SPAS · SECURE PLATFORM AUTOMATION SUITE · V1.0

LENNLAY · REFERENZ-ARCHITEKTUR

Plattform-Härtung in der Mythos-Ära.

Ein KI-Modell findet in Stunden, wofür Angreifer bisher Monate brauchten. Die Antwort ist keine neue Software, sondern die Plattform selbst: kontinuierlich gehärtet, auditierbar automatisiert, dauerhaft standardisiert.

EINORDNUNG · MISSVERSTÄNDNIS-KILLER

- **Die Secure Platform Automation Suite (SPAS) ist kein Tool, kein Scanner, kein SaaS.**
- SPAS ist eine **Referenz-Architektur mit Prinzipien-Framework**, die Plattform-Härtung von einer Projektdisziplin in einen pipeline-getriebenen Betriebszustand überführt.
- Der Wert entsteht durch **Reproduzierbarkeit, Evidenz und Governance**, nicht durch ein einzelnes Produkt.

EXECUTIVE SUMMARY

- Anthropic Claude Mythos hat am 9. April 2026 **181 Firefox-Exploits** in einem autonomen Lauf gefunden, 90-fach gegenüber dem Vorgänger. Wettbewerber-Modelle folgen laut Gartner in **6 bis 18 Monaten.**
- Die bisherige Praxis, Jahres-Pentest plus einmalige Härtung, begegnet den Anforderungen nach **NIS2UmsuCG und KRITIS-Dachgesetz** in aller Regel nicht mehr belastbar.
- Der Brief beschreibt die SPAS-Referenz-Architektur anhand von **7 Kernfähigkeiten,** ein JBoss-EAP-Referenzszenario und einen **30-Tage-Einstiegspfad** mit Scoping-Checkliste.

Stand April 2026 · Version 1.0 · Ausgabe für geladene Empfänger

EXECUTIVE SNAPSHOT

Was in diesem Brief steht, in vier Kennzahlen.

181 ×
Firefox-Exploits in einem Lauf durch Anthropic Claude Mythos (April 2026), 90-fach gegenüber dem Vorgänger

6–18
Monate bis Wettbewerber-Modelle vergleichbare Fähigkeiten erreichen (Gartner-Prognose)

7
Kernfähigkeiten tragen das operative Fundament und die Governance darüber

14 Tage
Frist nach dem KRITIS-Dachgesetz für die initiale Meldung eines erheblichen Sicherheitsvorfalls

KERNGEDANKE

Die bisherige Praxis - Jahres-Pentest plus einmalige Härtung - reicht in aller Regel nicht mehr aus, um Audit- und Aufsichtsanforderungen (NIS2UmsuCG, KRITIS-Dachgesetz) belastbar zu bedienen. Gefordert ist **Prävention als kontinuierlicher, pipeline-getriebener Prozess**, der Evidenz als Automatismus erzeugt, nicht als Quartalsend-Übung.

INHALT

01 · BEDROHUNGSMODELL

Mythos hat die Regeln geändert.

Am 9. April 2026 hat Anthropic das autonome Sicherheitsforschungs-Tool **Project Glasswing** auf Basis des Modells **Claude Mythos** veröffentlicht. Die dokumentierten Ergebnisse verändern die Prämisse, unter der Plattform-Sicherheit bisher gedacht wurde.

Was belegt ist

- **181 belegte Firefox-Exploits** in einem einzigen autonomen Lauf, darunter 14 bisher unbekannte Zero-Days. Der Vorgänger hatte im vergleichbaren Lauf 2 Exploits gefunden.
- **Autonome Exploit-Entwicklung** von der Vulnerability-Entdeckung bis zum funktionierenden Proof-of-Concept ohne menschliche Nacharbeit.
- **Niveau hochqualifizierter Softwareentwickler** bei der Analyse von Angriffspfaden über verteilte Systeme (bestätigt durch das Projekt-Paper).
- **Laut Gartner-Prognose** erreichen vergleichbare Modelle auf Wettbewerber-Seite (OpenAI, Google DeepMind, Meta, chinesische Labs) das Mythos-Fähigkeitsniveau binnen 6 bis 18 Monaten.

