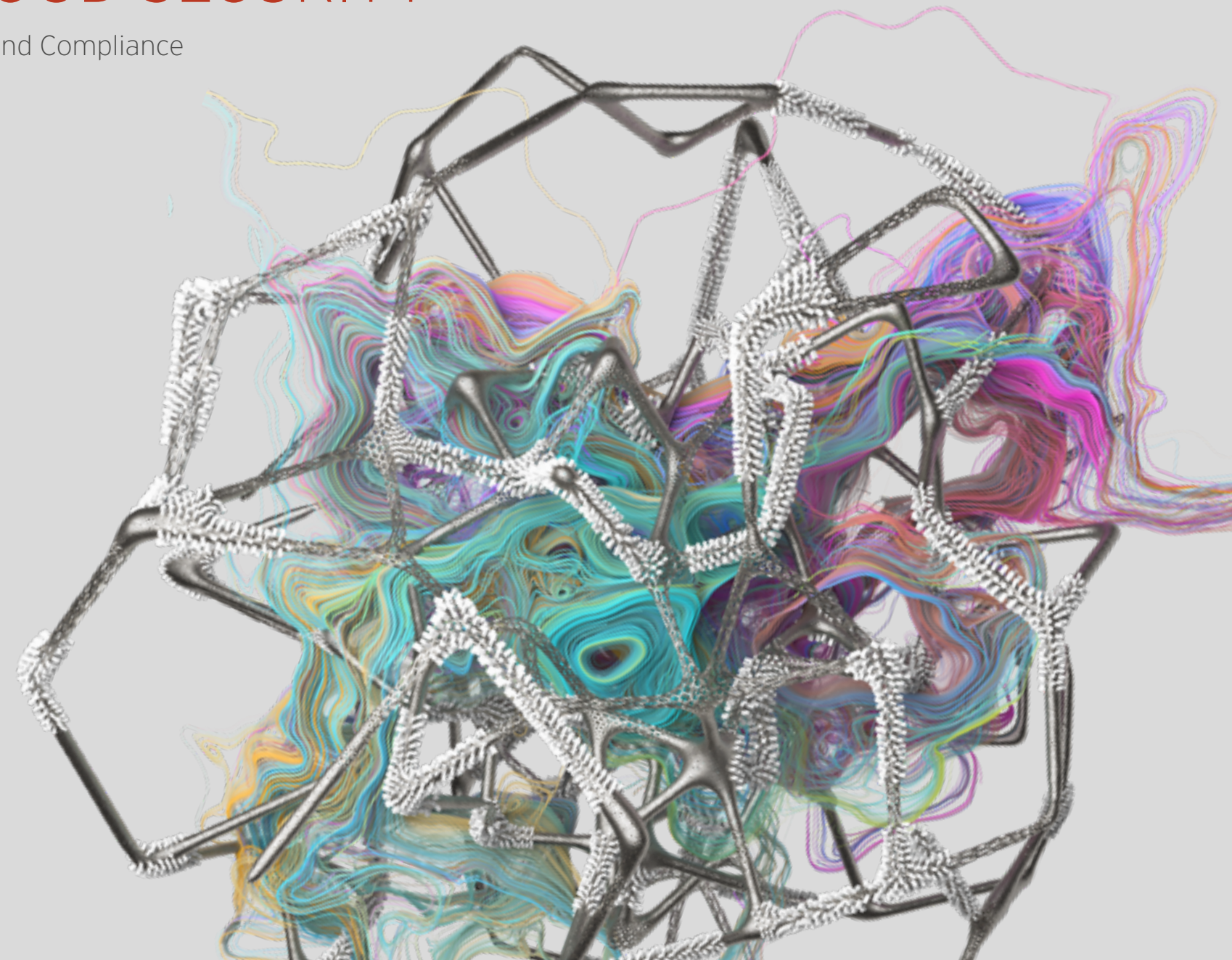
SALES PLAYBOOK: HYBRID CLOUD SECURITY

Cloud, Container, DevOps und Compliance



INHALT

SECURITY: VERÄNDERUNGEN BEI KÄUFERN UND BEEINFLUSSERN Ein Problem mit zwei Boxen

LINKE BOX – SICHERHEIT

Wer bin ich?

