ONEKEY.COM



VORSCHRIFTEN FÜR DIE SOFTWARE-LIEFERKETTE

Wie lässt sich ein effektives und effizientes SBOM-Management erreichen?

ONEKEY

WHITEPAPER

ZUSAMMENFASSUNG

Warum jeder Hersteller weltweit Software-Stücklisten (SBOMs) implementieren muss

Lesezeit: Ungefähre Lesezeit 15 Minuten.

Dieses Whitepaper richtet sich an Produktverantwortliche, Product-Security-Manager und Compliance-Experten von Herstellern weltweit, die ein effektives und effizientes SBOM-Management verstehen und umsetzen müssen, um internationale regulatorische Anforderungen zu erfüllen.

Dieses Whitepaper untersucht die Notwendigkeit für jeden Hersteller weltweit, die Risiken in der Lieferkette im Zusammenhang mit Softwareanbietern und -betreibern zu managen, wie sie von Aufsichtsbehörden in verschiedenen Branchen erkannt wurden.

Jüngste Vorfälle im Bereich der Cybersicherheit haben Schwachstellen in modernen Software-Lieferketten aufgezeigt, was zur Einführung neuer Regeln und Vorschriften geführt hat. Software Bills of Materials (SBOMs) haben sich als ein zentrales Element innerhalb dieser Vorschriften herausgebildet und bieten greifbare Artefakte, die ein effektives Risikomanagement in der Lieferkette ermöglichen.

Dieses Paper hat zum Ziel, Hersteller, Entwickler und Integratoren von vernetzten Produkten (IoT/IIoT/OT) über die Bedeutung von SBOMs und die notwendigen Schritte zu informieren, um damit umzugehen.

Es erörtert die Bedeutung von SBOMs im Kontext der jüngsten Cybersicherheitsvorfälle, die Herausforderungen der Integration von Softwarekomponenten, die Rolle und Herausforderungen von SBOMs im Risikomanagement der Lieferkette, die Erstellung von SBOMs, das Teilen von SBOMs und den Einsatz von SBOMs zur Einhaltung von OSS-Lizenzen, der Verringerung von Schwachstellen und der Sicherung von Software-Lieferketten. Das Paper schließt mit der Betonung der Notwendigkeit, dass Organisationen das Management der Software-Lieferkette priorisieren und robuste Sicherheitspraktiken implementieren, um Risiken effektiv zu mindern.

HINTERGRUND

Regulierungsbehörden in verschiedenen Branchen haben die Dringlichkeit erkannt, die Risiken in der Lieferkette im Zusammenhang mit Softwareanbietern und -betreibern zu managen. Jüngste Ereignisse haben die Schwachstellen von vernetzten Systemen aufgrund moderner Software-Lieferketten aufgezeigt, was zur Einführung neuer Vorschriften und Regeln geführt hat. Die Nichteinhaltung dieser Vorschriften kann zum Ausschluss von Märkten und zu einer potenziellen Haftung wegen Fahrlässigkeit führen.

Diese Vorschriften decken eine Vielzahl von Bereichen ab, einschließlich des Konsumgüter-Internet of Things (IoT), wobei Software Bills of Materials (SBOMs) als ein herausragendes Element innerhalb dieser Vorschriften hervorgehoben werden, da sie als greifbare Artefakte dienen, die wichtige Prozesse ermöglichen. Mehrere Vorschriften erwähnen explizit SBOMs, was ihnen erhebliche Aufmerksamkeit verschafft. Die folgenden Abschnitte konzentrieren sich darauf, Hersteller, Entwickler und Integratoren von vernetzten Produkten (IoT/IIoT/OT) über die Bedeutung von SBOMs und die notwendigen Schritte zu ihrer Behandlung aufzuklären.

Die heutigen Produkte und Geräte basieren stark auf einer komplexen Kombination von Open-Source- und Drittanbieter-Softwarekomponenten, die aus der Lieferkette bezogen werden, zusätzlich zum intern entwickelten Code. Allerdings führt die Häufigkeit von extern entwickelter Software zu einem Mangel an Transparenz für Geräte- und Produkthersteller hinsichtlich der damit verbundenen Risiken. SBOMs wurden als regulatorische Anforderung eingeführt, um dieses Problem zu adressieren und eine Möglichkeit zu bieten, Transparenz und Kontrolle über die Risiken in der Lieferkette zu erlangen. Sie ermöglichen es Herstellern, die Softwareressourcen innerhalb ihrer Produkte und Geräte zu verstehen, über das hinaus, was von ihren Anbietern offengelegt wird.

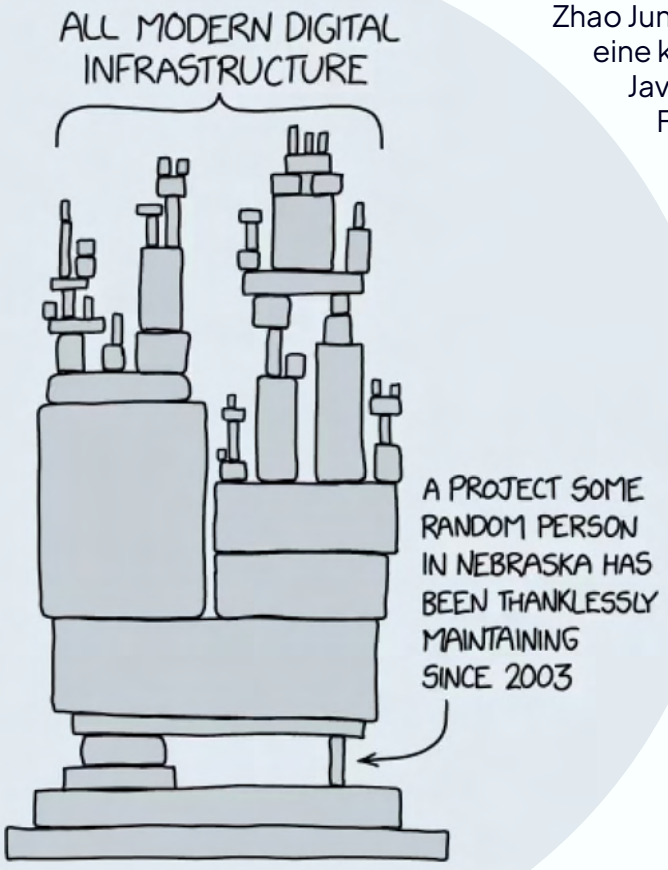
Die Erstellung eines SBOMs erfordert das Verständnis des Prozesses und der Inhaltsanforderungen. Darüber hinaus kann die Nutzung automatisierter SBOMs in Verbindung mit kontinuierlichem Bedrohungsmonitoring die Entwicklungseffizienz erheblich steigern und die Markteinführungszeit für Geräte und Produkte verkürzen, während gleichzeitig auf die sich entwickelnde Bedrohungslandschaft reagiert wird.