Was das operativ bedeutet

Das ökonomische Modell von Security-Pipelines verändert sich strukturell. Was bisher ein signifikanter menschlicher Aufwand war - Schwachstellenforschung, Exploit-Entwicklung, Kettenbildung - wird durch Mythos-Klasse-Modelle parallelisierbar, beschleunigt und kostengünstiger. Die Angreiferseite erhält damit einen strukturellen Hebel, den Verteidiger mit bisheriger Arbeitsweise zunehmend schwerer kompensieren können.

Für regulierte Plattformen - Banken-IT, Versicherungen, KRITIS-Betreiber, Öffentliche Hand - bedeutet das eine Verschiebung der Begründungslast: Der bisherige Nachweis "CIS-Benchmark PDF vorhanden, Pentest einmal jährlich durchgeführt" reicht nach aktuellem Auslegungsstand der Anforderungen aus NIS2UmsuCG und KRITIS-Dachgesetz in aller Regel nicht mehr aus.

ZEITFENSTER

Der realistische Vorbereitungszeitraum für eine Neuausrichtung der Plattform-Härtung beträgt 6 bis 18 Monate. Wer jetzt beginnt, kann den Umbau in kontrollierten Schritten machen. Wer wartet, läuft Gefahr, ihn unter Vorfalls- oder Auditdruck umsetzen zu müssen.

01 · BEDROHUNGSMODELL · REGULATORISCHER KONTEXT

Was NIS2UmsuCG und KRITIS-Dachgesetz operativ verlangen.

Die deutsche Umsetzung der NIS2-Richtlinie (NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz, NIS2UmsuCG) sowie das KRITIS-Dachgesetz verändern die Anforderungen an betroffene Betreiber in drei Dimensionen:

DIMENSION	BISHERIGE PRAXIS	AB 2026 ERFORDERLICH
Risikomanagement	ISMS-Policy als Dokument, quartalsweise Review.	Kontinuierliche technisch-organisatorische Maßnahmen auf Plattform-Ebene, prüfbar aus Systemdaten.
Meldepflicht	Informeller Vorfallsbericht an das BSI.	Strukturierte Erstmeldung binnen 24 Stunden, vollständige Meldung binnen 72 Stunden, Abschlussbericht binnen 1 Monat.
Geschäftsleiter-Verantwortung	Sicherheits-Thema auf CTO/CISO delegiert.	Billigung und Überwachung der Risikomaßnahmen durch Geschäftsleitung, belegbar, mit Haftungsrisiko im Fall nachweislich unterlassener Maßnahmen.
Lieferkette	Vertrauensbasiert.	Explizite Steuerung von Software-Lieferanten, inkl. SBOM-Nachweis und dokumentierter Lifecycle-Kontrolle.

Der operative Bruch

Alle vier Dimensionen verlangen **fortlaufende, technisch überprüfbare Evidenz**, nicht Einmal-Dokumente. Aus Audit-Sicht führt das direkt zu einer veränderten Prüfkultur: Der Wirtschaftsprüfer und die Aufsicht wollen nicht mehr das PDF auf SharePoint sehen, sondern den Auszug aus der Plattform, der zeigt, dass die Policy heute Nacht durchgesetzt wurde - und gestern, und vorgestern.

> **KONSEQUENZ FÜR DIE PLATTFORM-STRATEGIE**
>
> Plattform-Härtung wird vom Projekt-Artefakt (einmal hergestellt, dann gepflegt) zu einem **kontinuierlichen, reproduzierbaren Zustand**, der aus einer Pipeline heraus erzeugt, geprüft und dokumentiert wird. Die folgenden Kapitel beschreiben, wie diese Pipeline aussieht.

02 · SECURE PLATFORM AUTOMATION SUITE (SPAS)

Sieben Kernfähigkeiten auf zwei Ebenen.

SPAS ist keine neue Scanner-Generation. Es ist die operative Klammer quer über die bestehende Werkzeug-Landschaft, die sie für die neue Anforderungslage auditfähig und dauerhaft wirksam macht. Die sieben Kernfähigkeiten gliedern sich in zwei Ebenen: Fundament (01–04) und Governance (05–07).

OPERATIVER KERN · 01–04

01 · Sicherheitsstandards, Baselines und Policies

Maschinenlesbare Baselines aus CIS, STIG, BSI und kundenspezifischen Anforderungen – versioniert und wiederverwendbar.

