Oldenburgische
Industrie- und Handelskammer

Abschlussprüfung Winter 2025

Fachinformatiker Fachrichtung: Digitale Vernetzung

Dokumentation zu betrieblichen Projektarbeit

Automatisierter Prüfprozess

Einführung eines automatisierten Prüfprozesses mit dem SINEC Security Inspector zur Asset-Erfassung und Schwachstellen-analyse in Industrieanlagen

Abgabedatum: Oldenburg, den 02.12.2025

Prüfungsbewerber:

Lennard Valk

Musterstraße 11

12345 Musterstadt

Ausbildungsbetrieb:

Musterfirma GmbH

Musterstraße 14

12345 Musterstadt

MUSTERFIRMA

Inhaltsverzeichnis

Inhaltsverzeichnis I
Tabellenverzeichnis III
Abbildungsverzeichnis IV
Abkürzungsverzeichnis V
1. Einleitung i
1.1. Projektbeschreibung i
1.2. Projektziel i
1.3. Projektumfeld i
1.4. Projektbegründung i
1.5. Projektabgrenzung ii
2. Projektplanung ii
2.1. Projektphasen ii
2.2. Ressourcenplanung ii
2.3. Entwicklungsprozess iii
3. IST-Analyse (aktueller Zustand) iii
3.1. Prozess heute iii
3.2. Technische Ausgangslage iii
3.3. Schwächen & Risiken im IST-Zustand iv
4. SOLL-Konzept (Zielbild) iv
4.1. Zielsetzung & Umfang iv
4.2. Zielprozess iv
5. Wirtschaftlichkeitsanalyse v
5.1. Lösungs- und Angebotsübersicht (Kurzvergleich) v
5.2. Nutzwertanalyse vi
5.3. Entscheidung und Begründung vi
6. Entwurfsphase (Plan) vii
6.1. Zielarchitektur vii
6.2. Netz- und Zugriffskonzept vii
6.3. Scanprofile & Parametrierung vii
6.4. Daten- und Berichtskonzept viii
6.5. Anwendungsfälle viii
6.6. Qualitätssicherung viii
7. Implementierungsphase (Do) ix
7.1. Vorbereitung ix

7.1.1. VM-Bereitstellung ix
7.1.2. SSI-Installation & Grundkonfiguration ix
7.1.3. Targets anlegen ix
7.1.4. Test-Cases x
7.1.5. Test-Szenario anlegen x
7.1.6. Testdurchlauf x
7.2. Vollständiger Scan xi
7.3. Ergebnisse xi
8. Test- und Abnahmephase (Check) xi
8.1. Prüfpunkte und Abnahmekriterien (Compliant Scan) xi
9. Ergebnisphase (Act) xii
9.1. Standardberichte & Kommunikation xii
9.2. Maßnahmenableitung & Priorisierung xii
9.3. Vergleichsläufe xii
9.4. Ablage & Versionierung xiii
9.5. Freigabe xiii
10. Fazit xiii
10.1. Soll-/Ist-Vergleich xiii
10.2. Lessons Learned xiv
10.3. Ausblick xiv
Literaturverzeichnis xvi
Eidesstattliche Erklärung ..... **Fehler! Textmarke nicht definiert.**
Anhang xvii
A1. Ereignisgesteuerte Prozesskette (EPK) xvii
A2. Detaillierte Stundenaufschlüsselung xviii
A3. Verwendete Ressourcen xix
A4. Funktionsumfangsvergleich der Lösungsmöglichkeiten xx
A5. Nutzwertanalyse xxi
A6. Virtual Network Editor xxii
A7. Target-Liste xxiii
A8. Weboberfläche SSI - Test Result xxiv
A9. Ergebnisausschnitt des Result Checker xxv
A10. Baseline-Regeln xxvi
A11. Result Evaluation Vulnerabilities xxvi
A12. „Compliant“ Scan xxvii

Tabellenverzeichnis

Tabelle 1: Grobe Projektzeitplanung ii
Tabelle 2: Kurzversion Funktionsvergleich vi
Tabelle 3: Detaillierte Stundenaufschlüsselung xviii
Tabelle 4: Nutzwertanalyse xxi

Abbildungsverzeichnis

Abbildung 1: EPK des Zielprozesses xvii
Abbildung 2: Virtual Network Editor xxii
Abbildung 3: Ansicht Target-Liste xxiii
Abbildung 4: Weboberfläche SSI ProjektScan Übersicht xxiv
Abbildung 5: Weboberfläche SSI ProjektScan Results xxiv
Abbildung 6: Ergebnisausschnitt des Result Checker vor dem Re-Scan xxv
Abbildung 7: Ergebnisausschnitt des Result Checker vor dem Re-Scan 2 xxv
Abbildung 8: Whitelist für Benutzer xxvi
Abbildung 9: Whitelist für Schwachstellen xxvi
Abbildung 10: Übersicht gefundene Schwachstellen xxvi
Abbildung 11: Übersicht gefundene Schwachstellen nach Re-Check xxvi
Abbildung 12: Weboberfläche SSI ProjektScan (Re-Check) Übersicht xxvii
Abbildung 13: Ergebnisausschnitt des Result Checker nach Re-Scan „Compliant Scan“ xxvii
Abbildung 14: Ergebnisausschnitt des Result Checker nach Re-Scan „Compliant Scan“ xxviii

Abkürzungsverzeichnis

Asset	IT-System bzw. Komponente im OT-Netz
Asset-Erfassung	Automatisierte Inventarisierung inkl. Hersteller/Modell/System-Stände
Baseline	Definierter Soll- und Referenzzustand für Konfiguration und Sicherheitsniveau
BSI	Bundesamt für Sicherheit in der Informationstechnik
CE	Conformité Européenne (CE-Kennzeichnung gem. Maschinenverordnung)
CSV	Comma Separated Values
CVE	Common Vulnerabilities and Exposures (Schwachstellen-IDs)
CVSS	Common Vulnerability Scoring System (Bewertungsverfahren für CVEs)
EPK	Ereignisgesteuerte Prozesskette
Feeds	Automatisch geladene Schwachstellen- und Produktinformationen
HMI	Human-Machine Interface
ICS	Industrial Control Systems (OT-Steuerungstechnik).
IPC	Industrial PC (z. B. Siemens SIMATIC IPC)
IT	Informationstechnik
Management-NIC	Netzwerkschnittstelle der VM für Management-Zugriff und Feed-Aktualisierung
NAT	Network Address Translation (Management-Anbindung der VM)
NIC	Network Interface Card (Management-NIC / Scan-NIC).
OT	Operational Technology (Produktions-/Anlagen-IT, meist vom Internet getrennt).
PDCA	Plan/Do/Check/Act
PDF	Portable Document Format (Standard-Reportformat)
PSIRT	Product Security Incident Response Team (Hersteller-Security-Team/Advisories)
Scan-NIC	Netzwerkschnittstelle der VM in Richtung OT-Netz, über die die Scans laufen
SIMATIC IPC	Siemens Industrie PC
SSH	Secure Shell
SSI	SINEC Security Inspector (Siemens-Tool für Asset-/Vulnerability-Prüfungen)
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VM	Virtuelle Maschine
XLSX	Microsoft Excel Open XML Spreadsheet
YML	YAML Ain't Markup Language

1. Einleitung

1.1. Projektbeschreibung

Der Ausbildungsbetrieb Musterfirma GmbH entwickelt und liefert Automatisierungs- und Montageanlagen. In diesen Anlagen kommen unter anderem Siemens-Industrie-PCs (SIMATIC IPC) sowie Netzwerkinfrastruktur für OT-Netze zum Einsatz. Die IPCs werden zur Maschinensteuerung, Datenerfassung und Auswertung verwendet. Die automatisierten Anlagen sind auf hohe Präzision und Effizienz ausgelegt. Ausfallzeiten oder Angriffe jeglicher Art können für Kunden erhebliche finanzielle Verluste zur Folge haben. Sicherheitsprüfungen der Hard- und Software zur Prävention erfolgten bislang manuell, projektspezifisch und ohne einheitliche Dokumentation. Zusätzlich tritt im Januar 2027 die neue Maschinenverordnung (EU) 2023/1230 in Kraft, welche für Musterfirma GmbH essenziell ist.
In diesem Projekt soll ein standardisierter, reproduzierbarer Prüfprozess eingeführt werden, um Sicherheitsrisiken schon während der Entwicklung zu entdecken und zu minimieren, sowie die Kunden über mögliche Sicherheitslücken informieren zu können. Die Prüfungen, welche für das Projektes erfolgen, werden ausschließlich in der Vorabnahmephase der Anlage getätigt und beeinträchtigen den laufenden Betrieb nicht.

1.2. Projektziel

Ziel des Projektes ist es einen einheitlichen Prüfprozess für eine Pilotanlage zu entwickeln. Dieser soll die automatische Asset-Erfassung von Hard- und Software (Discovery, Ports/Services), eine Schwachstellenanalyse mit Priorisierung anhand CVSS im OT-Kontext, sowie die Erstellung standardisierter Ergebnisberichte umfassen. Die Prüfung soll später auf andere Anlagen transferierbar sein und als Baustein der Qualitätssicherung dienen.

1.3. Projektumfeld

Das Projekt ist im Bereich Engineering/IT/OT angesiedelt. Diese Abteilung übernimmt die Aufgabe der Einrichtung und Vorbereitung der IPCs, Firewalls etc. Die technische Umgebung besteht aus zellbasierten, vom Internet physisch getrennten OT-Netzen (airgapped) mit verschiedenen SIMATIC IPCs, InduSol-Switches und Cisco-Firewalls. Auf den IPCs kommen unter anderem Engineering- und Visualisierungssysteme, Mess- und Diagnosetools, Servicetools sowie Datenbanken und Auswertesoftware zum Einsatz. Für einen Testdurchlauf werden zwei IPCs einer Laboranlage, kurz nach Abschluss der Einrichtung, verwendet. Anschließend folgt ein Gesamtscan einer ausgewählten Pilotanlage, welche kurz vor der Übergabe steht.

1.4. Projektbegründung

Der automatisierte Prüfprozess senkt das Sicherheitsrisiko messbar: Schwachstellen und Angriffsflächen (z. B. offene Ports, unsichere Dienste, veraltete Softwarestände) werden

systematisch erkannt und priorisiert. Einheitliche Asset-Übersichten und standardisierte Berichte schaffen Transparenz und Nachvollziehbarkeit über alle Prüfungen und Anlagen hinweg. Die Ergebnisse sind vergleichbar und wiederholbar. Der Aufwand für Recherche und Kommunikation sinkt, da betroffene Anlagen, bzw. Komponenten schneller identifiziert, bewertet und adressiert werden können. Gleichzeitig entsteht eine belastbare Grundlage für wiederkehrende Prüfzyklen und einen skalierbaren Prozess, im Sinne der neuen Maschinenverordnung (EU) 2023/1230 sowie der IEC 62443 und damit für eine nachhaltige Verankerung in der Qualitätssicherung. Besonders im Bereich Hard- und Software ist es essentiell über potentielle Sicherheitsupdates so schnell wie möglich zu informieren und einen sicheren Ausgangspunkt nachweisen zu können.