DIE SICH VERÄNDERNDE LANDSCHAFT DER SOFTWARE-LIEFERKETTEN: SBOMS UND IHRE HERAUSFORDERUNGEN

Cybersicherheitsvorfälle zeigen die Notwendigkeit von SBOMs

Die Bedeutung von SBOMs im Hinblick auf jüngste Cybersicherheitsvorfälle

Die Bedeutung von Software Bills of Materials (SBOMs) wurde durch zwei bedeutende Cybersicherheitsvorfälle unterstrichen. Im August 2021 hob die ONEKEY-Warnung schwerwiegende Sicherheitslücken im SDK von Realtek hervor, die eine Vielzahl von IoT-Geräten betrafen und Hunderttausende von Geräten gefährdeten. Diese Schwachstellen, die auf unzureichende Sicherheitspraktiken zurückzuführen sind, bestehen weiterhin in vielen Kundenprodukten, wie von Palo Alto Anfang 2023 aufgedeckt wurde. Dies verdeutlicht die dringende Notwendigkeit von Supply Chain Bills of Materials (SBOMs), die Transparenz und Verantwortlichkeit in der Softwareproduktion und -verteilung schaffen. SBOMs spielen eine entscheidende Rolle dabei, Schwachstellen zu identifizieren und zu beheben, bevor sie die Endbenutzer erreichen, und stärken so die Sicherheit von IoT-Ökosystemen.



Ein weiterer Vorfall ereignete sich im November 2021, als Chen Zhao Jun, ein Sicherheitsanalyst bei Alibaba Cloud Services, eine kritische Sicherheitslücke in der weit verbreiteten Java-Protokollierungsbibliothek Log4j an die Apache Foundation meldete. Diese Schwachstelle, bekannt als Log4Shell (CVE-2021–44228), löste eine weltweite Krise aus. Trotz der schnellen Veröffentlichung von Fixes nach der öffentlichen Bekanntmachung von Apache wurde Log4Shell rasch und umfassend ausgenutzt. IT-Organisationen hatten Schwierigkeiten zu identifizieren, ob ihre Lieferanten Log4j in ihre Produkte integriert hatten, was die Bemühungen zur Schadensminderung behinderte. Softwareanbieter wurden mit Anfragen überflutet und mussten nach Log4j in ihren eigenen Produkten suchen, während sie gleichzeitig versuchten, nachfolgende Fixes zu veröffentlichen. In vielen Fällen mussten sie auf ihre Lieferanten für Patches aus den upstream-Quellen zurückgreifen.

Infolgedessen blieben zahlreiche Organisationen sich der Gefahr nicht bewusst und unternahmen keine Maßnahmen.

Diese Vorfälle verdeutlichten zwei wichtige Lektionen: Zufällige Schwachstellen können verheerende Folgen haben, die vergleichbar mit Angriffen auf die Lieferkette sind, und das Management der Exposition gegenüber beiden Risikotypen ist in modernen, erweiterten Software-Lieferketten eine Herausforderung.

Sicherheitslücken könnten als Waffe eingesetzt werden

Zusätzlich weckten diese Vorfälle Bedenken hinsichtlich des möglichen Missbrauchs von Sicherheitslücken, wenn diese nicht öffentlich offengelegt werden, wie das Beispiel zeigt, dass Log4Shell möglicherweise heimlich als Waffe eingesetzt worden wäre, wenn es ausschließlich den chinesischen Behörden offengelegt worden wäre, wie es durch ein kürzlich verabschiedetes chinesisches Gesetz vorgeschrieben ist. Die Folgen dieser Ereignisse haben die Aufmerksamkeit der Regulierungsbehörden auf die kritische Bedeutung von Software-Lieferketten gelenkt.

Die Wiederverwendung von Komponenten hat die Produktivität gesteigert

Die weit verbreiteten Herausforderungen der Integration von Softwarekomponenten in der modernen Entwicklung.

In modernen Softwareentwicklungspraktiken liegt ein starker Fokus auf der Integration bestehender Softwarekomponenten, anstatt von Grund auf neu zu beginnen. Dieser Ansatz umfasst die Kombination einer kleineren Menge neuen Codes mit zahlreichen bereits vorhandenen Komponenten, einschließlich proprietärer und Open-Source-Bibliotheken und -Dienste. Die Fähigkeit, diese Softwarekomponenten wiederzuverwenden, hat die Abstraktion, das Teilen und den Verbrauch solcher Komponenten erheblich vorangetrieben, was zu erheblichen Verbesserungen der Produktivität von Entwicklern geführt hat.

Die IoT-Revolution hat die Verfügbarkeit hochgradig wiederverwendbarer eingebetteter und Cloud-Softwareplattformen effektiv genutzt. Diese Plattformen integrieren Lösungen für verschiedene Designherausforderungen zu niedrigen Kosten und ermöglichen so die weitverbreitete Einführung vernetzter eingebetteter Systeme.

Viele dieser Systeme verwenden ein „IoT-Betriebssystem“ oder eingebettetes Betriebssystem, oft in Form von Referenzcode des Mikrocontroller-Herstellers, zusammen mit zusätzlichem importiertem Code wie Peripherietreibern, Board-Support-Paketen und anwendungsspezifischen Bibliotheken. In zahlreichen Fällen umfasst dieser importierte Code die Mehrheit des gesamten Codes, der zwischen 90 % und 99 % des gesamten Codes ausmacht. Dieser Ansatz hat die Kosten für die Entwicklung von IoT/OT-Geräten erheblich gesenkt.

Das Importieren von Softwarekomponenten ist zu einer so alltäglichen und mühelosen Praxis geworden, dass viele Projekte diese ohne viel Überlegung einbeziehen, obwohl diese Komponenten oft zahlreiche Abhängigkeiten mit sich bringen. Alles, was den Projektfortschritt fördert, wird schnell übernommen. Allerdings haben sich mit der zunehmenden Verbreitung dieser Praxis drei bedeutende Herausforderungen herauskristallisiert.

Die erste Herausforderung besteht darin, dass Organisationen, die stark auf extern entwickelte Komponenten angewiesen sind, die Kontrolle über die Qualität und Sicherheit ihrer eigenen Software abgeben. Auch wenn sie modernste Qualitätstechniken in ihren eigenen Projekten anwenden, haben sie nur begrenzte Einflussmöglichkeiten auf die Qualität und Sicherheit der verwendeten externen Komponenten. Zudem haben sie möglicherweise nur eingeschränkte Transparenz über die gesamte Lieferkette jenseits ihrer direkten Lieferanten.