- InfoSec
- Cloud-Sicherheit
- IT-Sicherheit
- App-Sicherheit

Meine Mission: Risikomanagement und Schutz des Unternehmens

- Verantwortlich für Sicherheit und Compliance
- Definiert Sicherheitsrichtlinien
- Geringe Interaktion mit anderen Geschäftseinheiten (BUs)
- Verwaltet das Sicherheitsbudget
- Managt die Sicherheitswerkzeuge

RECHTE BOX

Wer bin ich?

- Cloud-Architekt
- Cloud Ops
- Cloud Engineer
- IT Operations
- Entwickler
- Middleware Engineer
- System Engineer
- Platform Engineer
- Automation Engineer
- DevOps Engineer
- CI/CD Engineer

Meine Mission: Schnelle Entwicklung und Bereitstellung von Applikationen

- Ansprechpartner für Geschäftseinheiten, Reporting an Geschäftseinheiten.
- Verantwortlich für Automation und Bereitstellung in konstanter Geschwindigkeit.
  - Infrastructure-as-Code / Schreibt Code für die IT-Automation.
- Implementiert Sicherheitsrichtlinien.
- Verwaltet das IT/Cloud-Budget (größer).
- Managt alle Werkzeuge inklusive Sicherheit.
- Beziehungen zu traditionellen Sicherheitsteams können von Herausforderungen gekennzeichnet sein.
- Verfügt über Cloud- und oftmals auch DevOps-Know-how.
- Anerkannte technische Expertise und Führungsposition.

VERTRIEBSHINWEISE

Aus Verschiebungen bei Kaufentscheidern / Beeinflussern entsteht das Zwei-Boxen-Problem:

- Traditionell befinden sich die für uns relevanten Entscheider / Beeinflusser in den InfoSec- und Sicherheitsteams, wobei unter Umständen neue Titel bzw. Aufgabenbeschreibungen verwendet werden, wie zum Beispiel Cloud-Sicherheit oder App-Sicherheit. Diese Personen sind auf Sicherheit und Compliance fokussiert und verwalten das Sicherheitsbudget. Ihre Mission ist das Management von Risiken und der Schutz des Unternehmens.
- DevOps ist ein Prozess bzw. eine Kultur, die Personen mit ganz unterschiedlichen Titeln und Aufgabenbereichen umfasst, wie zum Beispiel Cloud Ops, IT Operations, Cloud-Architektur. Manchmal findet sich der Begriff DevOps sogar im Titel des Ansprechpartners. Diese Personen fokussieren sich stark auf Automation und Monitoring aller Schritte in der Software CI/CD-Pipeline (Continous Integration and Continous Delivery). Hinsichtlich Implementierung und Entwicklung interagieren sie mit den Geschäftseinheiten und verwalten außerdem die IT- und Cloud-Gesamtbudgets, die wesentlich größer sind als das Sicherheitsbudget. Ihre Mission ist die bestmögliche Unterstützung des Unternehmens durch schnelle Entwicklung und Bereitstellung von Applikationen.
- Wir benötigen Vertriebsbotschaften, die Kaufentscheider / Beeinflusser in beiden Boxen ansprechen.

DIE RECHTE BOX KENNENLERNEN

Job:
- Entwicklung und Bereitstellung von Applikationen und Updates sowie Funktionen für neue Anwendungsergebnisse.
- Schnellstmögliche Produktivsetzung durch wiederholbare und automatisierte Aufgaben.
- Typischerweise innerhalb einer einzelnen Geschäftseinheit angesiedelt.

Wünsche:
- In einer anderen oder stärker spezialisierten Position arbeiten (33 Prozent).
- Ein eigenes Unternehmen gründen bzw. mitgründen (25,7 Prozent).