1.5. Projektabgrenzung

Das Projekt beschränkt sich auf die Vorbereitung und Durchführung des Prüfprozesses an einer Pilotanlage. Ein Rollout auf weitere Anlagen ist nicht Bestandteil. Ebenso ist keine produktive Patch- oder Firmware-Verteilung enthalten. Es werden ausschließlich Maßnahmenempfehlungen dokumentiert. Ein unternehmensweites Cross-Plant-Impact-Assessment sowie die feste Prozessverankerung sind außerhalb des Projektrahmens.

2. Projektplanung

2.1. Projektphasen

Der Gesamtumfang beträgt 40 Stunden. Eine detaillierte Stundenaufschlüsselung der Teilaufgaben folgt im Anhang A2.

Phase	Aufwand
Ist-Analyse	5 h
Soll-Konzept & Wirtschaftlichkeitsanalyse	8 h
Planung & Entwurf	4 h
Installation & Pilotkonfiguration	9 h
Validierung & Ergebnisphase	7 h
Dokumentation	8 h
Gesamt	**40 h**

Tabelle 1: Grobe Projektzeitplanung

2.2. Ressourcenplanung

In Anhang A3 Verwendete Ressourcen auf Seite xix ist eine vollständige Aufstellung sämtlicher im Projekt eingesetzter Ressourcen enthalten.

2.3. Entwicklungsprozess

Für den Entwicklungsprozess wird ein inkrementelles Vorgehen nach PDCA (Plan/Do/Check/Act) gewählt. In der Planphase werden Zielarchitektur, Scan-Umfang, Scan-Profile, das Berichtskonzept sowie Maßnahmen zur Qualitätssicherung festgelegt. In der Do-Phase wird das Analysesystem aufgesetzt, zunächst ein Netzwerkscan durchgeführt und die Scantiefe schrittweise bis zur Schwachstellenerfassung erweitert. In der Check-Phase werden die Ergebnisse konsolidiert, „False Positives" bereinigt und die Betriebsrelevanz bewertet. In der Act-Phase entstehen Standardberichte. Außerdem werden priorisierte Maßnahmenempfehlungen formuliert und diese bei Bedarf eskaliert. Alle Artefakte werden mit Datum versioniert und abgelegt. Bei Bedarf erfolgen Vergleichsläufe (Re-Check), bzw. Neuprüfungen (Re-Scan).

3. IST-Analyse (aktueller Zustand)

3.1. Prozess heute

Sicherheitsprüfungen werden derzeit in erster Linie durch Hersteller-Hinweise (Security-Advisories) ausgelöst, insbesondere durch eigene Meldungen der PSIRTs von Lieferanten wie Siemens, Indu-Sol und Cisco. Als Eingangsquellen dessen dienen Hersteller-E-Mails, sowie die jeweiligen Portale der Hersteller. Ergänzend fließen persönliche Recherchen des Verantwortlichen für Electrical Engineering / Hardware-Design ein. Die Prüfung erfolgt ausschließlich manuell durch diese Person, eine Stellvertretungsregel ist nicht dokumentiert.

Der Ablauf gestaltet sich wie folgt: Nach dem Eingang einer Herstellermeldung wird deren Inhalt und Relevanz bewertet, etwa hinsichtlich der vorhandenen Internettrennung oder der konkret betroffenen Produktlinien. Anschließend erfolgt der Abgleich mit dem verbauten Bestand durch die händische Sichtung der PC-Datenblätter je Anlage. Ein abfrage- oder suchfähiger Gesamtüberblick über alle Anlagen steht nicht zur Verfügung. Auf der Basis der PC-Datenblätter werden betroffene Anlagen und Komponenten identifiziert, z. B. Switch-Typ, IPC-Modell oder auch Software- und Betriebssystemstände relevanter Systeme. Die Kunden werden, sofern erforderlich, per E-Mail über eine vorhandene Sicherheitslücke informiert. Gegebenenfalls wird ein Serviceauftrag mit Update oder Workaround erstellt und in ein geeignetes Wartungsfenster eingeplant. Ist die betroffene Anlage noch nicht an den Kunden übergeben, erfolgt die Umsetzung ad hoc, beim Kunden innerhalb des Wartungsfensters oder durch den Kunden selbst. Die Ergebnisartefakte bestehen aus PC-Datenblättern, Kunden-E-Mails und Serviceaufträgen. Nach aktuellem Stand besteht nach BSI keine Verpflichtung, dem Kunden eine Asset-Übersicht zu übergeben. Der Aufwand der Prüfung ist sehr hoch und variiert stark je nach Anzahl, Standort und Ausmaß betroffener Anlagen, sowie nach Umfang der Herstellerhinweise.

3.2. Technische Ausgangslage

Die OT-Netze sind logisch sowie physisch aufgeteilt und segmentiert und grundsätzlich vom Internet getrennt. Es kommen verschiedene SIMATIC IPC/HMI, industrielle Switche und Firewalls zum Einsatz. Softwareseitig sind typischerweise Engineering- und Visualisierungssysteme, Mess- und Diagnosetools, sowie Datenbanken und Auswertesoftware in Verwendung. Die Pflege des Überblicks über Geräte, Versionen und Services ist zeitaufwendig, weit

zerstreut und fehleranfällig.

3.3. Schwächen & Risiken im IST-Zustand

Die derzeitige manuelle Vorgehensweise ist nicht skalierbar und hängt stark von der verfügbaren Zeit und dem Wissen Einzelner ab. Durch die fehlende Automatisierung entstehen Blindstellen, sodass offene Ports, unsichere Dienste oder veraltete Versionen unentdeckt bleiben. Die Dokumentation ist uneinheitlich, wodurch Vergleichbarkeit und Wiederholbarkeit der Prüfungen nur eingeschränkt möglich sind. Es existiert keine zentrale, durchsuchbare Asset-Liste über alle Anlagen. Der Bestand liegt verteilt in PC- und Anlagendatenblättern. Der gesamte Prüfprozess ist abhängig von einer einzigen Person, sodass die Bearbeitung bei Urlaub oder Krankheit stillsteht. Ein automatisierter Abgleich gegen CVE/CVSS sowie BSI findet nicht statt. Die Bewertung stützt sich auf Herstellermeldungen, mit der Folge, dass das Risiko übersehener Schwachstellen erhöht ist. Die Relevanzbewertung erfolgt ad hoc und ohne dokumentierten Bewertungsleitfaden. Dokumentierte Nachverfolgung und Wissenstransfer erfolgen E-Mail-basiert, ohne feste Fristen und ohne definierten Eskalationsweg. Eine systematische Übertragung von Erkenntnissen auf andere Anlagen und ein verbindlicher Team-Wissensaustausch finden nicht statt. Insgesamt ist der Recherche- und Kommunikationsaufwand hoch. Die Umsetzung von Maßnahmen verursacht lange Durchlaufzeiten und entsprechend höhere Kosten.

4. SOLL-Konzept (Zielbild)

4.1. Zielsetzung & Umfang

Ziel ist ein wiederholbarer, möglichst automatisierter Prüf- und Dokumentationsprozess für OT-Anlagen, der alle eingesetzten Komponenten inventarisiert, den Sicherheitszustand objektiv bewertet und Ergebnisse standardisiert bereitstellt. Schwerpunkte sind in diesen OT-Netzwerken Windows-basierte IPCs, industrielle Switches, HMIs und zentrale OT-Server.
Im Projekt soll dieser Prozess entwickelt und eine Umsetzungsmöglichkeit erarbeitet werden, sowie die dokumentierte Durchführung an einer Pilotanlage erfolgen. Als Abschluss des Prozesses soll ein standardisierter Bericht vorbereitet und angelegt werden.

4.2. Zielprozess

Der Zielprozess sollte wie folgt aussehen:

1. Planung & Freigaben
   Zu Beginn werden Umfang und zu prüfende Anlagenteile festgelegt und ein Scantermin eingeplant. Hierfür soll in der Projektplanung ein ganzer Tag berücksichtigt werden. Dieser Termin liegt in der Regel kurz vor der Übergabe der Anlage an den Kunden.

2. Discovery & Inventarisierung
   Anschließend erfolgt der Discovery-Scan in den relevanten Ethernet-Segmenten. Dabei werden die Assets mit Hersteller, Modell und Firmwarestand erfasst.

3. Port- und Schwachstellenscan
   Darauf folgt der Port- und Schwachstellenscan, welcher geöffnete Ports, sowie Softwarestände erfasst und diese gegen bekannte Sicherheitslücken abgleicht. Für den Abgleich ist die Aktualität der Schwachstellendatenbank essenziell. Der Scan beeinflusst die geprüften Komponenten nicht und hinterlässt auch keine Rückstände.

4. Auswertung & Bewertung
   Die Ergebnisse werden konsolidiert (Geräte, Ports/Services, CVEs/CVSS). Auffälligkeiten und Änderungen werden hervorgehoben und mit der Baseline verglichen. Anschließend erfolgt die Bewertung der Betriebsrelevanz (z. B. Internettrennung, mögliche Angriffspfade), wie auch ggfs. die Bereinigung von „False Positives".

5. Maßnahmen
   Bei Handlungsbedarf erfolgt die Eintragung im Projekt Center und damit die Weitergabe an die Verantwortlichen (informelle Eskalation) um das gefundene „Problem" zu beheben. Gegebenenfalls wird das Team per Info-Mail informiert. Falls erforderlich wird der Scan erneut ausgeführt, um den Erfolg der Maßnahmen in einem Report ohne Auffälligkeiten zu dokumentieren.

6. Dokumentation & Ablage
   Zum Abschluss eines fehlerfreien Scans werden die Standardberichte erstellt, nach dem vorgegebenen Schema mit Datum abgelegt und der Meilenstein im Projekt Center als abgeschlossen vermerkt.

Im Anhang A1 Ereignisgesteuerte Prozesskette (EPK) auf Seite xvii ein Diagramm der ereignisgesteuerten Prozesskette (EKP) dieses Prozesses dargestellt.

5. Wirtschaftlichkeitsanalyse

Im Januar 2027 tritt die neue Maschinenrichtline Maschinenverordnung (EU) 2023/1230 in Kraft. Diese macht die Umsetzung des Projektes zwingend erforderlich. Ob die Realisierung mit z. B. dem Siemens SINEC Security Inspector aber auch aus wirtschaftlichen Gesichtspunkten gerechtfertigt ist, soll in den folgenden Abschnitten geklärt werden.

5.1. Lösungs- und Angebotsübersicht (Kurzvergleich)

Verschiedene Unternehmen bieten unterschiedliche Software an, mit welcher die geforderten Ziele erfüllt werden können. Im Folgenden werden die Funktionsumfänge unterschiedlicher Lösungsmöglichkeiten miteinander verglichen:

	SSI	**Framatome**	**AUVESY-MDT octoplant**	**Eigenentwicklung**
Inventarisierung	x			x
Port-Scan	x	x		x

Schwachstellenanalyse	x	x	x	x
Patch Deployment		x		x
Laufzeitüberwachung		x	x	x
Backup/Versionierung			x	x

Tabelle 2: Kurzversion Funktionsvergleich

Eine ausführliche Beschreibung der verschiedenen Lösungsmöglichkeiten ist im Anhang A4 Funktionsumfangsvergleich der Lösungsmöglichkeiten auf Seite xx aufgeführt.

5.2. Nutzwertanalyse

In Anhang A5 Nutzwertanalyse auf Seite xxi ist eine vollständig gewichtete Nutzwertanalyse der Lösungsansätze für das Projekt zu finden.