Die zweite Herausforderung liegt darin, mit Problemen und Sicherheitsupdates in einer Vielzahl von extern gepflegten Komponenten Schritt zu halten. Softwareanbieter müssen Sicherheitsbenachrichtigungen zu diesen Komponenten umgehend bewerten und darauf reagieren, da jede Schwachstelle Kunden Angriffen aussetzen kann. Diese Aufgabe effektiv zu managen, ist jedoch notorisch schwierig. Selbst Organisationen, die in diesem Bereich exzellent arbeiten, sind oft auf ihre Lieferanten angewiesen, um dasselbe zu tun.

Die dritte Herausforderung ergibt sich, wenn extern entwickelte Software unter mehreren Urheberrechtslizenzen bereitgestellt wird. Es ist leicht, den Überblick über die kumulierten Bedingungen dieser Lizenzen zu verlieren und unbeabsichtigt nicht konform zu werden.

Obwohl dies nicht direkt mit Cybersicherheit zu tun hat, stellt die Nichteinhaltung ein Risiko für Störungen durch mögliche Klagen der Urheberrechtsinhaber dar. Daher haben Unternehmensrechtsabteilungen begonnen, diesem Thema mehr Aufmerksamkeit zu schenken.

Während die Integration von Softwarekomponenten Vorteile in Bezug auf Produktivität und Kostensenkungen bietet, stellt sie auch erhebliche Herausforderungen bei der Sicherstellung von Qualität, Sicherheit und Compliance in der gesamten Lieferkette dar. Die Bewältigung dieser Herausforderungen erfordert, dass Organisationen das Management der Software-Lieferkette priorisieren, robuste Sicherheitspraktiken implementieren und eine effektive Kommunikation und Zusammenarbeit mit ihren Lieferanten etablieren.

Verstehen der Rolle und Herausforderungen von SBOMs im Risikomanagement der Lieferkette

Während Software Bills of Materials (SBOMs) erhebliche Aufmerksamkeit erhalten haben, ist es wichtig zu erkennen, dass sie keine eigenständige Lösung für Risiken in der Lieferkette darstellen. Stattdessen ermöglichen SBOMs effektive Lösungen, indem sie eine umfassende Liste von Softwarekomponenten bereitstellen.

Cybersicherheitstools, -prozesse und -richtlinien werden wirkungsvoller und weniger anfällig für blinde Flecken, wenn sie systematisch gegen ein sorgfältig gepflegtes SBOM angewendet werden. Daher sollte der Fokus auf der Implementierung eines breiteren Satzes von Lösungen liegen, anstatt sich ausschließlich auf SBOMs zu verlassen.

Es ist entscheidend zu verstehen, dass die Erstellung eines verwendbaren SBOMs schwieriger ist, als es zunächst erscheinen mag. Ein gut gestaltetes SBOM muss Softwarekomponenten universell und eindeutig identifizieren. Es sollte zusätzliche Informationen wie Abhängigkeitsbeziehungen, Wartende und Lizenzen enthalten, alles in einem standardisierten und weit verbreiteten Format.

Darüber hinaus sollte es Vollständigkeit über verschiedene Komponententypen hinweg anstreben und kontinuierlich aktualisiert werden, um Änderungen in der dokumentierten Software widerzuspiegeln. Ideal wäre es, wenn jede Softwarekomponente ihre eigenen Abhängigkeiten dokumentiert, was die Erstellung eines umfassenden SBOMs erleichtern würde.

Es ist erwähnenswert, dass SBOMs nicht ganz neu sind. Viele Betreiber von IoT/OT-Bibliotheken und Geräten verwenden bereits eine Art Softwareinventar, um diese Herausforderungen zu adressieren oder ihre Anwendungen zu erstellen.

Zudem haben mehrere Anbieter die Fähigkeit, automatisch qualitativ hochwertige SBOMs zu generieren, auch wenn sie diese derzeit nicht nutzen. Neu ist das wachsende Interesse, das durch regulatorische Initiativen vorangetrieben wird, die Sicherheitslage in der Lieferkette zu verbessern. Dies umfasst die Standardisierung und Kommunikation von SBOMs entlang der Lieferketten sowie erhöhte Erwartungen an deren effektive Nutzung.

In den folgenden Abschnitten werden wir die wesentlichen Komponenten und Hauptstandards für SBOMs skizzieren. Wir werden auch erörtern, wie IoT/OT-Anbieter SBOMs erstellen und teilen sollten sowie wie alle Stakeholder in der IoT/OT-Lieferkette SBOMs effektiv nutzen können, um Cybersicherheitsrisiken für IoT/OT-Betreiber zu mindern.

Die ONEKEY Product Cybersecurity & Compliance Platform (OCP) ermöglicht es Herstellern, ihr Produkt-Sicherheitsmanagement von der Gestaltung bis zum Ende des Lebenszyklus zu automatisieren, über den gesamten Produktlebenszyklus hinweg:

Die einzigartige und proprietäre Binärextraktionstechnologie von ONEKEY ermöglicht eine tiefere und präzisere Analyse des Binärfirmware-Images ohne die Notwendigkeit von Quellcode.

ONEKEY generiert automatisch ein detailliertes SBOM, einschließlich Softwareabhängigkeiten auf allen Ebenen der Firmware.

Anschließend verwendet ONEKEY basierend auf künstlicher Intelligenz (KI) und maschinellem Lernen einen Natural Language Processing (NLP)-Ansatz, um festzustellen, ob es öffentlich bekannte Schwachstellen gibt, die diese Softwareversion betreffen. Darüber hinaus analysiert der KI/ML-basierte Ansatz von ONEKEY automatisch die Voraussetzungen für die Ausnutzbarkeit der Schwachstellen. In einer integrierten, automatisierten Auswirkungsbewertung wird das Zielgerät daraufhin analysiert, ob die Voraussetzungen für die Ausnutzbarkeit erfüllt sind, wobei nicht relevante Schwachstellen herausgefiltert werden. Dieser einzigartige Ansatz verkürzt die Reaktionszeiten erheblich, indem er die manuelle Auswirkungsbewertung deutlich reduziert und es den Entwicklungs- und ProductSecurity Incident Response Teams (PSIRT) ermöglicht, sich auf die wirklich relevanten Schwachstellen zu konzentrieren.