Herausforderungen / Pain Points:
- Wachsende Sicherheits- und Compliance-Anforderungen an Unternehmen (Governance, Regulierungen) erfüllen.
- Sicherheit ist schwer zu implementieren und zu automatisieren, sodass es zu einer Verlangsamung der Abläufe kommt.
- CI/CD- und DevOps-Werkzeugsets lassen sich aufgrund des Sicherheitsaufwand nur schwer verschlanken.
- Fehlende Sichtbarkeit und Automation über mehrere Umgebungen hinweg (zum Beispiel Rechenzentrum, AWS®, Microsoft® Azure® und Container).
- Unter Umständen geringes Verständnis des Modells der geteilten Verantwortung für Cloud-Sicherheit oder sogar der grundsätzlichen Notwendigkeit von Sicherheit.

Bedürfnisse:
- Integration mit automatisierten Prozessen (reduzierte Reibung).
- Application Programming Interfaces (APIs), mit denen sich Aufgaben automatisieren lassen.
- Integration mit unterschiedlichen Umgebungen (zum Beispiel AWS, Azure, VMware® und Docker®).
- Integration mit unterschiedlichen Plattformen (Betriebssystemen).
- Bevorzugt funktionierende Demos statt Powerpoint-Präsentationen.
- Wünscht sich direkte Antworten auf Fragen.
- Erwartet individuelles Eingehen auf Problemstellungen statt Standard-Präsentationen.

Wichtige Entscheidungskriterien:
- Überzeugung, dass ein Werkzeug einfach in die bestehende Umgebung integriert werden kann und keine zusätzliche Reibung verursacht.
- Vertrauen auf den Entwickler-Support, inklusive Unterstützung von Automation / Scripting in der Umgebung, Interoperabilität der Werkzeuge und Beispiel-Code.
- Andere Produkte wurden getestet und konnten die Anforderungen nicht erfüllen.

Verbreitete Jobbezeichnungen:
DevOps, DevSecOps, Cloud Architect, Cloud Ops, Cloud Engineer, IT Operations, Developer, Middleware Engineer, System Engineer, Platform Engineer, Automation Engineer, DevOps Engineer, CI/CD Engineer

Position in der Organisation:
Geschäftseinheit, Reporting an CIO oder CEO

Rolle für Kaufentscheidungen:
Anwender, Beeinflusser

Unternehmensgröße:
Mittlere bis große oder sehr große Unternehmen

Alter:
Überwiegend zwischen 25 und 39 Jahren (49 Prozent)

Geschlecht:
Überwiegend männlich (mehr als 90 Prozent)

DIE RECHTE BOX KENNENLERNEN

Fortsetzung

Weiwale:

- Bevorzugt Interaktion mit Kollegen aus der Praxis; skeptisch gegenüber Informationen von dritter Seite.
- Kompetenter Käufer, recherchiert eigenständig und bereitet sich vor.
- Möglicherweise geringes Verständnis der Marke und des Wertes von Trend Micro.

Interaktion und Anknüpfungspunkte:

- GitHub®
- Kostenfreie Demos
- Stack Overflow
- Google (intensive Google-Nutzer)
- Twitch
- Blogs, Reddit
- Meetup-Gruppen und Hackathons
- Videos (kurzgefasste Inhalte)
- Gleichrangige Kollegenbeziehungen (hinsichtlich Anbieterauswahl oder Lösungsevaluierung)
- Events (re:invent, Automationskonferenzen, Puppet®)

Häufig verwendete Begriffe:

- Automation
- CI/CD-Pipeline
- Tool Stack / Chain
- Cloud und Cloud-Bereitstellung
- Integration
- Elastizität
- Immutable Infrastructure
- Microservices
- Container
- Serverless

Anmerkungen:

- Verbringt täglich im Durchschnitt 9 bis 12 Stunden am Computer, Verbundenheit mit anderen Entwicklern / Cloud-Verantwortlichen.
- Genießt soziale Zusammenkünfte mit alkoholischen Getränken.
- Favorisiert ein lässig-cooles Auftreten und hat Spaß an Stickern, T-Shirts etc.
- Nutzt Code und Anwendungsergebnisse, um innerhalb des kollegialen Umfeldes Anerkennung und Respekt zu erhalten (wichtiger als Anerkennung durch Management).