Die gewichtete Bewertung ergibt folgendes Ranking (Gesamtpunkte, max. 5,0):

- SSI: 4,3 - Rang 1
- Framatome: 3,6 - Rang 2
- Eigenentwicklung: 3,45 - Rang 3
- AUVESY-MDT octoplant: 2,55 - Rang 4

5.3. Entscheidung und Begründung

Entscheidung: Einsatz von Siemens SINEC Security Inspector (Basic + Nessus Add-on).

Begründung: SSI deckt Discovery, Port/Service-Scan, CVE-Abgleich, Konsolidierung sowie Standard-Berichte (PDF/XLSX) ab und erfüllt damit die Zielpassung mit prüffähiger Nachweisbarkeit. Framatome ist stark, wenn Patch-Management und Verteilung (PAR/PBA/Sentrigard) gefordert sind, bringt jedoch höheren Einstiegs-/Folgeaufwand und zusätzliche wiederkehrende Kosten mit. Octoplant ist für Backup/Versionierung exzellent, adressiert aber kontinuierliches Schwachstellen-Management nicht als Kern. Der Einführungs- und Betriebsaufwand ist bei SSI überschaubar (VM mit zwei NICs, eigenständige Einrichtung, automatische Software-Aktualisierungen). Wirtschaftlich erreicht SSI im Jahresvergleich den höchsten Nutzwert bei moderaten Kosten. Die Jahreslizenz erlaubt beliebig viele unterschiedliche Scans. Eine Eigenentwicklung ist zwar möglich, wäre für dieses Prüfungsprojekt jedoch zu aufwendig und risikobehaftet. Sie würde die Entwicklung und Bereitstellung eigener Feeds, Reporting, Prüfprotokolle und Exporte erfordern, sowie hohe Personal-/Pflegekapazitäten binden.

Fazit: SSI liefert die beste Zielabdeckung mit geringem Einführungsaufwand und erzeugt prüffähige Standardberichte. Für ein mögliches Folgeprojekt kann Framatome gezielt zur Patch-Automatisierung ergänzt werden. Octoplant bleibt Backup/Versionierungs-Baustein und ist damit von weniger Relevanz. Die Eigenentwicklung wird bewusst verworfen, um Projektrisiko und Pflegeaufwand zu begrenzen und die Anforderungen der Maschinenverordnung (EU) 2023/1230 rechtssicher und fristgerecht bedienen zu können.

6. Entwurfsphase (Plan)

6.1. Zielarchitektur

Die Lösung basiert auf einer dedizierten virtuellen Maschine mit zwei getrennten Netzwerkschnittstellen. Diese VM wird auf einer SSD gespeichert, um diese bei Bedarf leicht im Team teilen zu können. Der (eigene) Host-PC der VM stellt die Netzwerkschnittstelle ins Internet bereit, um Updates zu beziehen (Management-NIC) und eine zweite Schnittstelle (ggfs. USB zu Lan Adapter) ist an das Maschinennetz angeschlossen (Scan-NIC). Die Management-NIC dient ausschließlich der Schwachstellen und Feed-Aktualisierung des SINEC Security Inspector. Die Scan-NIC ist in das freigegebene OT-Segment bzw. Subnetz(en) der Pilotanlage angeschlossen und kann auch bei Bedarf mit mehrere IP-Adressen konfiguriert werden. Auf der VM wird der SINEC Security Inspector installiert und mit mindestens 4 CPU-Kernen, 16 GB RAM und 250 GB Speicher provisioniert. Zugriff und Bedienung des SSI erfolgt über ein Webinterface außerhalb der VM auf dem Host-PC. Auch die entstehenden Exporte können hierrüber heruntergeladen werden, um auf dem Firmenserver im Projektordner gesichert zu werden.

6.2. Netz- und Zugriffskonzept

Der Umfang der Scans ist auf die freigegebenen Subnetze der Pilotanlage begrenzt. Das jeweils genutzte Subnetz wird projektspezifisch eingetragen. Zur Abdeckung und Erreichung aller physischen Ethernet-Netze erfolgt der aufeinanderfolgende Anschluss an unterschiedliche Switche, sodass die physische Trennung gewahrt bleibt. Diese befinden sich teilweise in verschiedenen Schaltschränken. Die Aufteilung, sowie Verkabelung der unterschiedlichen Netze kann für jedes Projekt in dessen E-Plan nachvollzogen werden.

6.3. Scanprofile & Parametrierung

Für die Pilotanlage sowie den Prüfprozess werden grundlegend sechs Test-Cases definiert, die zusammen ein Test-Szenario ergeben. Ausgewählt wurden diese Test-Cases, um zum einen auf Netzwerkebene alle relevanten Aspekte abzudecken, als auch um auf Betriebssystemebene alle nötigen Informationen für einen Vergleich untereinander und für den Abgleich gegen bekannte Schwachstellen zu erhalten.

Zunächst führt der Test-Case „Asset and Vulnerability Discovery“ einen Netzwerkscan mit gängigen ICS-Protokollen durch. Dabei werden grundlegende Geräteinformationen ermittelt und bekannte Schwachstellen in Siemens-OT-Geräten erkannt. Im nächsten Schritt identifiziert der Port-Scan „Solution Port Scan“ mithilfe von Nmap alle erreichbaren Teilnehmer und deren geöffnete Ports, wobei der gesamte TCP-Bereich sowie ausgewählte UDP-Bereiche überprüft werden. Danach meldet sich das Modul „Discovery Scan (OS Enumerations)“ über die hinterlegten Zugangsdaten auf dem IPC an. So können Betriebssysteminformationen, installierte Programme sowie laufende Dienste und Prozesse ausgelesen werden. Anschließend vergleicht der „Vulnerability Scan (Nessus)“ die installierten Softwareversionen mit aktuellen CVE- und CVSS-Feeds und meldet mögliche Schwachstellen. Nachdem diese

fachlichen Scans abgeschlossen sind, sorgt das Bereinigungsmodul „Test Case Utils Target Cleanup“ dafür, dass keine temporären Dateien oder Konfigurationen auf den Zielsystemen verbleiben. So wird versichert, dass die Umgebung in den Ausgangszustand zurückkehrt. Zum Schluss fasst der „Result Checker (Security Inspector Check)“ alle Befunde zusammen, vergleicht sie mit einer definierten Baseline oder einer Liste zulässiger Schwachstellen und offener Ports und erstellt einen strukturierten Bericht im XLSX- und PDF-Format.

6.4. Daten- und Berichtskonzept

Berichte und Logs der einzelnen Test-Cases, sowie die des Result Checkers werden in einer ZIP-Datei verpackt. Der Result Checker listet die Ergebnisse aller Test-Cases in einer Report-XLSX-Datei vergleichbar auf und wertet diese ggfs. gegen eine Baseline aus. Die Asset-Liste aus diesem Report enthält die jeweilige IP-Adresse, MAC-Adresse, Hostname, Betriebssystem und Version, vorhandene Benutzerkonten, Laufwerke, sowie deren Freigaben, geöffnete Ports, installierte Programme, laufende Dienste und Prozesse, sowie Netzwerkschnittstellen und gespeicherte Routen. Der Vulnerability-Test-Case deckt anschließend unter anderem mithilfe der gesammelten Ergebnisse mögliche Sicherheitslücken auf, indem er die geöffneten Ports und Softwareversionen gegen bekannte Sicherheitslücken abgleicht. Diese Ergebnisse umfassen dann den Host-Bezug, die CVE-ID, den CVSS-Basiswert, den betroffenen Dienst/Port/Protokoll und eine Kurzbeschreibung. Zuletzt werden diese Ergebnisse nach CVSS-Basiswert sortiert.

Die Logs liegen standardmäßig in der ZIP-Datei des vollen Exports vor und unterstützen bei Bedarf die Nachvollziehbarkeit vergangener Scans. Ablage und Versionierung der Sammlung aller Ergebnisse erfolgen im Projektordner nach festgelegtem Benennungsschema.

6.5. Anwendungsfälle

Der Prüfprozess vor der Übergabe (Pre-Shipment-Prüfung) an den Kunden ist fester Bestandteil eines Projektes und liefert mithilfe des Berichtes einen wichtigen Teil der Qualitätssicherung und Dokumentation. Er ist außerdem mit Blick auf die neue Maschinenverordnung (EU) 2023/1230 für die CE-Zertifizierung relevant.

Bei z. B. herstellerseitigen Advisories werden gezielte Re-Scans der betroffenen Segmente durchgeführt. In Gewährleistungsfällen ist dies auch für bereits übergebene Anlagen wichtig. Darüber hinaus kann auf Kundenwunsch in einem Wartungsfenster ein Vollscan als Dienstleistung erfolgen, welcher dann einen eindeutigen Vergleich gegenüber einem vorherigen Scan ermöglicht.

6.6. Qualitätssicherung

Der erste Vollscan dient als Baseline. Abweichungen werden in Folgescans oder -prüfungen (Re-Scan oder Re-Check) mit dem Result Checker hervorgehoben. Der Re-Check wird so oft wiederholt, bis ein konformer (compliant) Scan vorliegt. Das False-Positive-Handling und das Whitelisting von Schwachstellen erfolgen ausschließlich begründet und wird im Ergebnis

des Result Checkers dokumentiert. Stichprobenartige manuelle Verifikationen sichern zudem die Ergebnisqualität.

7. Implementierungsphase (Do)

7.1. Vorbereitung

7.1.1. VM-Bereitstellung

Für den Betrieb wird eine virtuelle Maschine mit VM-Ware aufgesetzt. Im Virtual Network Editor (Abbildung 2: Virtual Network Editor) wird ein zusätzlicher Netzwerkadapter angelegt, der später auf den USB-zu-LAN-Adapter, welcher an der Anlage angeschlossen ist, gebrückt wird. Ein zweiter Adapter wird als NAT-Schnittstelle für das Management konfiguriert. Anschließend erfolgt die Standardinstallation von Debian. Während der Installation wird der Benutzer „admin-user“ angelegt, außerdem werden die Debian Standard Systemwerkzeuge und der Open-SSH-Server installiert und das System anschließend zur Übernahme der Änderungen neu gestartet.

7.1.2. SSI-Installation & Grundkonfiguration

Die Ersteinrichtung beginnt mit der Anmeldung als root. Es wird „sudo“ installiert und der „admin-user“ der sudo-Gruppe zugewiesen. Das Installationsskript (*install.sh*) wird per SSH auf die VM übertragen und ausgeführt. Nach Abschluss folgt ein Neustart. Die Konsole zeigt anschließend die Adresse des Web-Interfaces an. Für den ersten Login werden die initialen Zugangsdaten auf dem Server via SSH mit dem Befehl „*sudo cat /opt/siesta/webcc_data/credentials.txt“* ausgelesen und im Web-Client verwendet, woraufhin direkt das Anlegen eines neuen Benutzers verlangt wird. Danach wird der First-Time-Wizard durchlaufen und Zeit, Lizenz sowie Updates werden heruntergeladen und konfiguriert. Die Lizenzvalidierung erfolgt über die von Siemens bereitgestellte Provisioning-Datei. Die Rollen User, Admin, ReadOnly, und Backup sind grundsätzlich verfügbar. Im Umfeld der Musterfirma GmbH wird aufgrund der sehr geringen Nutzerzahl jedoch nur der Admin-Benutzer verwendet. Abschließend wird über den Network-Setup-Wizard der zuvor konfigurierten Scan-NIC ein Netzwerkprofil im SSI zugeordnet.