02 · Golden Images und Plattform-Baselines

Geprüfte, reproduzierbare Systemabbilder als definierter Ausgangszustand für alle Deployments.

03 · Automatisierung, Deployment und Plattformintegration

Pipeline-getriebene Auslieferung in bestehende Infrastruktur, CI/CD-Workflows und Plattformprozesse.

04 · Compliance-Prüfung und Reporting

Kontinuierliche Scans mit automatisch erzeugter Audit-Evidenz – keine manuell gepflegten Compliance-Berichte.

GOVERNANCE · 05–07

05 · Dokumentation, Nachvollziehbarkeit und Auditierbarkeit

Lückenlose, maschinell erzeugte Nachweise aus Systemdaten – kein manuell gepflegtes Audit-Dokument.

06 · Lifecycle- und Update-Management

Gesteuerte Patch-, Update- und Versionszyklen über alle relevanten Plattformkomponenten mit dokumentierter Lifecycle-Kontrolle.

07 · Drift-Erkennung und Enforcement

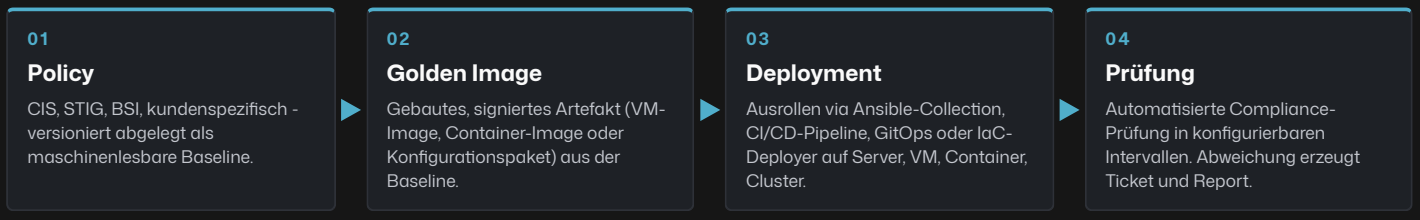
Automatische Erkennung von Abweichungen vom Sollzustand – Drift wird gemeldet und regelbasiert korrigiert.

Der operative Kern (01–04) bringt Policies kontinuierlich auf die Plattform: von der Baseline zum Golden Image, vom Image ins Deployment, vom Deployment in den Prüflauf. Governance (05–07) macht diesen Prozess auditierbar und steuerbar. Seiten 6 bis 8 beschreiben jede Ebene im Detail.

02 · KERNFÄHIGKEITEN 01–04 IM BETRIEB

Der operative Kern: Policy → Golden Image → Deployment → Prüfung.

Die Kernfähigkeiten 01 bis 04 bilden einen durchgängigen Fluss. Jede Station ist eigenständig versionier- und prüfbar, jeder Übergang ist reproduzierbar und automatisiert. Das ist das operative Fundament, ohne das keine Auditierbarkeit entstehen kann.



Was pro Station konkret passiert

01 · Sicherheitsstandards, Baselines und Policies

Kunden wählen die für sie relevanten Policy-Profile (CIS, STIG, BSI IT-Grundschutz, eigene Standards). Daraus werden Golden Images und Baselines gebaut. Die Policies sind maschinenlesbar, versioniert und reproduzierbar. Dokumentation der eingesetzten Profile folgt nachgelagert.

02 · Golden Images und Plattform-Baselines

Aus der Policy wird ein gehärtetes Basis-Artefakt gebaut. Für Linux: ein VM-Image oder Container-Image. Für Windows: ein gehärtetes Windows Imaging Format (WIM) oder eine Desired State Configuration (DSC). Bei Containern und Kubernetes fließt die Härtung direkt in den Image-Build. Jedes Artefakt ist signiert, versioniert und hat eine nachvollziehbare Ableitung von Upstream bis Produktion.

03 · Automatisierung, Deployment und Plattformintegration

Deployment ist die Fähigkeit, die in vielen Debatten fehlt. Policies und Golden Images allein verändern keinen Produktionsserver. Für Legacy-VMs und Middleware: Ansible-Collections und CI/CD-Pipelines bringen die Baseline auf den Host. Für Container und Kubernetes: ArgoCD, Flux oder vergleichbare GitOps-Tools deployen die gehärteten Images in Pods und Cluster. Manuelle Einzelschritte sind an dieser Stelle der kritische Pfad - wo sie bleiben, bleibt Drift.