ABLAUF IN DER FINDUNGSPHASE

Anwendungsfälle für die rechte Box

Stellen Sie diese Schlüsselfragen (Key Questions, KQ), um den Anwendungsfall zu identifizieren.

COMPLIANCE

- **Key Question Eins (KQ1):**

  Muss Ihre Umgebung Compliance- oder Governance-Anforderungen erfüllen?

CLOUD MIGRATION

- **Key Question Zwei (KQ2):**

  Werden in Ihrer Organisation aktuell Cloud-Projekte geplant oder durchgeführt?

AUTOMATION

- **Key Question Drei (KQ3):**

  Verwenden Sie bzw. Ihre internen Kunden CI/CD oder eine Art automatisierter Bereitstellung?

CONTAINERS

- **Key Question Vier (KQ4):**

  Führen Sie bzw. Ihre internen Kunden aktuell Container-Projekte durch oder planen diese?

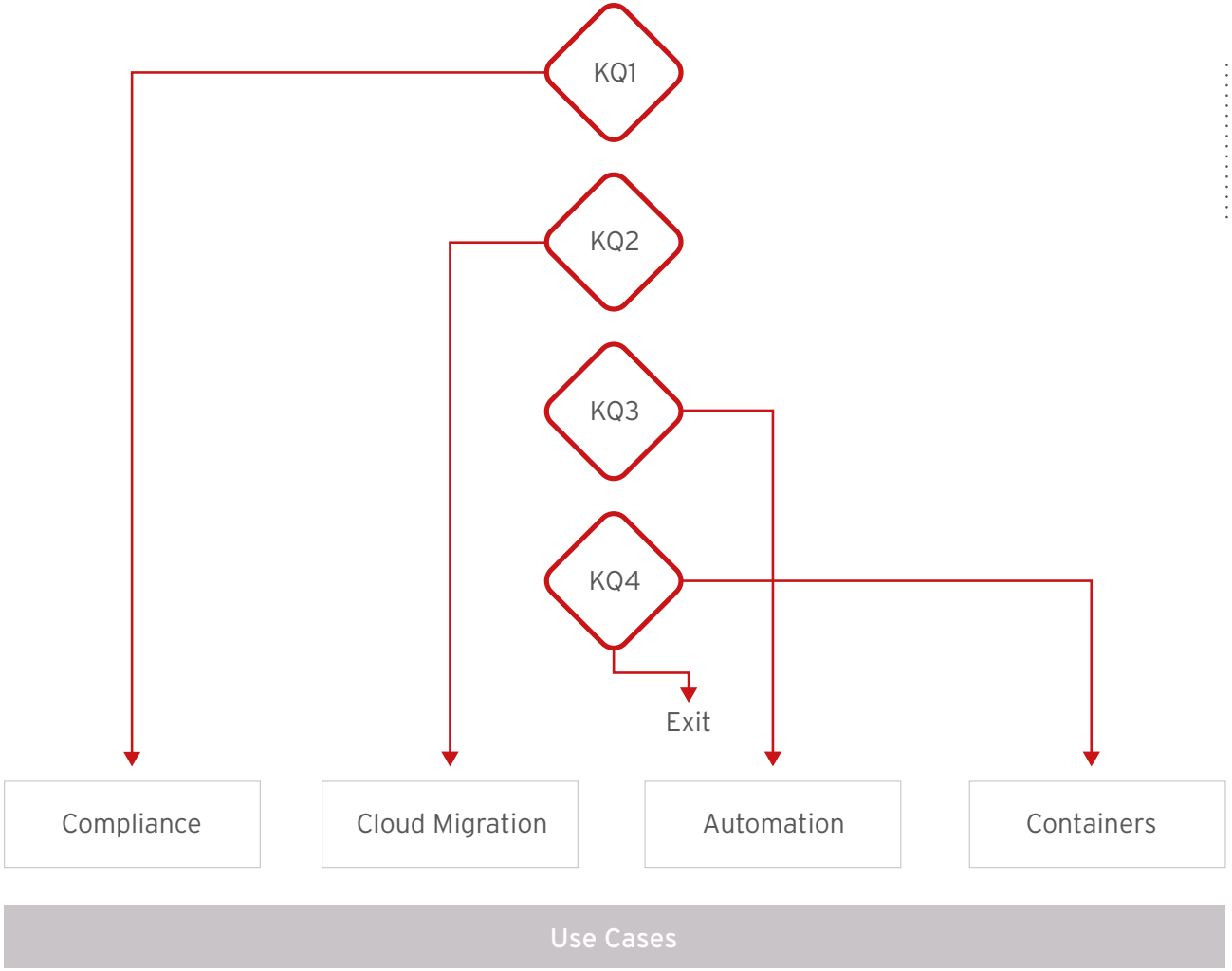
- **Achten Sie darauf, dass Sie Antworten auf ALLE VIER Fragen erhalten!**