7.1.3. Targets anlegen

Die Zielsysteme (Targets) können per CSV/YMLimportiert oder manuell angelegt werden. Ein Target kann entweder ein Gerät (z. B. 192.168.XXX.XXX) oder ein Subnetz (z. B. 192.168.XXX.0/24) sein. Pro Zielsystem werden Name, IP-Adresse, Netzwerkprofil und, falls erforderlich, Target-Attribute gepflegt. Target-Attribute sind Parameter, wie Anmeldedaten o.ä. welche dann bei einem Scan zur Verfügung stehen. Alternativ steht der „Automated Target Detection Wizard“ zur Verfügung, mit dem ein Subnetz automatisch nach verfügbaren

Zielsystemen durchsucht werden kann. In der Weboberfläche des SSI tauchen diese dann in einer Liste auf (siehe Abbildung 3: Ansicht Target-Liste).

7.1.4. Test-Cases

Die mitgelieferten Testfälle werden initial importiert bzw. heruntergeladen. Für den Prüfprozess wurden folgende Test-Cases ausgewählt, um alle relevanten Aspekte erfassen zu können:

- Test 1 - Asset and Vulnerability Discovery (OT Scanner): Netzwerk und Port-Scan mit dem SiESTA OT Scanner von Siemens
- Test 2 - Solution Port Scan (Nmap, all TCP ports, common UDP ports): Kurz- und Vollcheck von UDP oder TCP-Bereichen mithilfe von Nmap
- Test 3 - Discovery Scan (OS Enumerations): Erfasst detallierte genutze Benutzerkonten, installierte Programme, usw.
- Test 4 - Vulnerability Scan (Nessus): Führt einen erweiterten Nessus-Schwachstellen-Scan und -Abgleich durch
- Test 5 - Test Case Utils Target Cleanup: ggfs. Aufräumen von Überbleibseln bei abgebrochenen Tests
- Test 6 - Result Checker (Security Inspector Check): Abgleich mit Baseline, bzw. zugelassenen Sicherheitslücken und offenen Ports, sowie Berichtserstellung

7.1.5. Test-Szenario anlegen

Es wird ein Test-Szenario erstellt, das eine Kombination aus einem oder mehreren Targets, einem oder mehreren Test-Cases sowie dem Result Checker bildet, um standardisierte und wiederholbare Ausführungen zu ermöglichen. In unserem Fall wird das entsprechende Subnetz mit den oben genannten Cases zu einem Szenario gebündelt. Über „Test Szenario Attributes“ (TSAs) werden globale Parameter für alle Targets gesetzt, wie z. B. die Windows-Zugangsdaten für authentifizierte Prüfungen. Die Zugangsdaten erscheinen nicht in Berichten und sind nur für IT/OT-Administratoren sichtbar. Eine wiederkehrende, automatische Ausführung ist grundsätzlich möglich, ist für unseren Anwendungsfall aber nicht relevant.

7.1.6. Testdurchlauf

Im Labor wird ein kleiner, repräsentativer Test mit nur einem Host durchgeführt, um die Konfiguration zu bestätigen und einen erfolgreichen Ablauf des Tests auf der Pilotanlage sicherzustellen. Dabei werden Erreichbarkeit, Laufzeit, Logging und die Berichtserstellung verifiziert. Das Zusatzmodul „Test Case Utils Target Cleanup“ sorgt zuletzt dafür, dass keine Testartefakte verbleiben.
Dieser Testdurchlauf hat gezeigt, dass im Projekt die Domain für die Windowsanmeldung in

den Target Attributes noch auf „WORKGROUP“ festgelegt werden muss, um ein erfolgreiches Scannen des Betriebssystems zu ermöglichen.

7.2. Vollständiger Scan

Der Vollscan an der Pilotanlage erfolgt im freigegebenen Wartungsfenster kurz vor der Übergabe. Er umfasst alle relevanten Subnetze und basiert auf dem vorbereiteten Szenario mit hinterlegten Zugangsdaten und Result Checker. Falls dies nicht bekannt ist, können zuvor mithilfe des E-Plans der Pilotanlage die verschiedenen, teilweise physisch getrennten, Subnetze und deren Anschlüsse nachgeschaut werden. An der Anlage wird nach dem Anstecken an einen Netzwerk-Switch im Schaltschrank zunächst die Erreichbarkeit eines Teilnehmers mithilfe eines Pings geprüft, um so die eingestellte Netzwerkkonfiguration zu bestätigen. Da der Scan einige Stunden in Anspruch nehmen kann, muss die Stromversorgung des Host-PCs gewährleistet sein. Abschließend kann das zuvor konfigurierte Scan-Szenario gestartet werden.
Der Scan an der Pilotanlage wurde am 12.11.2025 um 15:55 Uhr gestartet und nach 103 Minuten beendet (siehe Abbildung 4: Weboberfläche SSI ProjektScan Übersicht und Abbildung 5: Weboberfläche SSI ProjektScan Results).
Im Folgenden wird beispielhaft stets der Scan des 192.168.213.0/24 Netzes betrachtet. Der Scan wurde identisch auch in den anderen verfügbaren Netzen durchgeführt, wird hier aber aus Gründen des Gesamtumfangs nicht aufgeführt.

7.3. Ergebnisse

Nach Abschluss werden die Standardberichte sowie die Scan-Logs, mit deren Hilfe der Scan jederzeit nachvollzogen werden kann, erzeugt, exportiert und strukturiert abgelegt. Dabei werden auch die gefundenen Schwachstellen systematisch aufgelistet. Da der Erst-Scan ohne Baseline erfolgte, lautet das Ergebnis „Not Compliant“ (siehe Abbildung 6: Ergebnisausschnitt des Result Checker vor dem Re-Scan, Abbildung 7: Ergebnisausschnitt des Result Checker vor dem Re-Scan 2 und Abbildung 10: Übersicht gefundene Schwachstellen).

8. Test- und Abnahmephase (Check)

8.1. Prüfpunkte und Abnahmekriterien (Compliant Scan)

Die entstandenen Ergebnisse sind zu prüfen und begründet zu bestätigen, bevor ein Re-Check zur Erlangung eines „Compliant“-Status durchgeführt werden kann. Für eine erfolgreiche Prüfung (Compliant Scan) wird zuallererst verifiziert, dass alle Test-Cases sowie der Result Checker erfolgreich abgeschlossen wurden (siehe Abbildung 5: Weboberfläche SSI ProjektScan Results). Die entstandenen Asset Listen werden auf Plausibilität geprüft, stichprobenartig mit Systemdaten abgeglichen. Bei Unklarheiten werden einzelne Hosts oder Segmente gezielt erneut gescannt. Zum Abschluss der Qualitätsprüfung werden die Ergebnisse begründet verifiziert, kommentiert und bereinigt. Es kann vorkommen, dass bestimmte Funde bzw. Schwachstellen aufgrund der Installationsweise oder Internet-Trennung nicht relevant für die Anlage sind („False Positives“). Diese können mit einer entsprechenden

Begründung bereinigt, also in die Whitelist aufgenommen, werden (siehe Abbildung 8: Whitelist für Benutzer und Abbildung 9: Whitelist für Schwachstellen). Die im betrachteten Subnetz gefunden Schwachstellen wurden in Absprache mit dem IT-/OT-Integrator als irrelevant eingestuft. Ein „compliant“ Scan liegt erst vor, wenn der Result Checker, ggfs. bei einem Re-Check, keine unbegründeten Funde oder Konfigurationen mehr feststellt (siehe Abbildung 11: Übersicht gefundene Schwachstellen nach Re-Check).

9. Ergebnisphase (Act)

9.1. Standardberichte & Kommunikation

Die Berichte des Result Checker wurden erfolgreich erstellt und abgelegt. Alle irrelevanten Ergebnisse („False Positives“) wurden begründet bereinigt und ggfs. wurden Maßnahmen, wie z. B. Softwareaktualisierungen an die zuständigen Personen eskaliert. Außerdem hat ein Teamaustausch in Form einer Rundmail stattgefunden.

9.2. Maßnahmenableitung & Priorisierung

Nachdem die Ergebnisse nach Kritikalität und Betriebsrelevanz priorisiert wurden, werden die kritische Punkte unmittelbar im Projekt Center als Action Item erfasst, einschließlich betroffener Systeme, verantwortlicher Personen, Umsetzungsfrist und eines Termins für die Gegenprüfung (Re-Scan nach Umsetzung). Bei Fristüberschreitung oder kritisch dringender Betriebsrelevanz erfolgt eine direkte Eskalation an die Projektleitung. Zudem ist der regelmäßiger Wissensaustausch im Team obligatorisch für eine produktive Zusammenarbeit. Im betrachteten Subnetz waren nach der Besprechung mit dem zuständige IT-/OT-Integrator keine weiteren Maßnahmen erforderlich.

9.3. Vergleichsläufe

Die entstehenden Maßnahmen aus den Ergebnissen des Result Checker können sehr verschieden ausfallen. Oftmals reicht eine Softwareaktualisierung oder geänderte Rechteverwaltung aus. Nach Umsetzung der Maßnahmen wird ein gezielter Folgescan (Re-Scan) durchgeführt. Sollten nur Anpassungen der Baseline (Whitelists) nötig sein, ist der Re-Check ausreichend. Der Result Checker erstellt einen Vergleich zwischen vorherigem und aktuellem Stand. Die Abschlussmeldung im Projekt Center erfolgt erst nach einem nachweislich erfolgreichen „compliant“ Folgescan.
Da im betrachteten Subnetz keine Maßnahmen erforderlich waren wurde statt des Re-Scans ein Re-Check durchgeführt. Dieser lieferte den geforderten „complaint“ Scan (siehe Abbildung 12: Weboberfläche SSI ProjektScan (Re-Check) Übersicht, Abbildung 13: Ergebnisausschnitt des Result Checker nach Re-Scan „Compliant Scan“ und Abbildung 14: Ergebnisausschnitt des Result Checker nach Re-Scan „Compliant Scan“).

9.4. Ablage & Versionierung

Die vollständigen Ergebnisse werden strukturiert abgelegt. Dazu gehören die Berichte und Exporte mit Datum/Version einheitlich gemäß dem vorgegebenen Schema. Dieses sieht wie folgt aus: *JJJJ-MM-TT_Anlage_Umfang_Version*. Die auf Basis der Whitelists erstelle Baseline wird mit betroffenen Subnetzten markiert, mit Datum versioniert und abteilungsintern abgelegt, sodass Veränderungen nachvollziehbar bleiben.

Im Fall der Pilotanlage werden de Artefakte unter folgendem Pfad abgelegt:
XXXXX\40_SSI\2025-11-13_20349_213_V1.zip

Der Re-Scan mit „compliant“ Scan liegt unter:
XXXXX\40_SSI\2025-11-13_20349_213_V2.zip

Die erstellte Baseline wird abteilungsintern auf dem geteilten Dateiserver abgelegt:
\\XXXXXX\Programme\Siemens\SSI\Baseline_213_2025-11-13.xlsx

9.5. Freigabe

Die Freigabe für die Anlage erfolgt im Projekt Center durch den IT-/OT-Administrator und wird mit Datum und Version dokumentiert, sobald ein „compliant“ Scan durchgeführt wurde. Mit dieser Freigabe ist ein Meilenstein im Kundenprojekt erreicht.

