalten, auf welchen Clients das Tool gelaufen ist. Annahme, ein SOAR Tool ist installiert.	<p>Velociraptor Query erstellen welcher den entsprechende Registry Key raussucht</p> <p>Velociraptor Query auf alle Win10 Clients anwenden</p>	2

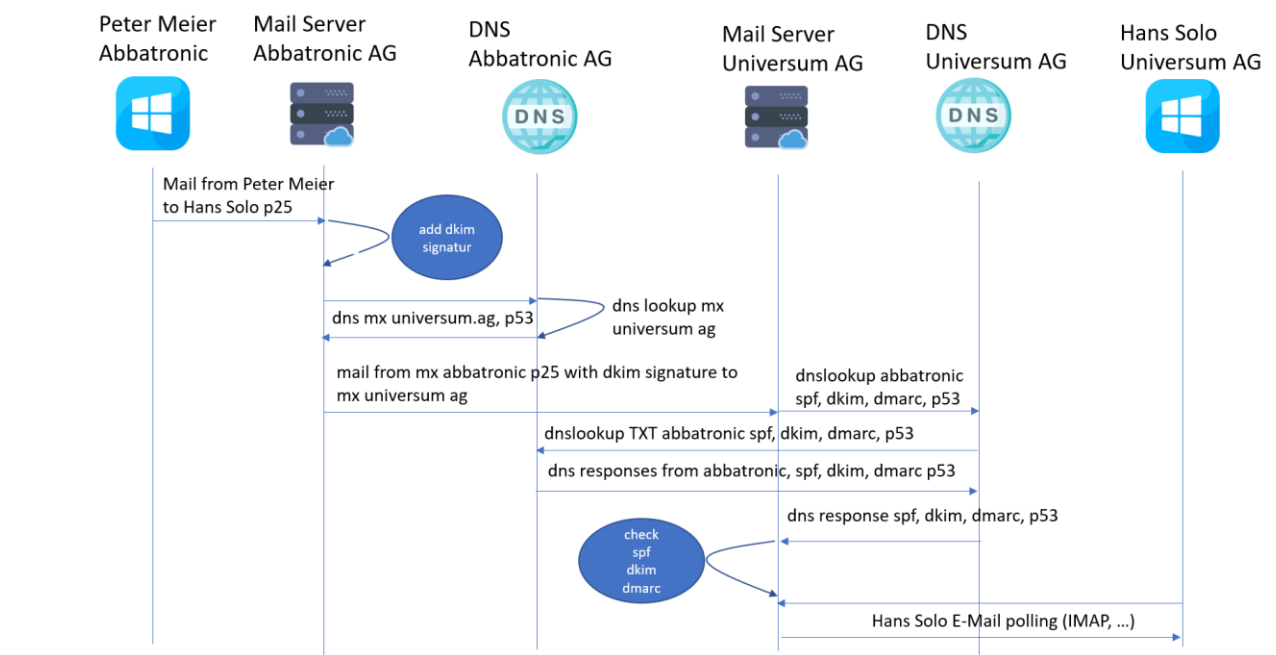
## 1.20 SPF/DKIM/DMARC (6 Punkte)

Peter Meier der Firma Abbatronic sendet von seinem PC via Mail Server von Abbatronic AG als [peter.meier@abbatronic.ch](mailto:peter.meier@abbatronic.ch) ein Mail an Hans Solo von Universum AG [hans.solo@universum.com](mailto:hans.solo@universum.com).

Zeichnen Sie in untenstehendes Diagramm ein, wie SPF, DKIM und DMARC angewendet wird in der Annahme, dass Sender und Empfänger SPF/DKIM und DMARC unterstützen. Zeichnen Sie folgende Protokolle ein

- SMTP
- DNS

Machen Sie Pfeile mit einer Richtung und beschriften Sie die Pfeile mit Protokoll





## 2 Anhang

### 2.1 Log4j Advisory

← → ↻ cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832 🔍 📄 ☆ 👤 ⋮

[Printer-Friendly View](#)

CVE-ID	
<b>CVE-2021-44832</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.	
References	
<p><b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</p> <ul style="list-style-type: none"><li>• CISCO:20211210 Vulnerabilities in Apache Log4j Library Affecting Cisco Products: December 2021</li><li>• URL:<a href="https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-gRuKNEbd">https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apache-log4j-gRuKNEbd</a></li><li>• CONFIRM:<a href="https://security.netapp.com/advisory/ntap-20220104-0001/">https://security.netapp.com/advisory/ntap-20220104-0001/</a></li><li>• CONFIRM:<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf">https://cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf</a></li><li>• URL:<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf">https://cert-portal.siemens.com/productcert/pdf/ssa-784507.pdf</a></li><li>• FEDORA:FEDORA-2021-1bd9151bab</li></ul>	