VERTRIEBSHINWEISE

- Es wird von den folgenden Prämissen ausgegangen:
  1. Mit Neukunden wurde bereits eine Sicherheitsdiskussion geführt. Die Fragen folgen typischerweise auf aktuelle Gespräche im Vertriebsprozess.
  2. Die Fragen können für die Weiterführung des Gesprächs verwendet werden oder auch als Diskussionsanstöße bei Bestandskunden dienen.
- Je nach Kundenumgebung können auch mehrere Themen zutreffen, daher sollten alle vier Fragen beantwortet werden. Für jedes „Ja“ finden Sie im Anschluss detaillierte Anwendungsszenarien für eine tiefergehende Diskussion.
- Werden alle Fragen mit „Nein“ beantwortet, haben Sie zwei Optionen:
  1. Führen Sie weitere Recherchen durch, um festzustellen, ob Ihr Ansprechpartner vielleicht noch nicht über das erforderliche Problembewusstsein verfügt.
     - Verwenden Sie zum Beispiel XING, disovery.org oder LinkedIn, um nach den bereits aufgeführten, häufigen Titeln und Aufgabenbereichen relevanter Ansprechpartner im Unternehmen zu suchen.
  2. Exit
- Aufgabenstellungen zur Compliance gehören nicht in jedem Fall in die rechte Box. Da Compliance aber von allen befragten Unternehmen als Anforderung genannt wurde, muss sie Teil des Ablaufdiagramms sein. Nachdem die anderen Fragen gestellt wurden, können Anschlussfragen zur Compliance weitere Möglichkeiten eröffnen.

ABLAUF IN DER FINDUNGSPHASE

Anwendungsfälle für die rechte Box



- **Stellen Sie sicher, dass jeder Pfad bis zum Ende verfolgt wird, auch wenn der Kunde bereits eine Frage mit „Ja“ beantwortet hat.**