10. Fazit

Im Projekt wurde ein einheitlicher, wiederholbarer Prüfprozess für OT-Anlagen entwickelt, technisch umgesetzt und an einer Pilotanlage produktionsnah erprobt. Der SINEC Security Inspector dient dabei als zentrale Plattform für Asset-Erfassung, Schwachstellenanalyse und die Erstellung standardisierter Berichte. Das im Anhang A1 dargestellte Prozessdiagramm fasst den Zielprozess grafisch zusammen und bildet die Grundlage für einen Standard in der Qualitätssicherung der Maschinen der Musterfirma GmbH.

10.1. Soll-/Ist-Vergleich

Ausgangspunkt war ein sehr aufwendiger und personenabhängiger Prüfprozess ohne Asset-Übersicht und ohne Schwachstellenanalyse. Schwachstellen wurden hauptsächlich anhand einzelner Hersteller-Advisories erkannt und bewertet.
Mit dem im Projekt entwickelten Zielprozess wird die Erfassung systematisiert und die Sicherheit der Anlagen mit angemessenem Aufwand verbessert. Es liegt nun eine definierte Zielarchitektur auf Basis einer virtuellen Maschine mit getrennten Management- und Scan-Schnittstellen vor. Die einzelnen Prozessschritte werden entlang des PDCA-Zyklus beschrieben. Sie beginnen mit der Definition des Umfangs und, falls erforderlich, der Terminplanung von Wartungsfenstern. Anschließend folgen die Durchführung von Discovery- und

Schwachstellenscans sowie die Auswertung der Ergebnisse und die strukturierte Ablage der Berichte. Die Ergebnisse werden automatisiert erfasst, mit aktuellen Feeds abgeglichen und über den Result Checker konsolidiert. Ein standardisiertes Berichtskonzept mit Baseline und Folgescan ermöglicht eine nachvollziehbare Bewertung von Schwachstellen und bei Bedarf einen Vergleich zwischen mehreren Scans. Zusätzlich wurde eine feste Ablagestruktur mit Versionierung und Verknüpfung zum Projekt Center definiert, sodass die Ergebnisse für spätere Prüfungen vergleichbar bleiben.
Im Pilotprojekt wurde der Zielprozess an einer realen Anlage durchgespielt. Beginnend mit einem Vollscan, der Bewertung der Findings und Priorisierung nach Relevanz bis hin zur Ableitung von Maßnahmen und der Ablage der Standardberichte.
Das im Projektantrag formulierte Ziel, einen automatisierten Prüfprozess zu entwickeln, in einer Pilotanlage zu erproben und standardisierte Ergebnisberichte bereitzustellen, kann damit als erreicht angesehen werden. Relevante Abweichungen vom genehmigten Projektantrag traten nicht auf. Themen wie ein unternehmensweiter Rollout auf alle relevanten Anlagen oder eine umfassende Kopplung an Patch- und Backup-Lösungen wurden bewusst nicht umgesetzt, da sie den zeitlichen Rahmen der Projektarbeit überschreiten würden. Sie bilden jedoch sinnvolle nächste Ausbaustufen.

10.2. Lessons Learned

Im Verlauf des Projekts hat sich gezeigt, dass sowohl technische als auch organisatorische Aspekte entscheidend für einen belastbaren Prüfprozess sind. Auf technischer Seite war insbesondere die saubere Trennung von Management- und Scan-Netz wichtig, um die Sicherheit der Umgebung zu gewährleisten und gleichzeitig aussagekräftige Ergebnisse zu erhalten. Ebenso hat sich die korrekte Auswahl der Test-Cases als kritisch erwiesen, da hier die Balance zwischen Scan-Tiefe, Schonung der produktiven Systeme und verfügbaren Wartungsfenstern gefunden werden musste. Ein weiterer zentraler Punkt war die Sicherstellung aktueller Feeds für CVEs und Security-Advisories, da die Aussagekraft der Scans direkt von der Aktualität dieser Daten abhängt.
Organisatorisch wurde deutlich, dass eine frühzeitige und enge Abstimmung mit IT- und OT-Beteiligten notwendig ist, um Umfang, Wartungsfenster und Verantwortlichkeiten verbindlich festzulegen. Die Einführung einer einheitlichen Ablagestruktur mit definierten Pfaden, Dateinamen und Versionierung hat sich als wichtiger Faktor für die Nachvollziehbarkeit erwiesen.
Im Rahmen der Wirtschaftlichkeitsbetrachtung hat es sich bestätigt, dass der gewählte Ansatz mit SINEC Security Inspector ein sinnvolles Verhältnis aus Funktionsumfang, Einführungsaufwand und laufenden Kosten bietet. Die Nutzwertanalyse zeigt, dass SSI im direkten Vergleich zu Alternativen wie Framatome, octoplant oder einer Eigenentwicklung den höchsten Gesamtnutzwert erreicht, ohne den Projektumfang zu sprengen. Damit ist die Entscheidung für SSI im Kontext der Pilotanlage fachlich und wirtschaftlich nachvollziehbar.

10.3. Ausblick

Auf Basis der im Pilotprojekt gewonnenen Erfahrungen bietet sich als nächster Schritt ein geplanter Rollout des Prüfprozesses auf weitere Anlagen an. Die erarbeiteten Test-Szenarien, Konfigurationen und Berichtsformate können dabei weitgehend wiederverwendet und bei Bedarf schrittweise angepasst werden. Ziel ist eine zentrale, durchsuchbare Übersicht über

Assets und Schwachstellen aller relevanten OT-Zellen, um Wiederholprüfungen und Vergleiche über die Zeit zu ermöglichen.

Zukünftig eröffnet die Nutzung der REST-Schnittstellen des SINEC Security Inspector weitere Möglichkeiten zur Automatisierung. Denkbar sind beispielsweise geplante Folgescans, eine automatisierte Report-Ablage oder die direkte Erstellung von Aufgaben und Maßnahmen im Projekt Center auf Basis der Ergebnisse. Auf diese Weise könnte der im Rahmen dieser Projektarbeit etablierte Prüfprozess von einer pilotierten Lösung hin zu einem festen Baustein der Qualitätssicherung weiterentwickelt werden, ohne den Betrieb der Anlagen mehr als nötig zu beeinträchtigen.

Literaturverzeichnis

- Siemens AG: **SINEC Security Inspector - Operating Instructions.** Doku-Nr. C79000-G8976-C701-04, Version 05/2025.
- Siemens AG: **Security settings for Siemens IPCs (Windows 10).** Beitrags-ID 109475014, 2019.
- Siemens AG: **Angebot Nr. XXXXXX - SINEC Security Inspector 2025.** Angebot vom 24.02.2025.
- AUVESY-MDT: **octoplant.** Angebot vom 03.11.2025.
- Framatome: **Proposal for Vulnerability and Patch Management.** Version 20240708_01_IBCY, vom 08.07.2024.
- IHK: **Handreichung / Leitfaden zur Abschlussprüfung - IT-Berufe (Projektarbeit / Dokumentation).** Stand: 07.02.2025.
- dieperfekteprojektdokumentation.de: **Vorlage Projektdokumentation IT-Berufe.** Online verfügbar unter: https://dieperfekteprojektdokumentation.de/MicrosoftWord_Vorlage_Projektdokumentation_ITBerufe.pdf, Abruf am 02.12.2025.
- Europäische Union: **Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates über Maschinenprodukte (Maschinenverordnung).** In: Amtsblatt der Europäischen Union, L 165/1 vom 29.06.2023. Online verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32023R1230, Abruf am 08.11.2025.

Anhang

A1. Ereignisgesteuerte Prozesskette (EPK)

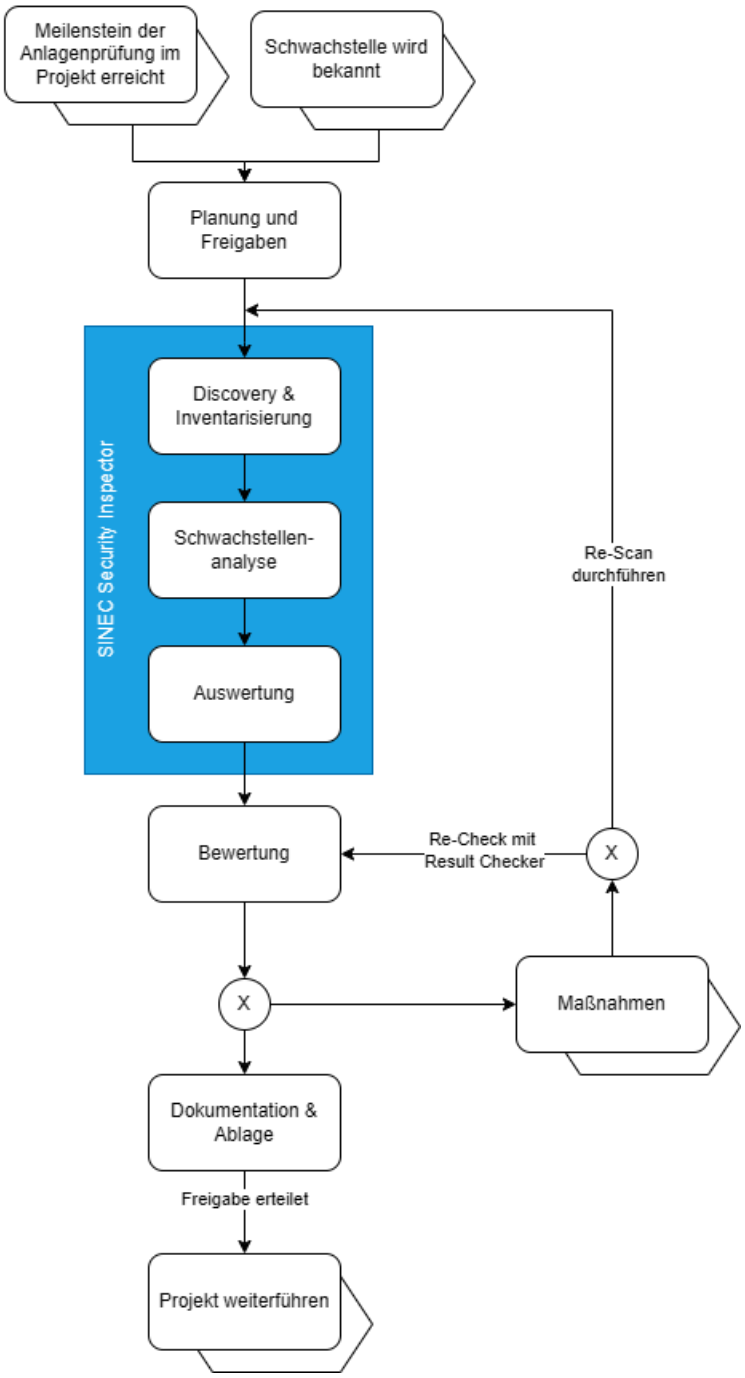


Abbildung 1: EPK des Zielprozesses

A2. Detaillierte Stundenaufschlüsselung

Phase	Aufwand
Ist-Analyse	**5 h**
Ist-Analyse durchführen	3 h
Aktuelle Prozesse bewerten	2 h
Soll-Konzept & Wirtschaftlichkeitsanalyse	**8 h**
Entwicklung des Zielprozesses	2 h
Klärung des Prüfumfangs und relevanter **Asset**s	2 h
Alternative Prüfprogramme bewertet vergleichen	4 h
Planung & Entwurf	**4 h**
Scan Umfang festlegen und Test Cases nach Bedarf auswählen	2 h
Berichtskonzept definieren	2 h
Installation & Pilotkonfiguration	**9 h**
Installation des SSI auf einer VM	3 h
Durchführung Testdurchlauf	2 h
Durchführung Vollscan der Pilotanlage	4 h
Validierung & Ergebnisphase	**7 h**
Erstellung, Prüfung und Ablage der Ergebnisse des Vollscans	4 h
Bereinigung, ReCheck und Freigabe der Ergebnisse	3 h
Dokumentation	**8 h**
Erstellung der Projektdokumentation	8 h
Gesamt	**40h**