Die ONEKEY Product Cybersecurity & Compliance Platform (OCP) stellt SBOMs sofort zur Verfügung – bereit für den Export in CycloneDX oder andere Formate

ONEKEY kann ein SBOM einfach aus einem binären Firmware-Image generieren. Das SBOM kann sowohl in maschinenlesbaren Formaten (z. B. CycloneDX, SPDX) als auch in menschenlesbaren Formaten (CSV, EXCEL) exportiert werden, um es anderen Systemen, Endbenutzern und Aufsichtsbehörden zur Verfügung zu stellen.

Das Firmware-Monitoring von ONEKEY analysiert täglich das Zielprodukt auf neue Zero-Day-Schwachstellen oder bekannte Schwachstellen und führt automatische, KI/ML-basierte Auswirkungsbewertungen für alle identifizierten Schwachstellen durch. Dies ermöglicht es Herstellern, schnell auf neue Schwachstellen zu reagieren und Sicherheits-Patches zu erstellen und zu verteilen.

Analyse und Überwachung für automatisierte Sicherheitsprüfung von Drittanbieterkomponenten – richten Sie ONEKEY einfach als Security Gate für jede Drittanbieterkomponente oder jedes Produkt ein.

VERSTÄNDNIS DES SBOM-INHALTS UND DER DAMIT VERBUNDENEN HERAUSFORDERUNGEN

NTIA-Mindestanforderungen für SBOMs

Die National Telecommunications and Information Administration (NTIA) der Vereinigten Staaten hat einen bedeutenden Beitrag zum Verständnis von SBOMs geleistet. Laut der NTIA besteht der Hauptzweck eines SBOM darin, Komponenten und ihre Beziehungen eindeutig und unmissverständlich zu identifizieren. Zu diesem Zweck umfassen die Mindestanforderungen an Datenelemente den Lieferanten, den Komponentennamen, die Komponentenversion, andere eindeutige Kennungen, Abhängigkeitsbeziehungen, den Autor der SBOM-Daten und den Zeitstempel. Zusätzlich zu diesen Mindestanforderungen kann ein SBOM auch zusätzliche Daten wie den SPDX-Lizenzkurz-ID und/oder den Lizenztext enthalten, je nach den spezifischen Bedürfnissen und Präferenzen der beteiligten Interessengruppen.

Identifikatoren sind für effektive Schwachstellen-Suche nützlich

Eine wichtige Anwendung von Software Bills of Materials (SBOMs) ist die Identifizierung von Schwachstellen aus Datenbanken. Um eine effiziente Schwachstellensuche zu ermöglichen, ist es vorteilhaft, wenn ein SBOM Kennungen enthält, die den Komponenten innerhalb dieser Datenbanken entsprechen. Zum Beispiel verwendet die National Vulnerability Database (NVD) der Vereinigten Staaten Common Platform Enumerations (CPEs) als Kennungen. Anfangs wurden CPEs den Komponenten zugewiesen, als Schwachstellen erstmals gemeldet wurden, was Herausforderungen bei der Einrichtung proaktiver automatisierter Suchen mit sich brachte. Eine mögliche Lösung besteht darin, dass Bibliotheks- und Gerätebetreiber eine CPE vorab registrieren. Es wird jedoch erwartet, dass die NVD möglicherweise CPEs zugunsten von Software Identification (SWID)-Tags aufgibt.

Ein empfohlener Ansatz besteht darin, lokal eine SWID zu generieren und daraus eine CPE abzuleiten, die beide als eindeutige Kennungen in SBOMs, die mit Kunden geteilt werden, integriert werden. Anschließend können der CPE-Name, SWID oder beide in der NVD oder einer anderen relevanten Schwachstellendatenbank registriert werden, je nach Bedarf. Die NTIA erkennt jedoch die Unpraktikabilität an, ein globales Namensschema zu etablieren, und schlägt vor, dass Software- und Gerätebetreiber eindeutige Lieferanten-, Komponenten- und Versionsnamen definieren und konsequent verwenden.

Idealerweise sollten diese Namen mit Hashes, UUIDs oder anderen eindeutigen Kennungen ergänzt werden.

In Fällen, in denen der ursprüngliche Lieferant einer Komponente seine bevorzugten Komponentennamen nicht in einem SBOM bereitgestellt hat, dürfen nachgelagerte Integratoren eine fundierte Vermutung anstellen und diesen Umstand mit dem „Autor der SBOM-Daten“-Element dokumentieren.

Vier mögliche Informationsquellen

Rationalisierung der SBOM-Generierung in CI/CD-Pipelines: Automatisierung und Informationsquellen

Die Automatisierung der Generierung von Software-Stücklisten (SBOMs) in Pipelines für kontinuierliche Integration/kontinuierliche Bereitstellung (CI/CD) ist von entscheidender Bedeutung. Es gibt vier potenzielle Informationsquellen für die SBOM-Generierung, von denen jede ihre eigenen Tools und Vorteile bietet.

1. **Paketmanager:** Häufig verwendete Paketmanager wie pip, Maven, npm und Cargo können Abhängigkeiten auflisten und wertvolle Informationen für die Generierung einer SBOM bereitstellen. Selbst in eingebetteten C/C++-Umgebungen, in denen Paketmanagement weniger verbreitet ist, können Build-Systeme wie Cmake oder Dienstprogramme wie West von Zephyr Project genutzt werden.

2. **Scannen des Quellcodes:** Tools zur Quellcodeanalyse und Scripting können Abhängigkeiten, verknüpfte Bibliotheken und eingebetteten Code effizient identifizieren. Tools zur kommerziellen Quellcodeanalyse (SCA) können auch kopierte und eingefügte Codefragmente erkennen. Dieser Ansatz erfordert zwar eine anfängliche Einrichtung und laufende Wartung, ist aber in CI/CD-Pipelines äußerst effektiv und lässt sich leicht automatisieren.



3. **Binäre Analyse:** Binärdateien können analysiert werden, um SBOM-Informationen zu extrahieren, wenn der Quellcode nicht verfügbar ist. Reverse-Engineering-Tools können Symbolnamen und Zeichenketten aus ELF- und Objektdateien extrahieren, sie jedoch in Komponentenidentitäten auflösen ist herausfordernd. Für verschiedene Arten von ausführbaren Dateien, Mikrocontroller- und Linux-Disk-Images, Patch-Dateien, Paketen und Over-the-Air-Update-Wrappern sind spezielle Analyseansätze erforderlich.