04 · Compliance-Prüfung und Reporting

In konfigurierbaren Intervallen läuft ein automatisierter Compliance-Lauf gegen alle Zielplattformen. Standardmäßig werden Reports erzeugt; automatisches Enforcement ist optional konfigurierbar. Abweichung vom Soll-Zustand erzeugt ein Ticket und geht in den strukturierten Report ein. Der Audit-Nachweis entsteht damit nicht zwei Wochen vor der Prüfung, sondern kontinuierlich im Betrieb.

02 · KERNFÄHIGKEITEN 05–07 · GOVERNANCE

Governance: Dokumentation, Lifecycle und Drift.

Die Kernfähigkeiten 05 bis 07 liefern, was Audit, Vorstandsreport und Lifecycle-Planung verlangen. Sie sind nur dann belastbar, wenn der Wirkpfad (01–04) kontinuierlich läuft.

05 · Dokumentation, Nachvollziehbarkeit und Auditierbarkeit

Jede Änderung erzeugt einen Audit-Eintrag. Jede Ausnahme vom Soll-Zustand ist mit Begründung und Ablaufdatum hinterlegt. Der Audit-Report für NIS2UmsuCG und KRITIS-Dachgesetz entsteht aus Plattform-Daten, nicht aus einer Excel-Sammlung zwei Wochen vor der Prüfung.

06 · Lifecycle- und Update-Management

Support-Enden, Versionen, CVE-Status und Migrationspfade sind Attribute am Asset, nicht Wissen in Köpfen. Für geschäftskritische Middleware wie JBoss EAP heißt das konkret: Das End-of-Support-Datum steht im zentralen Dashboard, die Migrationspipeline ist sichtbar, und die Reihenfolge der Migrationen ist dem Audit und dem Vorstand in einem Klick zu zeigen.

07 · Drift-Erkennung und Enforcement

Zwischen zwei Deployments verändert sich der tatsächliche Zustand einer Plattform: Admin-Eingriffe, Fachverfahrens-Installationen, Notfall-Patches. Drift Detection vergleicht Ist- mit Soll-Zustand. Ergebnis ist nicht zwangsläufig ein automatisches Rollback - das wäre für viele geschäftskritische Plattformen gefährlich - sondern **Transparenz**: Jede Abweichung ist erkannt, bewertet und entweder bewusst geduldet oder kontrolliert zurückgeführt.

> **ENFORCEMENT NACH RISIKOPROFIL**
>
> Automatisches Enforcement ist nicht überall angemessen. Für hoch-verfügbare Fachverfahren mit engen Change-Fenstern gilt: Drift wird **erkannt und gemeldet**, der Rückweg läuft kontrolliert im nächsten Change-Slot. Gerade bei Middleware wie Tomcat oder JBoss EAP erfordert eine Korrektur einen kontrollierten Neustart im Change-Fenster. Für zustandslose Infrastruktur (Container-Cluster, standardisierte Web-Frontends) ist automatisches Enforcement direkt einsetzbar.

Vergleich: bisherige Praxis vs. Anforderung

FÄHIGKEIT	HEUTE TYPISCH	AB MYTHOS ERFORDERLICH
Drift	Fällt im nächsten Audit auf, oder gar nicht.	Nächtlich erkannt, Ticket automatisch, Enforcement nach Risikoprofil.
Lifecycle	Support-Ende landet per Memo bei Ops, Planung im Kopf weniger Personen.	EOL-Daten als Asset-Attribut, Update-Pipeline als sichtbarer Prozess.
Dokumentation	Audit-Vorbereitung als Kraftakt zwei Wochen vor der Prüfung.	Evidenz entsteht im Betrieb, Audit-Report auf Knopfdruck.

02 · MODUL-SCHNITT

Plattform-Module im SPAS-Portfolio.

Jedes SPAS-Modul ist eigenständig einsetzbar und baut auf den sieben Kernfähigkeiten auf. Der typische Einstieg erfolgt über das Modul mit dem höchsten Hebel, meist Middleware oder ein Betriebssystem-Modul, weitere Module folgen schrittweise.