Tabelle 3: Detaillierte Stundenaufschlüsselung

A3. Verwendete Ressourcen

Personen

- IT-Integrator: Festlegung der Anforderungen und Abnahme des Projektes
- OT-/IT-Team: Freigaben und fachliche Rückfragen

Sachmittel

- Hardware: Laptop, SSD, Netzwerkkabel, USB-Netzwerkadapter
- Software: Windows 11, Debian GNU/Linux, Jahreslizenz für SINEC Security Inspector, VM-Ware, PDF-Viewer Microsoft 365

Rahmenbedingungen

- Keine ausgehende Internetverbindung aus der Anlage, Aktualisierungen nur über Management-NIC, Scan-NIC
- Alle IT/OT-Elemente sind in der Anlage abgeschlossen
- Keine der Anlagen ist in Produktion
- Zugänge: Physische Zugänge möglich, Netzwerkzugang über verschlossenen Schaltschrank

A4. Funktionsumfangsvergleich der Lösungsmöglichkeiten

Option 1 - Siemens SINEC Security Inspector (SSI)
Leistungsumfang: OT-Asset-Discovery, Port/Service-Erkennung, Schwachstellenanalyse mit Result Checker für Konsolidierung, Standard-Reports als PDF und XLSX
Jährlich wiederkehrende Kosten: Modell pro Nutzer/Instanz: SSI Basic + Nessus Add-on, 9.000,00€

Option 2 - Framatome (Cyberwatch / PAR / PBA / Sentrigard)
Leistungsumfang: Cyberwatch für Vulnerability-, bzw. Compliance-Management (maximal 50 Assets), on-prem, Port-Scan, ergänzend PAR/PBA (Patch-Verfügbarkeit und Binary-Beschaffung) und Sentrigard (Patch-Deployment)
Jährlich wiederkehrende Kosten: Cyberwatch OT 50 Assets, Compliance Management, PAR/PBA Run, Sentrigard Maintenance, 21.000,00€
Einmalige Einrichtung: PAR/PBA Build, Sentrigard, zwei Support Tage: 20.000,00€

Option 3 - AUVESY-MDT octoplant
Leistungsumfang: Schwerpunkt Backup/Versionierung/Change-Tracking in OT, „Threat Protection“ mit Schwachstellen-/Risikoanalyse als einmalige bzw. monatliche on-demand-Leistung
Jährlich wiederkehrende Kosten: Premium Paket 54.000,00€ inkl. 100 Upload-, Backup- und Vergleichsschritte (Jobs) und 5 Benutzern, weitere Jobs und Benutzer gegen Aufpreis

Option 4 - Eigenentwicklung
Leistungsumfang (Zielbild): Kombination aus automatischen Scans (z. B. Nmap), Vulnerability-Engine (z. B. OpenVAS), eigener CVE-Feed-Anbindung, Skripte zur Datenkonsolidierung und Report-Erstellung
Jährlich wiederkehrende Kosten (geschätzt): 50.000,00€ für regelmäßige Updates, CVE-Feeds und Qualitätssicherung
Implementierungsaufwand: 150.000,00€ (Entwicklung und Implementierung einer Scansoftware)

A5. Nutzwertanalyse

Kriterien/Gewichtung (abgeleitet aus Zielbild):

Kriterium	Gewichtung	SSI (Siemens SINEC Security Inspector)	gewichtet	Framatome	gewichtet	AUVESY-MDT octoplant	gewichtet	Eigenentwicklung	gewichtet
A. Passgenauigkeit	20%	5	1	4	0,8	2	0,4	4	0,8
B. OT-Tauglichkeit	15%	4	0,6	5	0,75	3	0,45	4	0,6
C. Implementie-rungs-aufwand Pilot	10%	4	0,4	2	0,2	2	0,2	1	0,1
D. Berichtsfähigkeit	10%	5	0,5	4	0,4	3	0,3	3	0,3
E. Betrieb/Updates/ Pflege	10%	4	0,4	3	0,3	3	0,3	2	0,2
F. Kosten für ein Jahr (nach Imple-mentierung)	15%	4	0,6	3	0,45	2	0,3	5	0,75
G. Reproduzierbar-keit/Vergleichbarkeit	10%	5	0,5	4	0,4	3	0,3	3	0,3
H. Risiko/ Abhängigkeit	10%	3	0,3	3	0,3	3	0,3	4	0,4
	100%	34	4,3	28	3,6	21	2,55	26	3,45

Tabelle 4: Nutzwertanalyse

Gesamtpunkte (max. 5,0):

- SSI: 4,3 - Rang 1
- Framatome: 3,6 - Rang 2
- Eigenentwicklung: 3,45 - Rang 3
- AUVESY-MDT octoplant: 2,55 - Rang 4

A6. Virtual Network Editor

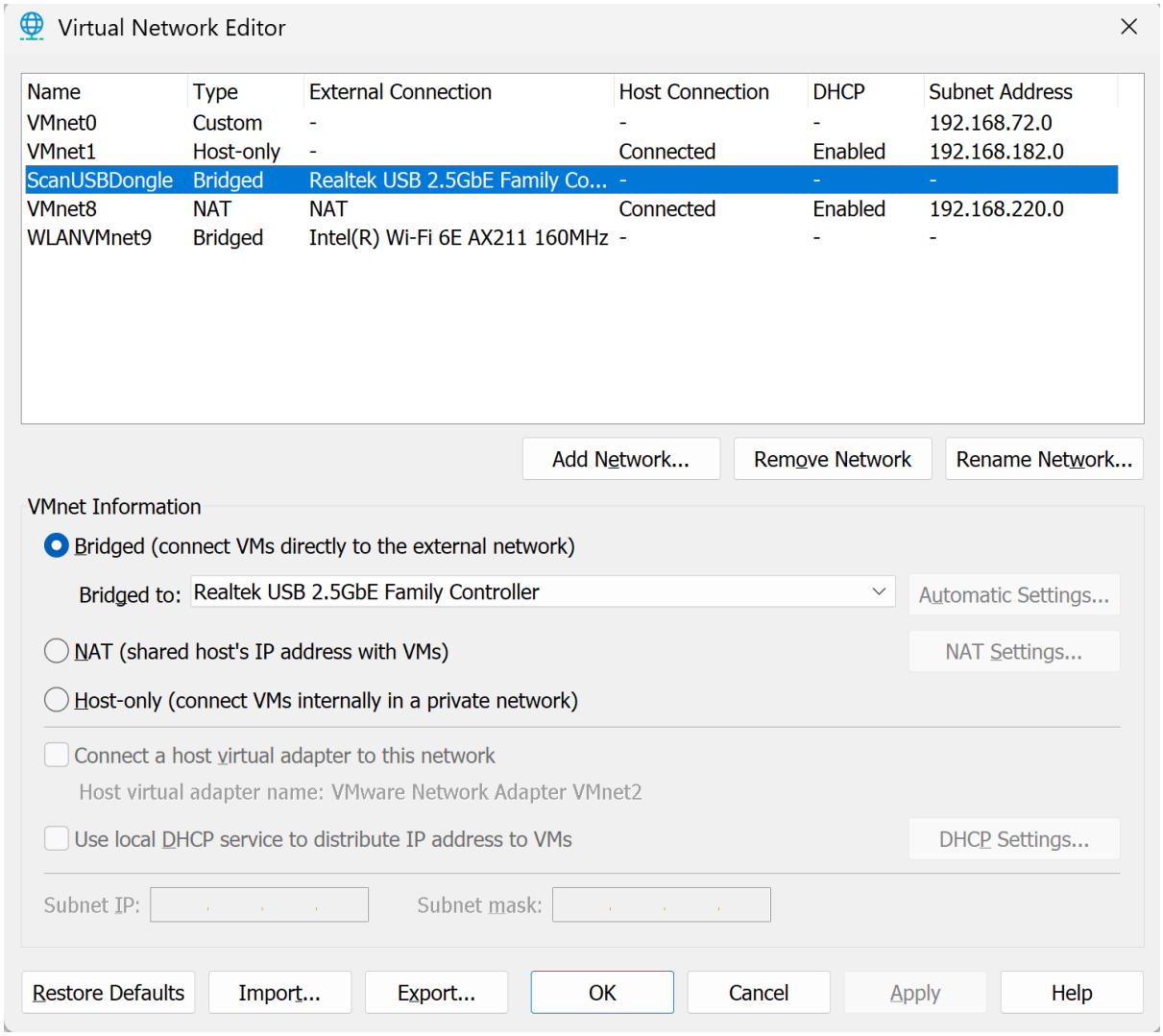


Abbildung 2: Virtual Network Editor

A7. Target-Liste

Availability	ID	Name	Tags	Host	Network Profile	Last Edit	Actions
subnet	19					2025-11-12 15:11:13	Edit
subnet	14					2025-11-12 15:10:58	Edit
reachable	15					2025-11-12 14:07:34	Edit
reachable	11					2025-10-13 15:15:59	Edit
reachable	17					2025-10-13 11:57:33	Edit
unreachable	16					2025-10-13 11:56:36	Edit
reachable	13					2025-09-15 11:21:44	Edit
reachable	12					2025-09-05 08:02:21	Edit