4. **SBOM-Dokumentation aus der Lieferkette:** SBOMs können von jedem Teilnehmer der Lieferkette unter Verwendung von Originalmetadaten, Quellen und vorgelagerter SBOM-Dokumentation generiert werden. Durch die gemeinsame Nutzung nach-

gelagerter SBOMs kann eine vollständigere und genauere Geräte-SBOM erstellt werden, wodurch Einschränkungen bei der Sichtbarkeit einer einzelnen Quelle überwunden werden. Die Praxis der umfassenden SBOM-Dokumentation befindet sich jedoch noch in der Entwicklung, und es kommt häufig vor, dass Projekten keine SBOMs für alle importierten Komponenten fehlen.

Die Automatisierung der Generierung und gemeinsamen Nutzung von SBOMs erfordert Zeit- und Arbeitsaufwand, aber die Verfügbarkeit von Tools hat den Prozess vereinfacht. Das Ausmaß des Aufwands skaliert mit der Größe und Komplexität des Projekts. Entwickler kleinerer IoT-Bibliotheken können ihrem Versionsskript einen Befehl hinzufügen, während größere eingebettete Projekte möglicherweise mehrere Monate an Detektivarbeit, Konsolidierung der Informationsquellen, Umwandlung in ein Standardformat und Automatisierung erfordern. Die positiven Vorteile der Automatisierung der SBOM-Generierung rechtfertigen den Aufwand in beiden Fällen.

Bedenken bezüglich der Sicherheitsinformationen in SBOMs?

Gemeinsame Nutzung von SBOMs: Vorteile für Verteidiger, die Sicherheitsbedenken überwiegen

Die gemeinsame Nutzung nachgelagerter SBOMs sollte automatisiert und einheitlich unter Verwendung einer kleinen Anzahl empfohlener Methoden10 für verschiedene Arten von Komponenten erfolgen.

Bedenken können hinsichtlich der Sicherheitsempfindlichkeit von SBOMs auftreten, insbesondere bei Binärdateien und Geräte-Images. Könnte der Zugriff auf eine Geräte-SBOM Angreifern dabei helfen, importierte Sicherheitslücken zu identifizieren, sie auszunutzen oder Angriffe auf die Lieferkette zu planen?

Transparenz birgt zwar einige Risiken, aber es ist wichtig zu verstehen, dass SBOMs in erster Linie Verteidigern und nicht Angreifern zugute kommen. Angreifer benötigen nicht unbedingt eine SBOM, um Sicherheitslücken zu finden; sie zielen häufig auf ungepatchte Sicherheitslücken ab, von denen sie bereits Kenntnis haben. Auf der anderen Seite können Verteidiger SBOMs als systematische Verteidigung gegen Risiken in der Software-Lieferkette nutzen. Selbst Unternehmen, die SBOMs nur an ihre Kunden verteilen, betrachten die Offenlegung nicht als Katastrophe und versuchen nicht, sie weiter abzusichern.

Zusammenfassend lässt sich sagen, dass die gemeinsame Nutzung von SBOMs den Verteidigern erhebliche Vorteile bei der Bekämpfung von Risiken in der Softwarelieferkette bietet, und die Bedenken, dass Angreifer SBOMs nutzen, werden durch die Vorteile, die sie für die Verteidigungsmaßnahmen bieten, aufgewogen werden.

Die beiden führenden SBOM-Standardformate

Standardisierung von SBOMs: CyclonedX und SPDX

Um den Austausch zu erleichtern und die Entwicklung interoperabler Tools und Dienste zu fördern, ist die Annahme von SBOM-Standards (Software Bill of Materials) unerlässlich. Die Übernahme eines dieser Standards vereinfacht die Generierung, Nutzung und gemeinsame Nutzung von SBOMs und senkt gleichzeitig die Kosten. Ein umfassender Überblick über die aktuellen Standards wurde von der NTIA 11 veröffentlicht.

Die beiden führenden Standards in diesem Bereich sind CyclonedX und der Software Product Data Exchange (SPDX). CyclonedX hat seinen Ursprung in der OWASP-Community für Informationssicherheit, während SPDX aus der OSS-Community hervorgegangen ist. Obwohl auch SWID-Tags in Betracht gezogen wurden, besteht ihr primärer Anwendungsfall darin, eindeutige und eindeutige Identifikatoren für Softwarekomponenten bereitzustellen.

Der ursprüngliche Zweck von SPDX besteht darin, die Einhaltung der Lizenzbestimmungen sicherzustellen. Es wird von einer Arbeitsgruppe innerhalb der Linux Foundation verwaltet. Der erste Entwurf wurde 2010 eingeführt, und die aktuelle Spezifikation ist als ISO/IEC-Norm ISO/ IEC 5962:2021 12 frei verfügbar. Der laufende Entwicklungsfortschritt kann über das öffentliche GitHub-Repository der Gruppe verfolgt werden.

CyclonedX hingegen wurde ursprünglich für die Identifizierung von Sicherheitslücken, die Einhaltung von Lizenzbestimmungen und die Analyse veralteter Komponenten entwickelt. Es folgt einem offenen Verwaltungsmodell. Der erste Spezifikationsentwurf wurde 2017 eingeführt, und der Standard hat nun Version 1.4 erreicht. Beide Standards wurden ausgiebig genutzt, was zu ihrer Reife geführt hat. Sie verfügen über aktive Gemeinschaften und werden kontinuierlich weiterentwickelt.

Reiche Untergüsse sind die besten

Sie sind bestrebt, alle SBOM-Anwendungsfälle zu unterstützen, und genießen breite Unterstützung durch verschiedene kompatible Tools. Viele Tools bieten sogar Unterstützung für beide Standards. Keines von ihnen bietet jedoch spezifische Vorteile für eingebettete Projekte.

SBOM-Vollständigkeit: Herausforderungen und Überlegungen

Der Nutzen einer SBOM (Software Bill of Materials) steigt mit ihrer Genauigkeit, ihrem Detaillierungsgrad und ihrer Vollständigkeit. Es ist jedoch wichtig, sich darüber im Klaren zu sein, dass SBOMs selten in der Lage sind, all diese Eigenschaften zu erreichen, und dass es schwierig sein kann, ihre Qualität objektiv zu messen.

Ein interner Versuch, eine SBOM zu generieren, kann einige Kennzahlen liefern, z. B. den Anteil der zugewiesenen Code-Artefakte oder die Anzahl der identifizierten Komponenten mit erkannten inkompatiblen Lizenzen. Bei diesen Metriken können jedoch wichtige Komponenten übersehen werden, einschließlich „unbe-

kannter Unbekannter“, die noch nicht berücksichtigt wurden.

Selbst nicht eingebettete Softwareprojekte haben Schwierigkeiten bei der Identifizierung und Dokumentation von Softwarekomponenten verschiedener Typen und Ebenen, wie Binärdateien, Quellcode, paketverwaltete und nicht paketverwaltete Komponenten, containerisierte Anwendungen, statische und dynamische Bibliotheken.