MIDDLEWARE — HÄUFIGSTER EINSTIEG

Secure JBoss EAP Platform Automation

Auditfähige Baselines, Ansible-Collections, Lifecycle-Management für geschäftskritische Middleware.

MIDDLEWARE

Secure Tomcat Platform Automation

Gehärtete Tomcat-Baselines für Web-Frontends und Applikationsserver in Bestandsarchitekturen.

BETRIEBSSYSTEM

Secure Linux Platform Automation

CIS/STIG-konforme RHEL-, SLES- und Debian-Baselines mit kontinuierlichem Enforcement.

BETRIEBSSYSTEM

Secure Windows Platform Automation

Windows-Server-Härtung mit DSC/Ansible-Integration und auditfähigem Compliance-Reporting.

WEB-PLATTFORMEN

Secure IIS Platform Automation

IIS-Härtung für klassische .NET-Stacks, Lifecycle-Management inklusive.

CONTAINER

Secure Container Platform Automation

Image-Baselines, Runtime-Enforcement, SBOM-Integration für Docker- und Podman-basierte Umgebungen.

ORCHESTRIERUNG

Secure Kubernetes Platform Automation

Cluster-Baselines, Policy-as-Code, Drift Detection, für On-Prem und Cloud-K8s gleichermaßen.

PERSPEKTIVISCH — PIPELINE

OpenShift · NGINX · Apache · Java Runtime

Weitere Plattform-Module in Vorbereitung, weitere Plattform-Familien auf Anfrage.

INTEGRATION IN BESTANDSTOOLS

SPAS ersetzt weder Security-Scanner noch SIEM noch Ticket-System. Sie bündelt deren Ergebnisse auf Plattform-Ebene und macht sie reproduzierbar. Bestehende Investitionen in Tools wie Tenable, Qualys, Splunk, ServiceNow oder Jira können integriert werden, nicht verdrängt.

03 · MAPPING AUF NIS2UMSUCG

Welche Kernfähigkeit welche NIS2UmsuCG-Anforderung bedient.

Das NIS2UmsuCG formuliert technisch-organisatorische Mindestmaßnahmen (§ 30 BSIG-neu). Die sieben Kernfähigkeiten decken diese Anforderungen auf Plattform-Ebene ab. Das folgende Mapping ist als Argumentationshilfe fürs interne Gap-Assessment gedacht, ersetzt keine rechtliche Prüfung.

NIS2UMSUCG-ANFORDERUNG (§ 30 BSIG-NEU)	PRIMÄR BEDIENT DURCH	UNTERSTÜTZEND
Konzepte in Bezug auf die Analyse von Risiken und die Sicherheit in der Informationstechnik	KF 01 · Baselines & Policies	KF 05 · Dokumentation
Bewältigung von Sicherheitsvorfällen	KF 07 · Drift-Erkennung & Enforcement	KF 04 · Reporting
Aufrechterhaltung des Betriebs, insbesondere Backup-Management und Krisenmanagement	KF 02 · Golden Images (reproduzierbare Wiederherstellung)	KF 06 · Lifecycle
Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Dienstleistern	KF 02 · Golden Images (signierte Artefakte, SBOM)	KF 06 · Lifecycle
Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen	KF 03 · Automatisierung & Deployment	KF 01 · Policies
Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen	KF 04 · Compliance-Prüfung & Reporting	KF 05 · Auditierbarkeit
Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen	KF 01 + KF 03 (versionierte Baselines, automatisiertes Deployment)	KF 05 · Dokumentation
Konzepte und Verfahren für den Einsatz von Kryptographie	KF 01 · Baselines (Crypto-Policies)	KF 02 · Golden Images (Artefakt-Signaturen)
Personalsicherheit, Konzepte für die Zugriffskontrolle und das Management von Anlagen	KF 06 · Lifecycle & Asset-Attribute	KF 01 · Policies
Verwendung von Multi-Faktor-Authentifizierung	KF 01 · Baselines (Auth-Policy)	KF 04 · Compliance-Prüfung

03 · KRITIS-DACHGESETZ & BSI-BEZUG

Was KRITIS-Betreiber zusätzlich brauchen.