Abbildung 3: Ansicht Target-Liste

A8. Weboberfläche SSI - Test Result

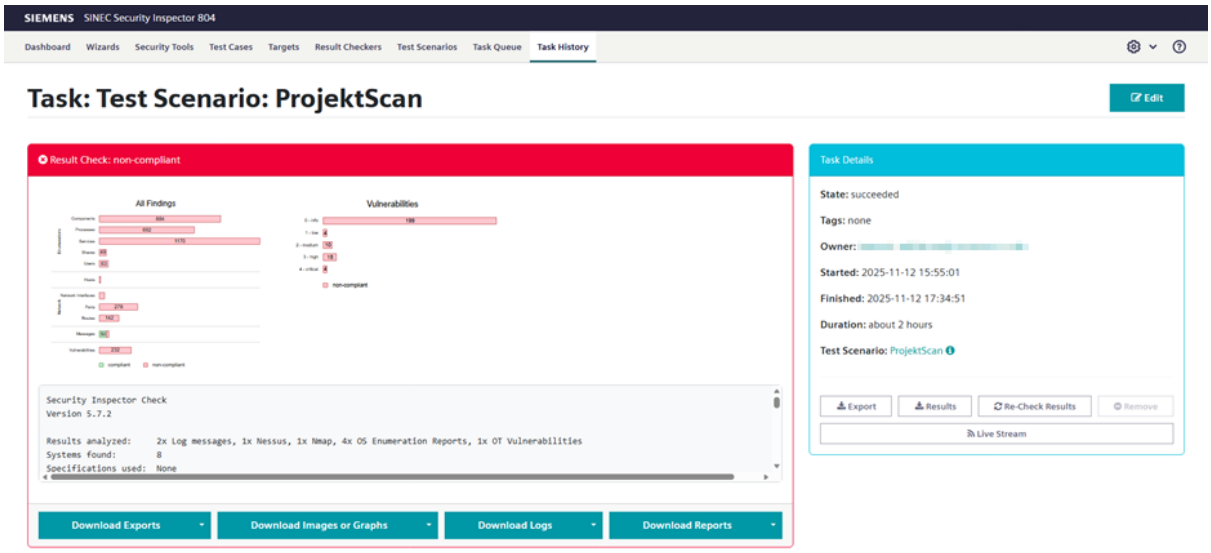


Abbildung 4: Weboberfläche SSI ProjektScan Übersicht

Results

Run	Target	Test Case / Result Checker	Version	Started	Duration	Progress	State
Run 1		Asset and Vulnerability Discovery (OT Scanner)	5.24.0	2025-11-12 15:55:02	3 minutes	100%	completed
Run 2		Solution Port Scan (Nmap, all TCP ports, common UDP ports)	0.10.0	2025-11-12 15:58:22	6 minutes	100%	completed
Run 3		Discovery Scan (OS Enumerations)	5.11.0	2025-11-12 16:04:07	20 minutes	100%	completed
Run 4		Vulnerability Scan (Nessus)	1.86.0	2025-11-12 16:23:43	39 minutes	100%	completed
Run 5		Test Case Utils Target Cleanup	2.6.0	2025-11-12 17:02:15	8 minutes	100%	completed
Run 6		Security Inspector Check	5.7.2	2025-11-12 17:10:29	24 minutes	100%	completed

Abbildung 5: Weboberfläche SSI ProjektScan Results

A9. Ergebnisausschnitt des Result Checker

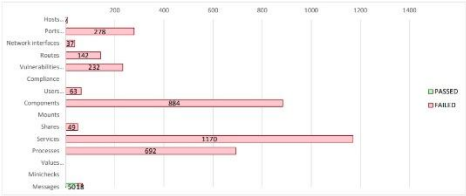
Inspector Check **Result Evaluation V5.7.2**

Summary

Evaluation Time:	2025-11-12 17:11:11
Test Scenario:	Test Scenario: ProjektScan, Identifier: siesta_box_id_804:eecc13076e7466e45a8006a63188c801
Version:	1.19.7.1 2025-03-11 (production heads/v1.19-stable-0-gd325ca6225)
Result Checker:	Security Inspector Check (gem version 5.7.2), Identifier: inspector

Overall Result	FAILED

Results per Test Category/Test				
Test Category /Tests		**Findings**	**PASSED**	**FAILED**
Host	Hosts	7		7
Network	Ports	278		278
	Network interfaces	37		37
	Routes	142		142
Vulnerabilities / Compliance	Vulnerabilities	232		232
	Compliance			
Enumerations	Users	63		63
	Components	884		884
	Mounts			
	Shares	49		49
	Services	1170		1170
	Processes	692		692
Miscellaneous	Values			
	Minichecks			
	Messages	68	50	18
Summary		**3622**	**50**	**3572**



Vulnerabilities			
Severity Level	**Findings**	**PASSED**	**FAILED**
4 - critical	4		4
3 - high	15		15
2 - medium	10		10
1 - low	4		4
0 - info	199		199
unclassified			

Results per Test Category/Test/System			IP Address:	
Test Category /Tests		**Findings**	**PASSED**	**FAILED**
Host	Hosts			
Network	Ports			
	Network interfaces			
	Routes			
Vulnerabilities / Compliance	Vulnerabilities			
	Compliance			
Enumerations	Users			
	Components			
	Mounts			
	Shares			
	Services			
	Processes			
Miscellaneous	Values			
	Minichecks			
	Messages			
Summary		**0**	**0**	**0**

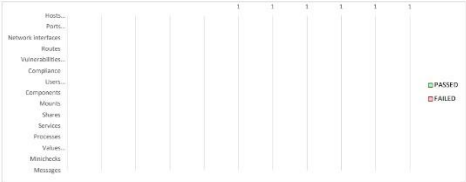


Abbildung 6: Ergebnisausschnitt des Result Checker vor dem Re-Scan

Inspector Check **Result Evaluation V5.7.2**

Summary

Evaluation Time:	2025-11-12 17:11:11
Test Scenario:	Test Scenario: ProjektScan, Identifier: [illegible]
Version:	1.19.7.1 2025-03-11 (production heads/v1.19-stable-0-gd325ca6225)
Result Checker:	Security Inspector Check (gem version 5.7.2), Identifier: inspector
Task:	162 https://192.168.220.130:443/tasks/162.html

E_rc (Errors/Warnings)	18
E_hosts (Failed):	7
Overall Verdict:	non-compliant

				Enumerations										Host		Network					
				Components		Processes		Services		Shares		Users		Hosts		Network Interfaces		Ports		Routes	
Target Name	**Host**	**Host Names**	**Verdict**	**Total**	**Failed**	**Total**	**Failed**	**Total**	**Failed**	**Total**	**Failed**	**Total**	**Failed**	**Total**	**Failed**	**Total**	**Failed**	**Total**	**Failed**	**Total**	**Failed**
[illegible]	[illegible]	[illegible]	non-compliant	884	884	692	692	1170	1170	49	49	63	63	7	7	37	37	278	278	142	142
[illegible]	[illegible]		compliant																		
[illegible]	[illegible]	[illegible]	non-compliant	330	330	187	187	307	307	12	12	16	16	1	1	10	10	66	66	41	41
[illegible]	[illegible]	[illegible]	non-compliant	226	226	243	243	323	323	13	13	27	27	1	1	9	9	101	101	33	33
[illegible]	[illegible]	[illegible]	non-compliant	82	82	134	134	272	272	12	12	10	10	1	1	9	9	47	47	35	35
[illegible]	[illegible]	[illegible]	non-compliant											1	1			8	8		
[illegible]	[illegible]	[illegible]	non-compliant	83	83	128	128	268	268	12	12	10	10	1	1	9	9	40	40	33	33
[illegible]	[illegible]	[illegible]	non-compliant	163	163									1	1						

Abbildung 7: Ergebnisausschnitt des Result Checker vor dem Re-Scan 2

A10. Baseline-Regeln

Inspector Check **Result Evaluation V5.7.2**

User/Group Specification

Users and user groups of the system are identified.

Performed test
Description of input values
Examples
Specified rules (* is mandatory)

Target	Source	User*	Group	Status	Type*	Valid until	Description	Comment
		[redacted]			may_exist			Standardbenutzer
		[redacted]			may_exist			Standardbenutzer
		[redacted]			may_exist			Standardbenutzer
		[redacted]			may_exist			Standardbenutzer
		[redacted]			may_exist			Standardbenutzer
		[redacted]			may_exist			Standardbenutzer
		[redacted]			may_exist			Standardbenutzer
		[redacted]			may_exist			Standardbenutzer

Abbildung 8: Whitelist für Benutzer

pector Check **Result Evaluation V5.7.2**

ılnerability Checks Specification

e system is checked for known vulnerabilities.

rformed test
escription of input values
amples
ecified exemptions (* is mandatory)

get	Port	Protocol	Path	Service	Type*	Tool	Value*	Valid until	Description	Comment
[redacted]	*	*	*	*	whitelist_check					Scan NIC
					allowed_severity_level	Nessus	info			Infos
					whitelist_check		65057			Nicht Relevant für uns
					whitelist_check		57608			Nicht Relevant für uns
					whitelist_check		57608			Nicht Relevant für uns
					whitelist_check		10114			Nicht Relevant für uns
					whitelist_check		10114			Nicht Relevant für uns

Abbildung 9: Whitelist für Schwachstellen

A11. Result Evaluation Vulnerabilities

Inspector Check **Result Evaluation V5.7.2**

Evaluation of Vulnerability Scan

This is a generated sheet. Do not edit it!

Target	Host Name	Target Nam	Port	Protocol	Servic	Verdi	Tool	Check ID	Check	CVE	Specified Rule	Detected Severity Level	CVSS Base Score
[redacted]	[redacted]	[redacted]	445	tcp	cifs	FAILED	Nessus	65057	Insecure Windows Service Permissions		no	3 - high	8.4
[redacted]	[redacted]	[redacted]	445	tcp	cifs	FAILED	Nessus	57608	SMB Signing not required		no	2 - medium	5.3
[redacted]	[redacted]	[redacted]	445	tcp	cifs	FAILED	Nessus	57608	SMB Signing not required		no	2 - medium	5.3
[redacted]	[redacted]	[redacted]	0	icmp	general	FAILED	Nessus	10114	ICMP Timestamp Request Remote Date Disclosure	CVE-1999-0524	no	1 - low	2.1
[redacted]	[redacted]	[redacted]	0	icmp	general	FAILED	Nessus	10114	ICMP Timestamp Request Remote Date Disclosure	CVE-1999-0524	no	1 - low	2.1
[redacted]	[redacted]	[redacted]	0	tcp	general	FAILED	Nessus	19506	Nessus Scan Information		no	0 - info	
[redacted]	[redacted]	[redacted]	0	tcp	general	FAILED	Nessus	21745	OS Security Patch Assessment Failed		no	0 - info	
[redacted]	[redacted]	[redacted]	0	tcp	general	FAILED	Nessus	92365	Microsoft Windows Hosts File		no	0 - info	
[redacted]	[redacted]	[redacted]	0	tcp	general	FAILED	Nessus	109142	Do not scan operational technology devices		no	0 - info	
[redacted]	[redacted]	[redacted]	0	tcp	general	FAILED	Nessus	121006	Detect PROFINET targets listening on the Network Layer.		no	0 - info	
[redacted]	[redacted]	[redacted]	445	tcp	cifs	FAILED	Nessus	10150	Windows NetBIOS / SMB Remote Host Information Disclosure		no	0 - info	
[redacted]	[redacted]	[redacted]	445	tcp	cifs	FAILED	Nessus	10394	Microsoft Windows SMB Log In Possible		no	0 - info	
[redacted]	[redacted]	[redacted]	445	tcp	cifs	FAILED	Nessus	10456	Microsoft Windows SMB Service Enumeration		no	0 - info	

Abbildung 10: Übersicht gefundene Schwachstellen

Inspector Check **Result Evaluation V5.7.2**

Evaluation of Vulnerability Scan

This is a generated sheet. Do not edit it!