IoT-Geräte haben zusätzliche Herausforderungen

IoT-Geräte stellen zusätzliche Herausforderungen dar, da sie den gesamten Stack vom Bare-Metal-Boot an umfassen und häufig tief eingebettete Firmware in Netzwerkschnittstellencontrollern (NICs), sicheren Elementen und anderen integrierten Schaltungen enthalten. Nur durch die sorgfältige und sorgfältige Inventarisierung undurchsichtiger und „versteckter“ Softwarekomponenten lassen sich diese in „bekannte Unbekannte“ umwandeln. “

Wenn ein Upstream-Lieferant nachgeschalteten Verbrauchern eine SBOM zur Verfügung stellt, kann nicht einfach sichergestellt werden, dass sie deren Standards erfüllt. Derzeit gibt es kein Standard- oder Zertifizierungssystem für diesen Zweck. Einige Verbraucher generieren und analysieren SBOMs selbst mithilfe ihrer eigenen Tools zur Softwarekompositionsanalyse (SCA), was Lieferanten dazu bewegen kann, ihre SBOMs zu verbessern. Die Verbraucher verlassen sich bei der Interpretation jedoch immer noch auf die Anbieter, und für viele ist der erforderliche Aufwand möglicherweise nicht gerechtfertigt.

Letztlich ist es wichtig, sich daran zu erinnern, dass selbst eine unvollständige SBOM besser ist, als gar keine SBOM zu haben. Durch den Einsatz von SBOMs können Compliance-Probleme und bekannte Sicherheitslücken zwar erheblich reduziert werden, es ist jedoch unwahrscheinlich, dass sie beseitigt werden.

STÄRKUNG DER SICHERHEIT UND KONFORMITÄT DER SOFTWARE-LIEFERKETTE

Bei Nichteinhaltung von Open-Source-Lizenzen besteht das Risiko rechtlicher Schritte

Rationalisierung der Einhaltung von Open-Source-Softwarelizenzen im Bereich IoT/OT

Die eingebettete Software eines IoT-Geräts besteht oft aus komplexen, aber im Wesentlichen standardisierten Funktionen,



die bis zu 90 % des Code-Basis ausmachen können. Die Kosten für die Entwicklung und Wartung eines solchen Software-Stacks übersteigen jedoch häufig die Mittel der meisten Hersteller eingebetteter Produkte. Daher beziehen Originalgerätehersteller (OEMs) diese Software von Bibliotheks- und Betriebssystemanbietern sowie von Open-Source-Software (OSS)-Projekten. Infolgedessen enthalten die meisten IoT-Geräte eine erhebliche Menge an Drittanbieter-Software, deren Urheberrecht beim ursprünglichen Ersteller verbleibt. Nutzer und Betreiber dieser Geräte dürfen diese Software nur im Rahmen der Lizenzvereinbarungen der Urheberrechtsinhaber verwenden. Während Lizenzen die Bedingungen festlegen können, die der Urheberrechtsinhaber auswählt, verwenden die meisten Open-Source-Software-Projekte standardisierte Lizenzformen, um die Einhaltung zu vereinfachen.

Die Nichteinhaltung der Bedingungen dieser Lizenzen setzt die Nutzer und Betreiber von IoT-Geräten dem Risiko rechtlicher Schritte durch die Urheberrechtsinhaber aus. Während die meisten Fälle im Zusammenhang mit Open-Source-Software (OSS) einvernehmlich gelöst werden, können Situationen, die kommerzielle Software, Zusammenbrüche im guten Willen oder Szenarien von Copyright-Trolling betreffen, zu erheblichen finanziellen Konsequenzen und Betriebsstörungen führen. Angestoßen durch einige prominente Rechtsstreitfälle haben viele Organisationen SBOMs eingeführt, um das Risiko von Lizenzverstößen zu verringern. Interessanterweise ist es oft der General Counsel und nicht der CTO oder CISO, der diese Initiative vorangetrieben hat.

Open Chain wird für eigene OSS-Lizenzprogramme empfohlen

Während der Beschaffung haben die Betreiber begonnen, von den Lieferanten den Nachweis der vollständigen Lizenzkonformität zu verlangen. Als Reaktion darauf haben die Lieferanten dieser Nachfrage teilweise entsprochen, indem sie SBOMs zur Verfügung stellten, in denen Softwarekomponenten und ihre jeweiligen Lizenzen aufgeführt sind. Die Betreiber können jedoch keine Garantie für die Vollständigkeit übernehmen und Richtigkeit solcher SBOMs, was sie dazu veranlasst, Schadensersatz für urheberrechtliche Ansprüche zu verlangen. Obwohl die Rechtsabteilung von Softwareanbietern kein Konzept ist, mit dem General Counsel vertraut sind, haben die Rechtsteams der Softwareanbieter im Laufe der Zeit einen Mittelweg mit den Ingenieurteams gefunden. Wenn das Inventar der OSS-Software umfassend und gut gepflegt ist und die Techniker darauf achten, ungewöhnliche Lizenzen zur Überprüfung zu identifizieren, können General Counsel unabhängig von der Anzahl der beteiligten OSS-Komponenten darauf vertrauen. IoT-/OT-Anbietern, die ein eigenes Programm zur Einhaltung der OSS-Lizenzen benötigen, wird die Implementierung des OpenChain-Standards (ISO/IEC 5230) 14 empfohlen.

Dieser Standard wurde von Pionieren solcher Programme als gemeinnütziger Dienst entwickelt. Wie SPDX ist es ein frei verfügbarer ISO-Standard, der aufgrund seiner Einfachheit und nachgewiesenen Wirksamkeit von technischen Abteilungen, Rechtsteams in Unternehmen und der OSS-Community weithin akzeptiert wird.

Vex hilft bei der Bewertung der Ausnutzbarkeit

Verbesserung des Schwachstellenmanagements in IoT/OT-Lieferketten

IoT/OT ist einem zunehmenden Risiko von Cyberangriffen ausgesetzt, wobei ungepatchte Software-Sicherheitslücken eine erhebliche Bedrohung darstellen. In der breiteren IT-Landschaft tragen diese Sicherheitslücken bekanntermaßen zu jeder dritten Verletzung der Informationssicherheit bei 15 16. Folglich ist die Verkürzung der Zeit zwischen der Entdeckung von Sicherheitslücken und der Implementierung von Abhilfemaßnahmen zu einem wichtigen Ziel für die gesamte IoT/OT-Lieferkette geworden.