Für Betreiber kritischer Infrastrukturen greifen NIS2UmsuCG **und** KRITIS-Dachgesetz gleichzeitig. Das KRITIS-Dachgesetz fokussiert auf physischen Schutz, Resilienz und Verfügbarkeit, setzt aber ebenfalls auf nachweisbare technisch-organisatorische Maßnahmen auf.

KRITIS-DACHGESETZ-ANFORDERUNG	SPAS-BEITRAG
Resilienzmaßnahmen, insbesondere zur Aufrechterhaltung des Betriebs nach Vorfällen	Golden Images ermöglichen reproduzierbare Neuaufstellung der Plattform in Stunden statt Tagen. Baseline-Artefakte sind signiert und offline verfügbar.
Vorfallsmeldung binnen 14 Tagen als strukturierte Erstmeldung	Compliance-Prüfung (KF 04) und Drift-Erkennung (KF 07) liefern strukturierte Evidenz über den Vorfalls-Perimeter direkt aus Plattform-Daten.
Nachweis von Schutzmaßnahmen gegenüber der zuständigen Aufsichtsbehörde	Dokumentation (KF 05) und Lifecycle-Reporting (KF 06) erzeugen Audit-Reports ohne Sonderprojekt.
Steuerung von Drittabhängigkeiten in der Lieferkette	SBOM-Integration im Container-Modul, signierte Golden Images mit nachvollziehbarer Ableitung.

Bezug zum BSI IT-Grundschutz

Die SPAS-Baseline-Struktur integriert den BSI IT-Grundschutz-Kompendium-Ansatz (Bausteine SYS.1.x, APP.3.x, NET.3.x u.a.) als versionierte, maschinenlesbare Policy. Die Zuordnung Baustein → technische Kontrolle → Prüfnachweis ist durchgängig, ein Grundschutz-Check wird damit zum Report aus Plattform-Daten.

> **ABGRENZUNG**
>
> SPAS liefert keine Rechtsberatung und keine fertige NIS2-Compliance-Bescheinigung. Sie liefert die technische Schicht, die nötig ist, damit interne Gap-Analyse, ISMS-Audit und behördlicher Nachweis **mit vertretbarem Aufwand** belastbar werden.

Abgrenzung zu SIEM und Schwachstellen-Scanner

SIEM-Systeme (Splunk, QRadar, Sentinel) beobachten Ereignisse. Scanner (Tenable, Qualys, Greenbone) finden bekannte Schwachstellen. Beide sind notwendig, aber nicht hinreichend für die neue Anforderungslage: Sie produzieren Funde, nicht den auditfähigen **Zustand** der Plattform. SPAS produziert den Zustand und liefert damit die Referenz, gegen die SIEM- und Scanner-Befunde bewertet werden.

04 · JBOSS-EAP-REFERENZSZENARIO

Wie SPAS bei JBoss EAP wirkt: alle sieben Kernfähigkeiten.

In vielen DACH-Enterprises trägt JBoss EAP geschäftskritische Fachverfahren: Kern-Banking, Versicherungs-Policen, ERP-Nahbereich, Fach-Portale der öffentlichen Hand. Lifecycle-Druck (EAP 7 → 8, Red-Hat-Support-Modell) und Härtungspflicht (CIS, STIG, Kundenvorgaben) machen diese Plattform zum typischen Einstieg.

01 · Sicherheitsstandards, Baselines und Policies

lennlay greift auf eine eigene JBoss-Hardening-Policy zurück, die auf über 20 Jahren Betriebserfahrung mit JBoss EAP und den Best-Practice-Empfehlungen von Red Hat basiert. Die Policy wird versioniert abgelegt und ist maschinenlesbar für den Image-Build. Sie ist frei konfigurierbar: Kunden-eigene Härtungsrichtlinien werden aufgenommen und eingebaut.

02 · Golden Images und Plattform-Baselines

Das Golden Image wird auf Basis der in KF 01 definierten Policy gebaut und enthält JVM-Konfiguration sowie grundlegende Sicherheitsparameter. Für containerisierte Umgebungen fließt die Policy direkt in den Image-Build ein. Für Legacy-Deployments auf VMs und Bare-Metal erfolgt die Resthärtung (Verzeichnisrechte, Security-Realms, TLS) durch die lennlay.jboss Ansible Collection beim Deployment.