VIER ANWENDUNGSFÄLLE FÜR DIE RECHTE BOX

Compliance

Cloud-Migration

DevOps und Automation

Container-Sicherheit

COMPLIANCE: TERMINOLOGIE

DSGVO	Die Datenschutz-Grundverordnung (DSGVO) stellt umfangreiche organisatorische und technische Anforderungen an alle Unternehmen, die persönliche Daten von EU-Bürgern sammeln, verarbeiten und speichern – auch wenn damit keine kommerzielle Transaktion verbunden ist. Weitergehende rechtliche Informationen zur DSGVO finden Sie hier.
PCI DSS	Der Payment Card Industry Data Security Standard (PCI DSS) gilt für Unternehmen jeder Größe, die Kreditkartenzahlungen akzeptieren. Voraussetzung für die Speicherung, Verarbeitung und Übertragung der Daten von Kreditkarteninhabern ist die Compliance mit den Datenschutzanforderungen, die durch PCI DSS gestellt werden.
HIPAA	Der US-amerikanische Health Insurance Portability and Accountability Act (HIPAA) definiert die Standards für den Schutz von Patientenakten und anderen Gesundheitsinformationen, die Krankenkassen, Ärzten, Krankenhäusern und anderen Einrichtungen des Gesundheitswesens zur Verfügung gestellt werden.
NIST 800-53	Mit der Publikation 800-53 empfiehlt das National Institute of Standards and Technology (NIST) Sicherheitskontrollen für Systeme und Dokumente in allen US-amerikanischen Bundesbehörden (ausgenommen nationale Sicherheit). Das Cybersecurity Framework (CSF) des NIST wird von Regierungen und Unternehmen weltweit als Richtlinie für Organisationen jeder Branche und Größe unterstützt.
ISO	Die International Organization for Standardization (ISO) ist ein Verband nationaler Normierungsorganisationen. Der ISO 27001 Standard stellt einen 6-stufigen Prozess für die Implementierung von Richtlinien und Abläufen zur Informationssicherheit bereit.
IT-Sicherheitsgesetz	Das IT-Sicherheitsgesetz (IT-SiG) soll die Sicherheit informationstechnischer Systeme erhöhen und zum Schutz von kritischen Infrastrukturen (KRITIS) in allen Bereichen beitragen, die für das öffentliche Leben in Deutschland essentiell sind. Dazu gehören Energie- und Wasserversorgung, Verkehr, Telekommunikation und weitere mehr. Das IT-SiG verpflichtet Betreiber zur Einhaltung eines definierten Mindestmaßes an IT-Sicherheit und zum Nachweis geeigneter technischer und organisatorischer Maßnahmen.
NIS	Bei der Richtlinie zur Gewährleistung der Netzwerk- und Informationssicherheit (NIS) handelt es sich im Wesentlichen um ein europäisches Pendant zum deutschen IT-Sicherheitsgesetz.

Was ist Compliance?

- Compliance bedeutet die angestrebte oder bereits hergestellte Übereinstimmung mit etablierten Richtlinien, branchenspezifischen Regelungen oder gesetzlichen Regelwerken. Der Compliance-Status von Unternehmen ist für CISOs und Sicherheitsverantwortliche von entscheidender Bedeutung.

COMPLIANCE: RECHTE BOX

SCHLÜSSELFRAGEN:

- Muss die Einhaltung interner Richtlinien für Server- und Cloud-Workloads sichergestellt werden?
- Welche gesetzlichen Regelungen müssen beachtet werden?
- Wie werden die Compliance-Anforderungen bislang erfüllt?

POSITIONIERUNG:

- Trend Micro™ Deep Security™ bietet Sicherheit für alle Entwicklungs- und Betriebsprozesse durch Container Image Scanning zur Build-Time und Workload-Schutz zur Laufzeit auf dem Host sowie für Kubernetes® und Docker Plattformen.
- Deep Security stellt RESTful APIs bereit, die eine kontinuierliche Überwachung und die Integration der Sicherheit mit der DevOps Toolchain ermöglichen, zum Beispiel mit Pipeline-Management- und Bereitstellungswerkzeugen wie GitHub, Jenkins®, Chef, Puppet, Ansible, AWS OpsWorks, SaltStack®, Kubernetes und Microsoft® PowerShell®.

STICHWORTE IM GESPRÄCH:

- Gesteigerte Anforderungen an Sicherheit und Compliance verursachen ungeplanten Mehraufwand.
- Sicherheit darf sich nicht negativ auf die Geschwindigkeit auswirken.

VORTEILE:

- Die Integration der Sicherheit als Code mittels APIs und Skripts reduziert die Anzahl benötigter Builds. Darüber hinaus bietet Deep Security konsistenten Schutz für die CI/CD-Pipeline und stellt damit Sicherheits- und Compliance-Teams zufrieden.

VERTRIEBSHINWEISE

- Sobald Sie ein Verständnis für die DevOps- und Automationsstrategie des Kunden gewonnen haben, sollten Sie sicherstellen, dass an allen weiterführenden Diskussionen zumindest ein Entwickler oder Engineer (oder ähnliche Positionen) beteiligt ist. Falls in den bisherigen Gesprächen bereits Container-Werkzeuge erwähnt wurden, kann außerdem die Einladung von Container-Architekten ratsam sein.
- Diese zusätzlichen Fragen ermöglichen Ihnen ein besseres Verständnis der internen Arbeitsabläufe / Aufgaben beim Kunden.
- Diese Fragen richten sich an Personen der rechten Box.