Tools und Best Practices sind zwar im Entstehen begriffen, aber die Einrichtung eines effektiven Schwachstellenmanagementprogramms bleibt eine Herausforderung. Obwohl Sicherheitslücken in der Regel zusammen mit Patches oder Abhilfemaßnahmen angekündigt werden, benötigen IT-Organisationen im Durchschnitt 60 bis 200 Tage, um diese Patches zu installieren. Zu den Faktoren, die zu dieser Verzögerung beigetragen haben, gehören ein Mangel an Situationsbewusstsein, was zu übersehenen Sicherheitslücken führt, und die Überforderung der SecOps-Teams, wenn ein verbessertes Bewusstsein zahlreiche Sicherheitslücken aufdeckt.

IoT-/OT-Anbieter, die sich für den Schutz ihrer Produkte einsetzen, sind jedoch bestrebt, die Risiken zu vermeiden, die mit ungepatchten Sicherheitslücken verbunden sind. Im Bereich des Schwachstellenmanagements entwickelt die National Telecommunications and Information Administration (NTIA) derzeit den Vulnerability Exploitability eXchange (VEX siehe 17). VEX ergänzt die Software Bill of Materials (SBOMs) und ermöglicht es Geräteherstellern, die Ausnutzbarkeit der in ihren Softwarekomponenten entdeckten Sicherheitslücken mitzuteilen. Mithilfe von VEX können Unternehmen feststellen, ob sich eine in einer SBOM aufgeführte Sicherheitslücke auf ihre Produkte auswirkt, ohne dass umfangreiche Untersuchungen erforderlich sind.

VEX ermöglicht es OEMs, zu beurteilen, ob Sicherheitslücken in den von ihnen verwendeten Komponenten im Produkt ausnutzbar sind. Faktoren wie Codeausführung, bedingte Kompilierungsanweisungen und bestehende Sicherheitskontrollen bestimmen, ob eine Sicherheitslücke ein Risiko darstellt. Dieses Wissen spart Entwicklern Zeit, da sie sich auf die Behebung von Sicherheitslücken konzentrieren, die eine echte Bedrohung darstellen, und nicht auf unnötige Korrekturen.

Vex allein macht nicht die (Ausnutzbar-keits-)Geschichte

VEX liefert zwar wertvolle Erkenntnisse, es wird jedoch empfohlen, diese mit kontextbasierten Analysen zu kombinieren, um die Risiken in der Lieferkette weiter zu minimieren. Die erweiterte kontextbasierte Analyse umfasst Hardwarearchitektur, Betriebssystemkonfigurationen, Verschlüsselungsmechanismen, Kontrollabläufe und API-Aufrufe und bietet so ein umfassendes Verständnis der Sicherheitslücken eines Produkts.

Um die Transparenz und Sichtbarkeit zu erhöhen, schlägt die NTIA vor, die SBOM-Anwendungsfälle zu erweitern, und ermutigt Unternehmen, zusätzliche Datenfelder wie Komponenten-Hash, Lebenszyklusphase, Beziehungen und Lizenzinformationen anzufordern.

Es betont auch die Notwendigkeit, SBOMs für Cloud-basierte Software und SaaS zu erstellen und zu verwalten, Integrität und Authentizität durch Mechanismen wie digitale Signaturen sicherzustellen, Links zu externen Schwachstellendatenquellen herzustellen, Schwachstellen und Ausnutzbarkeit von Abhängigkeiten mithilfe von VEX zu bewerten, binäre Analysetools für ältere Software einzusetzen und die Flexibilität und Einheitlichkeit der Implementierung aufrechtzuerhalten.

Durch die Kombination automatisierter Tools wie VEX, umfassender SBOMs und kontextsensitiver Schwachstellenanalysen können Unternehmen Schwachstellen in der Lieferkette effizient verwalten und ihre allgemeine Sicherheitslage stärken.

SBOMs als Top-Liste

Gewährleistung der Lieferkettensicherheit in IoT/OT-Umgebungen

Das Management von Lieferkettenrisiken erfordert oft, dass Lieferanten nachweisen, dass sie bestimmte Richtlinien einhalten. Dazu gehören Ursprungsregeln, sichere Softwareentwicklungsstandards und Wartungsverpflichtungen. Im Idealfall würden Softwarelieferanten anhand allgemein anerkannter Kennzahlen, die optional von unabhängigen Dritten zertifiziert werden, selbst über ihre Leistung in Bezug auf die Einhaltung der Sicherheitsvorschriften in der Lieferkette berichten. Derzeit müssen Unternehmen jedoch ihre eigenen Recherchen durchführen und die Ergebnisse in ihren eigenen Metriken abbilden, wobei sie eine SBOM als To-do-Liste verwenden. IoT-/OT-Softwareanbieter sind bestrebt, qualitativ hochwertige Software bereitzustellen, um Kunden zufrieden zu stellen, den Umsatz zu steigern, die Supportkosten zu senken und sich auf die Entwicklung neuer Produkte zu konzentrieren. Die Sicherstellung gleichbleibender Qualität und Sicherheit durch Upstream-Entwickler ist jedoch eine Herausforderung, da für viele Entwickler keine formalen Anforderungen gelten.

Nach der Umsetzung interner Richtlinien sollten importierte Komponenten auf das gleiche Konformitätsniveau gebracht werden.

Die vollständige Einhaltung der Vorschriften kann einige Zeit in Anspruch nehmen, aber eine SBOM kann als To-do-Liste dienen, um die Compliance-Pläne und Fortschritte aufzuzeichnen. Bei kleinen Open-Source-Softwarekomponenten (OSS) empfiehlt sich die Zusammenarbeit, entweder indem sie abgezweigt und die Einhaltung der Vorschriften in das Produkt integriert wird, oder indem Verbesserungen im Vorfeld vorgenommen werden.

Informelle OSS-Komponenten können mit Wartungsverpflichtungen zu kämpfen haben, aber aktuelle Aktivitäten und die Behandlung von Defekten können genutzt werden, um Wartungserwartungen zu extrapolieren oder Wartungsverträge zu prüfen. Die Abwägung zwischen OSS und Sicherheit in der Softwarelieferkette ist eine sich ständig weiterentwickelnde Praxis, für die noch weitere Einzelheiten ausgearbeitet werden müssen.

Bei der Implementierung von Sicherheitsprogrammen für die Lieferkette sollten Erstausrüster (OEMs) von IoT-/OT-Geräten mehrere Faktoren berücksichtigen, wie z. B. Gerätedesign, Herstellung, Bereitstellungsprozesse und die Softwarelieferkette. Umgekehrt müssen sich die Betreiber bewusst sein, dass die Zusammenarbeit mit Lieferanten, die keine angemessenen Investitionen in Qualität und Sicherheit getätigt haben, sie immer größeren Sicherheitslücken aussetzt.