03 · Automatisierung, Deployment und Plattformintegration

Konfiguration ist vom Deployment getrennt. Für VM-basierte Systeme (Legacy-VMs und Cloud-VMs) appliziert die lennlay.jboss Ansible Collection die anwendungs- und stage-spezifische Konfiguration (Datasources, Messaging, Cluster-Einstellungen). Dadurch lassen sich viele Anwendungen und Stages ohne großen Konfigurationsaufwand mit derselben Collection verwalten. Ansible wird getriggert über AAP (Ansible Automation Platform, Enterprise), AWX (Community-Variante) oder CI/CD-Tools wie Jenkins oder GitLab.

Für Container-Umgebungen gilt ein anderer Ansatz: Container-Images tragen die Policy bereits im Image-Build. Das Ausrollen übernehmen GitOps-Tools wie ArgoCD oder Flux (OpenShift, AKS, EKS und weitere Kubernetes-Distributionen) - Ansible greift hier nicht.

04 · Compliance-Prüfung und Reporting

Der lennlay Compliance Scanner prüft JBoss-EAP-Instanzen gegen die definierten Policies. Er erkennt laufende und nicht laufende Plattform-Instanzen und erzeugt strukturierte Prüfergebnisse. Aktuell werden VM-basierte Umgebungen (Legacy und Cloud) unterstützt; eine Lösung für Container-Umgebungen ist in Entwicklung.

Für das Reporting werden die Ergebnisse zentral verarbeitet, geparst und in eine Datenbank geschrieben. Darauf aufbauend sind möglich: Reporting, Dashboard-Darstellung und perspektivisch KI-gestützte Auswertung.

04 · JBOSS-EAP-REFERENZSZENARIO · GOVERNANCE

Kernfähigkeiten 05–07 bei JBoss EAP.

05 · Dokumentation, Nachvollziehbarkeit und Auditierbarkeit

Fachverfahren haben historisch gewachsene Anforderungen, die nicht jede Policy-Vorgabe ohne Rückfrage tragen. Typische JBoss-EAP-Ausnahmen: Legacy-Datasources ohne TLS-Transportverschlüsselung, Security-Realms mit veralteten Authentifizierungsprotokollen, EAP-Subsystem-Settings (Messaging, Remoting), die produktionsbedingt von der Baseline abweichen, oder JVM-Heap-Konfigurationen außerhalb der Standardbandbreite für spezifische Workloads. Das Policy-Profil erlaubt explizite, signierte Ausnahmen pro Anwendung oder Basis-Image, mit Begründung und Ablaufdatum. Ausnahmen erscheinen im Audit-Report als technische Schuld versioniert und tauchen beim nächsten Lifecycle-Review automatisch auf. Jede Konfigurationsänderung erzeugt einen Audit-Eintrag.

06 · Lifecycle- und Update-Management

End-of-Support- und ELS-Daten (Extended Life Support) pro EAP-Version sind als Asset-Attribut im Dashboard sichtbar: Welche Cluster laufen auf welcher Version, wann läuft regulärer Support aus, welche Instanzen befinden sich im ELS-Fenster, wie ist der Migrationsstand. Der Übergang EAP 7 → 8 folgt einem strukturierten Migrationspfad: Abhängigkeitsanalyse der Deployments, Baseline-Anpassung auf EAP-8-Standards, Test-Stage-Rollout, Produktiv-Migration. Für den Weg EAP → OpenShift containerisiert lennlay die Deployments, überführt EAP-Konfigurationen in Container-native Strukturen und deployt über GitOps. Die Reihenfolge aller Migrationen ist dem Audit und dem Vorstand in einem Klick zu zeigen.

07 · Drift-Erkennung und Enforcement

Zwischen zwei Deployments verändert sich der EAP-Zustand: Admin-Eingriffe, Datasource-Änderungen, Notfall-Patches. Drift wird erkannt und gemeldet. Bei geschäftskritischer Middleware gilt: automatisches Enforcement erfordert einen kontrollierten Neustart im Change-Fenster, kein blindes Rollback. Drift-Berichte fließen in das SIEM oder das Ticket-System.