COMPLIANCE: LINKE BOX

SCHLÜSSELFRAGEN:

- Wie hoch ist der Regulierungsgrad Ihrer Branche?
- Mit welchen branchenspezifischen und gesetzlichen Regularien muss Compliance hergestellt werden?
- Wie groß war der benötigte Aufwand für die Compliance mit der DSGVO und die Vermeidung der Strafen in Höhe von bis zu vier Prozent des globalen Umsatzes?

POSITIONIERUNG:

- Deep Security beschleunigt die Compliance in heterogenen Umgebungen mit physischen, virtuellen und Cloud-Workloads auf unterschiedlichen Plattformen, darunter Microsoft® Windows® und viele Linux-Versionen. Darüber hinaus kann auch bei Computing-Architekturen wie Containern mit Deep Security schneller Compliance hergestellt werden. Das Reporting erstreckt sich über alle Umgebungen hinweg.
- Deep Security umfasst Firewalls, Antivirus, Schwachstellen- und Patch-Management, Kontrolle von Software-Änderungen, Log-Inspektion, Intrusion Detection / Intrusion Prevention Systeme (IDS/IPS) und File Integrity Monitoring (FIM).
- Deep Security unterstützt Organisationen bei der Erfüllung von Compliance-Anforderungen durch Regularien wie DSGVO, IT-SiG, NIS, PCI DSS, HIPAA, ISO und NIST 800-53.
- Deep Security as a Service ist ein Level One Service Provider gemäß PCI DSS.
- Deep Security ist validiert nach Common Criteria Evaluation Assurance Level 2 (EAL2) und Federal Information Processing Standard (FIPS) 140-2.

STICHWORTE IM GESPRÄCH:

- Besorgnis hinsichtlich DSGVO, IT-SiG, NIS, PCI DSS, HIPAA, ISO, NIST 800-53 und anderen Regularien oder Richtlinien.
- Unternehmensführung erhöht den Druck beim Thema Compliance.
- Besorgnis hinsichtlich der Strafen für fehlende Compliance.
- Besorgnis, wie und ob Compliance in neuen Umgebungen hergestellt werden kann. So zum Beispiel in der Cloud, in der es keinen traditionellen, kontrollierbaren Perimeter mehr gibt.
- Bevorstehende Audits oder Auditor Reports, in denen Bereiche identifiziert werden, die nicht Compliance-konform sind oder Verbesserungen erfordern.
- Hoher Zeit- und Arbeitsaufwand für Audits.
- Anforderungen an Firewalls, Antivirus, Schwachstellen- und Patch-Management, Kontrolle von Software-Änderungen, Log-Inspektion, Intrusion Detection / Intrusion Prevention Systeme (IDS/IPS) und File Integrity Monitoring (FIM).

VORTEILE:

- Detaillierte, Audit-fähige Reports dokumentieren geschützte Schwachstellen, erkannte Angriffe und den Compliance-Status der Sicherheitsrichtlinien.
- Automatisiertes Compliance-Reporting über die gesamte Hybrid Cloud hinweg.
- Vorbereitung auf Audits erfordert weniger Zeit und Aufwand durch zentralisierte Sicherheitskontrollen und konsolidiertes Reporting.
- Unterstützung für interne Compliance-Initiativen zur Steigerung der Sichtbarkeit interner Netzwerkaktivitäten.
- Unterstützung bei der Compliance mit DSGVO, IT-SiG, NIS, PCI DSS, HIPAA, ISO, NIST 800-53 und anderen Regularien oder Richtlinien.

VERTRIEBSHINWEISE

- Verwenden Sie diese Informationen, um herauszufinden, ob Compliance-Anforderungen für Ihren Gesprächspartner / das Unternehmen relevante Themen sind.
- Die Schlüsselfragen helfen Ihnen dabei, die Compliance-Anforderungen des Unternehmens besser zu verstehen.
- Die Fragen richten sich in erster Linie an Personen der linken Box, können aber auch Informationen über möglicherweise relevante Personen der rechten Box liefern.
- Nachdem Sie den Interessenten mithilfe der Fragen näher kennengelernt haben, können die Gespräche telefonisch oder persönlich weitergeführt werden. Dabei sollten dann relevante Personen der rechten Box anwesend sein und die entsprechenden Rechte-Box-Fragen zur Vertiefung verwendet werden.