Priorisieren Sie Ihr SBOM-Projekt entsprechend Ihrer Produktkritikalität

Die Dringlichkeit der Bewertung der Lieferkettensicherheit während des Beschaffungsprozesses hängt von der Wichtigkeit der betreffenden Anträge ab. Um diese Bewertung einzuleiten, ist es ratsam, dass sich die Betreiber anhand einer Software-Stückliste (SBOM) bei OEM-Lieferanten über die Lieferkette, einschließlich der Softwarelieferkette, erkundigen. Darüber hinaus ist es wichtig, die Integrität und Qualität der Anlagen sicherzustellen. Zwar gibt es derzeit keinen umfassenden Standard für die IoT-/OT-OEM-Zertifizierung, aber Betreiber sollten ihre eigenen Kriterien festlegen, die auf verschiedenen Aspekten basieren, wie z. B. der Widerstandsfähigkeit der Geräte gegenüber Angriffen, der Integrität von Softwarebeständen, der Vertraulichkeit von Gerätegeheimnissen und der Kontrolle der Vertrauensketten von Zertifikaten. Wenn es um Sicherheitsanforderungen in der Software-Lieferkette geht, ist es ratsam, sie wie andere Anforderungen in Form messbarer Ergebnisse zu formulieren. Da die genaue Anzahl der ausnutzbaren Sicherheitslücken nicht bestimmt werden kann, ist es sinnvoll, sich auf Stellvertreterkennzahlen wie Kennzahlen zur Codequalität, durchschnittliche Reaktionszeit und Einhaltung bewährter Verfahren zu verlassen. Für IoT-/OT-Betreiber ist es wichtig, einen bestimmten Satz von Metriken auszuwählen oder zu erstellen, die ihren Bedürfnissen entsprechen, wie der Ansatz, den die US-Bundesregierung mit EO 14028 verfolgt hat.

Ein Ausblick auf CSAF

Die Integration des Cybersecurity Assurance Framework (CSAF) in die Sicherheitsbemühungen der Lieferkette sorgt für eine zusätzliche Robustheit. CSAF bietet einen strukturierten Ansatz zur Bewertung und Verbesserung der Cybersicherheitspraktiken in

der gesamten Lieferkette. Durch die Nutzung von CSAF können Unternehmen klare Benchmarks für Compliance und Leistung festlegen und so eine reibungslosere Zusammenarbeit mit Lieferanten ermöglichen.

Dieses Framework bietet eine standardisierte Sprache für die Erörterung von Cybersicherheitsmaßnahmen und gewährleistet eine umfassendere Bewertung der Sicherheitslage. Die Implementierung von CSAF zusammen mit SBOMs und anderen Kennzahlen kann die allgemeine Sicherheitslage von IoT-/OT-Umgebungen erheblich verbessern.

In Zukunft sollten Unternehmen die Synergien zwischen CSAF und bestehenden Sicherheitsstrategien für die Lieferkette untersuchen, um ein widerstandsfähigeres und sichereres Ökosystem aufzubauen.

WICHTIGE ERKENNTNISSE FÜR EIN EFFEKTIVES UND EFFIZIENTES SBOM-MANAGEMENT:

- **Zentralisieren Sie das SBOM-Management** - Verschaffen Sie sich einen umfassenden Einblick in Ihre Lieferkette, Software von Drittanbietern und den internen Code aller Komponenten, Produkte und Geschäftsbereiche.
- **Vereinfachen Sie die Compliance-Verfahren** - Erstellen, überprüfen und generieren Sie im Handumdrehen Berichte, um mühelos Branchenstandards einzuhalten, wie sie beispielsweise von der FDA, ISO und anderen Stellen festgelegt wurden.
- **Integrieren Sie die SBOM-Erstellung in aktuelle Workflows** - Integrieren Sie problemlos in Ihre vorhandenen Systeme wie PLM, CI/CD und Softwareupdate-Mechanismen und unterstützen Sie gleichzeitig alle SBOM- und VEX-Formate, einschließlich CyclonedX und SPDX, mit Import- und Exportfunktionen.
- **Gehen Sie über einfache SBOMs hinaus** - Enthüllen Sie alle damit verbundenen Risiken, die über reine SBOMs hinausgehen und HW-Stücklisten, Kryptografie, Passwörter, PII, Betriebssystemkonfigurationen und mehr umfassen.

- **Priorisieren Sie Sicherheitsforschung vor SBOM-Verifizierung** - Vermeiden Sie den teuren und arbeitsintensiven Prozess manueller Audits, sodass Sie Ihre Zeit effektiv darauf verwenden können, Risiken zu minimieren und wichtige Sicherheitslücken zu beheben.
- **Seien Sie bereit für Audits** - Stellen Sie sicher, dass SBOMs auf die Einhaltung gesetzlicher Vorschriften vorbereitet sind und schnell geteilt oder exportiert werden können, sodass Sie sich auf die Sicherung zukünftiger Vorhaben konzentrieren können.

Möchten Sie sich weiter mit unseren Sicherheitsexperten austauschen, um zu erfahren, wie Sie die Cybersicherheit Ihrer Produkte durch effektives und effizientes SBOM-Management sicherstellen können?

Kontaktieren Sie bitte unsere Sicherheitsexperten unter: experts@onekey.com



ONEKEY
onekey.com
+49 211 1587 41 04
info@onekey.com

SecurITy made in Germany

© 2025 ONEKEY. Alle Rechte vorbehalten. Vervielfältigung nur mit Genehmigung von ONEKEY gestattet. Alle aufgeführten Marken sind die Marken der jeweiligen Eigentümer. Irrtümer, Änderungen und Verfügbarkeiten der aufgeführten Produkte, Dienstleistungen , Eigenschaften und Anwendungsmöglichkeiten bleiben vorbehalten. ONEKEY übernimmt keine Gewähr für Auskünfte Dritter über Eigenschaften, Leistungen und Verwendbarkeit. ONEKEY behält sich vor, Produkte und Leistungen im Rahmen der Produktentwicklung auch ohne vorherige Ankündigung zu ändern. Bei Abweichungen von den Vertragsunterlagen und Allgemeinen Geschäftsbedingungen von ONEKEY und deren verbundenen Unternehmen und Tochtergesellschaften in Verbindung mit diesem Dokument haben die Vertragsunterlagen und Allgemeinen Geschäftsbedingungen stets Vorrang vor diesem Dokument.

V2024090IDE