Target	Host Name	Target Name	Port	Protocol	Servic	Verdi	Tool	Check ID	Check	CVE	Specified Ru	Detected Severity Level	CVSS Base Score
[redacted]	[redacted]	[redacted]	445	tcp	cifs	PASSED	Nessus	65057	Insecure Windows Service Permissions		<whitelisted>	3 - high	8.4
[redacted]	[redacted]	[redacted]	445	tcp	cifs	PASSED	Nessus	57608	SMB Signing not required		<whitelisted>	2 - medium	5.3
[redacted]	[redacted]	[redacted]	445	tcp	cifs	PASSED	Nessus	57608	SMB Signing not required		<whitelisted>	2 - medium	5.3
[redacted]	[redacted]	[redacted]	0	icmp	general	PASSED	Nessus	10114	ICMP Timestamp Request Remote Date Disclosure	CVE-1999-0524	<whitelisted>	1 - low	2.1
[redacted]	[redacted]	[redacted]	0	icmp	general	PASSED	Nessus	10114	ICMP Timestamp Request Remote Date Disclosure	CVE-1999-0524	<whitelisted>	1 - low	2.1
[redacted]	[redacted]	[redacted]	0	tcp	general	PASSED	Nessus	19506	Nessus Scan Information		0 - info	0 - info	
[redacted]	[redacted]	[redacted]	0	tcp	general	PASSED	Nessus	21745	OS Security Patch Assessment Failed		0 - info	0 - info	
[redacted]	[redacted]	[redacted]	0	tcp	general	PASSED	Nessus	92365	Microsoft Windows Hosts File		0 - info	0 - info	
[redacted]	[redacted]	[redacted]	0	tcp	general	PASSED	Nessus	109142	Do not scan operational technology devices		0 - info	0 - info	
[redacted]	[redacted]	[redacted]	0	tcp	general	PASSED	Nessus	121006	Detect PROFINET targets listening on the Network Layer.		0 - info	0 - info	
[redacted]	[redacted]	[redacted]	445	tcp	cifs	PASSED	Nessus	10150	Windows NetBIOS / SMB Remote Host Information Disclosure		0 - info	0 - info	
[redacted]	[redacted]	[redacted]	445	tcp	cifs	PASSED	Nessus	10394	Microsoft Windows SMB Log In Possible		0 - info	0 - info	
[redacted]	[redacted]	[redacted]	445	tcp	cifs	PASSED	Nessus	10456	Microsoft Windows SMB Service Enumeration		0 - info	0 - info	
[redacted]	[redacted]	[redacted]	445	tcp	cifs	PASSED	Nessus	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure		0 - info	0 - info	
[redacted]	[redacted]	[redacted]	445	tcp	cifs	PASSED	Nessus	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration		0 - info	0 - info	

Abbildung 11: Übersicht gefundene Schwachstellen nach Re-Check

A12. „Compliant“ Scan

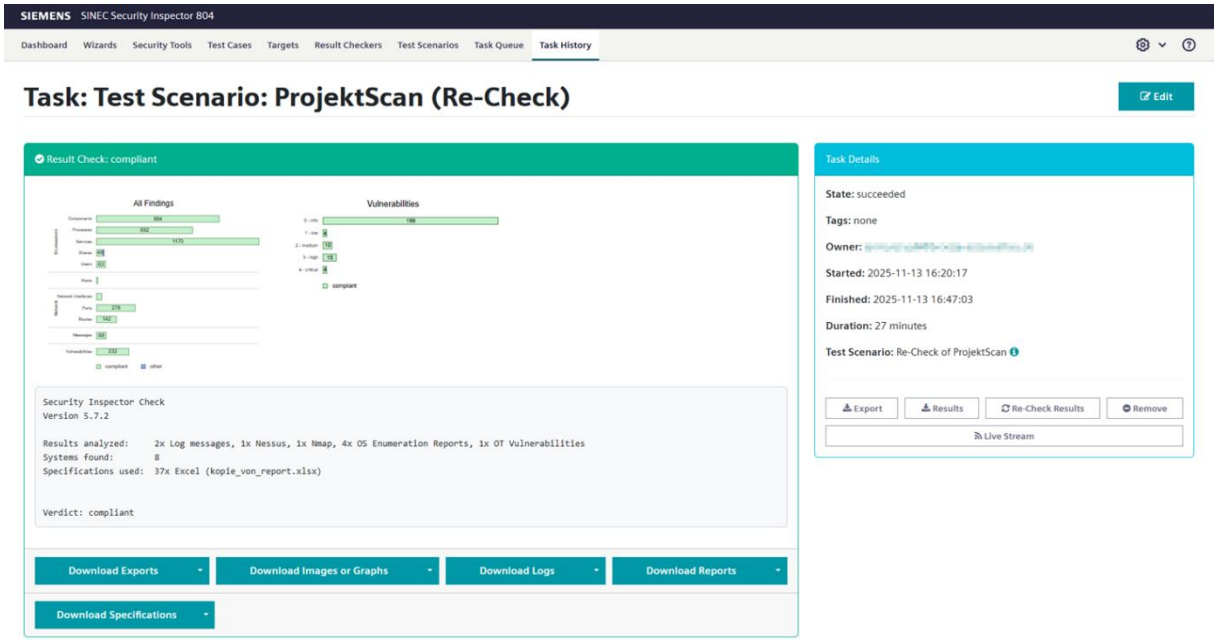
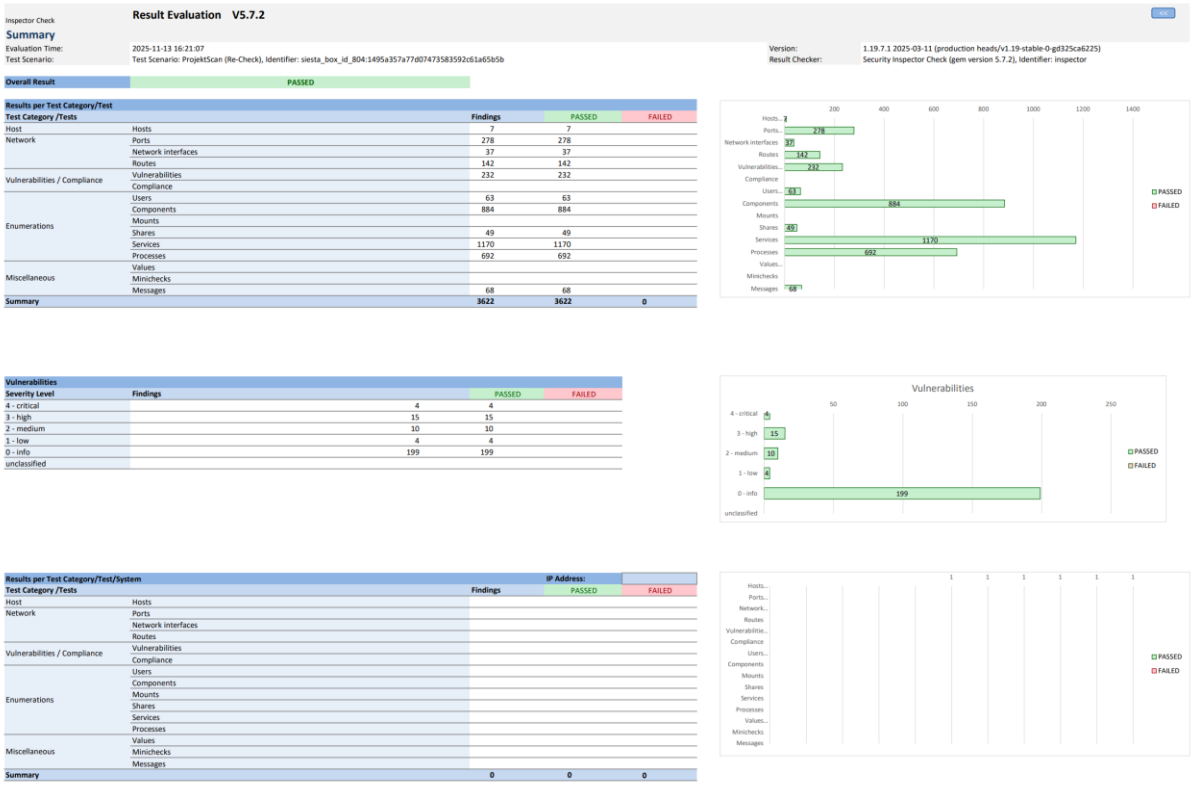


Abbildung 12: Weboberfläche SSI ProjektScan (Re-Check) Übersicht



Inspector Check — Result Evaluation V5.7.2

Summary

Evaluation Time:	2025-11-13 16:21:07
Test Scenario:	Test Scenario: ProjektScan (Re-Check), Identifier: siesta_box_id_804:1495a357a77d07473583592c61a65b5b
Version:	1.19.7.1 2025-03-11 (production heads/v1.19-stable-0-gd325ca6225)
Result Checker:	Security Inspector Check (gem version 5.7.2), Identifier: inspector

Overall Result	PASSED

Results per Test Category/Test				
Test Category /Tests		Findings	PASSED	FAILED
Host	Hosts	7	7	
Network	Ports	278	278	
	Network interfaces	37	37	
	Routes	142	142	
Vulnerabilities / Compliance	Vulnerabilities	232	232	
	Compliance			
Enumerations	Users	63	63	
	Components	884	884	
	Mounts			
	Shares	49	49	
	Services	1170	1170	
	Processes	692	692	
Miscellaneous	Values			
	Minichecks			
	Messages	68	68	
Summary		**3622**	**3622**	**0**

Vulnerabilities			
Severity Level	Findings	PASSED	FAILED
4 - critical	4	4	
3 - high	15	15	
2 - medium	10	10	
1 - low	4	4	
0 - info	199	199	
unclassified			

Results per Test Category/Test/System			IP Address:	
Test Category /Tests		Findings	PASSED	FAILED
Host	Hosts			
Network	Ports			
	Network interfaces			
	Routes			
Vulnerabilities / Compliance	Vulnerabilities			
	Compliance			
Enumerations	Users			
	Components			
	Mounts			
	Shares			
	Services			
	Processes			
Miscellaneous	Values			
	Minichecks			
	Messages			
Summary		**0**	**0**	**0**

Abbildung 13: Ergebnisausschnitt des Result Checker nach Re-Scan „Compliant Scan“

Inspector Check **Result Evaluation V5.7.2**

Summary

Evaluation Time:	2025-11-13 16:21:07
Test Scenario:	Test Scenario: ProjektScan (Re-Check), Identifier: [redacted]
Version:	1.19.7.1 2025-03-11 (production heads/v1.19-stable-0-gd325ca6225)
Result Checker:	Security Inspector Check (gem version 5.7.2), Identifier: inspector
Task:	174 https://192.168.220.130:443/tasks/174.html

E_rc (Errors/Warnings)	18
E_hosts (Failed):	0
Overall Verdict:	compliant

				Enumerations										Host		Network					
				Components		Processes		Services		Shares		Users		Hosts		Network Interfaces		Ports		Routes	
Target Name	**Host**	**Host Names**	**Verdict**	Total	Failed	Total	Failed	Total	Failed	Total	Failed	Total	Failed	Total	Failed	Total	Failed	Total	Failed	Total	Failed
[redacted]	[redacted]	[redacted]	**compliant**	**884**	**0**	**692**	**0**	**1170**	**0**	**49**	**0**	**63**	**0**	**7**	**0**	**37**	**0**	**278**	**0**	**142**	**0**
[redacted]	[redacted]		compliant																		
[redacted]	[redacted]	[redacted]	compliant	330	0	187	0	307	0	12	0	16	0	1	0	10	0	66	0	41	0
[redacted]	[redacted]	[redacted]	compliant	226	0	243	0	323	0	13	0	27	0	1	0	9	0	101	0	33	0
[redacted]	[redacted]	[redacted]	compliant	82	0	134	0	272	0	12	0	10	0	1	0	9	0	47	0	35	0
[redacted]	[redacted]	[redacted]	compliant											1	0			8	0		
[redacted]	[redacted]	[redacted]	compliant	83	0	128	0	268	0	12	0	10	0	1	0	9	0	40	0	33	0
[redacted]	[redacted]	[redacted]	compliant	163	0									1	0						

Abbildung 14: Ergebnisausschnitt des Result Checker nach Re-Scan „Compliant Scan“