Warum dieses Referenzszenario trägt

Alle sieben Kernfähigkeiten werden bei JBoss EAP exemplarisch einmal vollständig durchgezogen. Die dabei entstehenden Artefakte und Prozesse - versionierte Baselines, Deployment-Automatisierung, Drift-Logik, Audit-Schema - sind direkt wiederverwendbar für Tomcat, IIS, Linux, Windows und Container. Der erste Einsatz liefert das operative Grundmuster für alle weiteren Module.

05 · EINSTIEGSPFAD

Vom Plattform-Check zum Produktiv-Modul.

SCHRITT 0
Plattform-Check
15–30 Min. Online. Plattform-Landschaft, Compliance-Druck und SPAS-Fit einschätzen. Kostenlos, kein Pitch.

▶

PRE-STAGE
Onboarding-Workshop
2 Tage, 2 lennlay-Experten. Assessment Plattform-Landschaft, Arbeitsweise, Automatisierungsreife. 4.900 € pauschal.

▶

WOCHE 1
Scoping & Baseline-Auswahl
Plattform-Inventar schärfen, Compliance-Ziele fixieren, gemeinsamer Zielzustand.

▶

WOCHE 2
Modul-Anpassung
Baselines auf die Kundenumgebung zugeschnitten, Collections versioniert (sofern Ansible im Einsatz), Test-Stage aufgesetzt.

▶

WOCHE 3–4
Rollout & Audit-Report
Produktiv-Rollout gegen definiertes Cluster-Set. Drift-Detection aktiv. Automatischer Compliance-Report.

WAS DIE SECURE PLATFORM AUTOMATION SUITE JE NACH MODUL UND SCOPE LIEFERN KANN

- Versionierte Golden Images & Baselines
- Automatisierungsbausteine, z. B. Ansible-Collections
- Lifecycle-Übersichten zu EoS, ELS und Migrationsständen
- Compliance-Reports mit Soll/Ist-Sicht und dokumentierten Ausnahmen
- Audit-Nachweise und nachvollziehbare Artefakt-Dokumentation
- Drift-Reports sowie Anbindung an Ticket- und SIEM-Prozesse

Verfügbarkeit und Automatisierungsgrad hängen vom Modul, der Zielplattform und dem vereinbarten Scope ab. Einzelne Bausteine befinden sich je nach Plattform noch im Ausbau.

Scoping-Checkliste für das interne Assessment

- ☐ Welche Plattform-Familien sind im Scope (Linux, Windows, JBoss EAP, IIS, Tomcat, Container, Kubernetes, andere)?
- ☐ Welche Baseline-Referenz ist bindend (CIS, STIG, BSI IT-Grundschutz, eigene Standards, Kundenvorgaben aus Fachverfahren)?
- ☐ Welche Regulatorik greift konkret (NIS2UmsuCG, KRITIS-Dachgesetz, BaFin-Rundschreiben, DORA, branchenspezifische Aufsicht)?
- ☐ Welche Betriebsumgebung: On-Premises, Cloud (AWS, Azure, GCP), Kubernetes (OpenShift, AKS, EKS), Hybrid?
- ☐ Welche Automatisierung existiert bereits (Ansible, Puppet, Chef, SaltStack, hauseigene Skripte)?
- ☐ Welche CI/CD- und GitOps-Landschaft ist betriebsintegriert (GitLab, Azure DevOps, Jenkins, ArgoCD, Flux)?
- ☐ Welche SIEM- und Scanner-Investitionen existieren (Splunk, QRadar, Sentinel, Tenable, Qualys, Greenbone)?
- ☐ Welche Change-Fenster und Freigabeprozesse sind für das erste Pilot-Set einzuhalten?
- ☐ Welche Personen bilden den internen Ansprechpartnerkreis (Plattform-Lead, Security-Owner, Audit-Liaison)?

Nächster Schritt

Buchen Sie einen kostenlosen Plattform-Check (15–30 Min. Online), um SPAS-Fit, Compliance-Druck und Einstiegspotenzial einzuschätzen. Folgender Schritt: zweitägiger Onboarding-Workshop, pauschal 4.900 €.

Plattform-Check vereinbaren

FRAGEN ZUM BRIEF? KONTAKTIEREN SIE UNS!

contact@lennlay.com