COMPLIANCE: ASSETS UND ANWENDERGESCHICHTEN

ASSETS (STUFE 1 BIS 5)

- **Stufe 1 bis 3 (Prospektierung)**
  - **Gartner CWPP Market Guide**
    www.trendmicro.com/de_de/business/products/hybrid-cloud.html?modal=6dba25
  - **Trend Micro Compliance-Webseite**
    https://www.trendmicro.com/de_de/business/capabilities/solutions-for/compliance.html
- **Stufe 4 (Relevanz bestätigt)**
  - **Hybrid Cloud Security Explainer-Video (englisch)**
    https://www.youtube.com/watch?v=ZBYIr83n1OY
  - **Hybrid Cloud Security Kundenpräsentation (englisch)**
    https://community-trendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0690B0000042CyrQAE
  - **Deep Security Compliance-Webseite (englisch)**
    https://help.deepsecurity.trendmicro.com/compliance.html
  - **AWS PCI Compliance mit Deep Security (englisch)**
    https://www.trendmicro.com/aws/acceleratingpci/
- **Stufe 5 (Einschätzung der technischen Lösung)**
  - **Proof-of-Concepts, Demos – siehe Anhang**
  - **AWS NIST Quick Start**
    https://aws.amazon.com/quickstart/architecture/compliance-nist-high-impact/

ANWENDERGESCHICHTEN (STUFE 6+)

- **Essilor (englisch)**
  https://www.trendmicro.com/en_us/about/customer-stories/essilor.html
- **Carhartt (englisch)**
  https://www.trendmicro.com/en_us/about/customer-stories/carhartt.html
- **Orion Health (englisch)**
  https://www.trendmicro.com/en_us/about/customer-stories/orion-health.html
- **McGill University Health (englisch)**
  https://www.trendmicro.com/en_us/about/customer-stories/mcgill-university-health-centre.html
- **MEDHOST (englisch)**
  https://www.trendmicro.com/en_us/about/customer-stories/medhost-aws.html

CLOUD-MIGRATION: TERMINOLOGIE

AWS	Amazon Web Services (AWS) ist eine sichere Cloud-Services-Plattform und bietet Rechenkapazität, Datenbank-Speicherung, Content-Verteilung und weitere Funktionalitäten, die Unternehmen Skalierbarkeit und Wachstum ermöglichen.
Azure	Microsoft Azure (ehemals Windows Azure) ist ein Cloud-Computing-Service für Entwicklung, Test, Bereitstellung und Management von Applikationen und Services über Rechenzentren, die von Microsoft verwaltet werden.
Google Cloud	Google Cloud ist eine Suite von Cloud-Computing-Services die auf derselben Infrastruktur basieren, die auch von Google intern für seine Endanwenderprodukte genutzt wird, wie zum Beispiel Google™ Search und YouTube™.
Oracle Cloud	Oracle® Cloud ist ein von der Oracle® Corporation bereitgestellter Cloud-Computing-Service und bietet Server, Speicher, Netzwerke, Applikationen und Services über ein globales Netzwerk von Rechenzentren, die von der Oracle Corporation verwaltet werden.
VPC	Eine Virtual Private Cloud (VPC) ist ein konfigurierbarer On-Demand-Pool geteilter Computing-Ressourcen innerhalb einer Public-Cloud-Umgebung. Dies gewährleistet einen gewissen Grad der Abgrenzung zwischen verschiedenen Organisationen, die auf die Ressourcen zugreifen.
Resource Group	Eine Resource Group umfasst verbundene Ressourcen für eine Azure Lösung. Innerhalb von Azure werden verbundene Ressourcen logisch gruppiert, wie zum Beispiel Speicher-Accounts, virtuelle Netzwerke und virtuelle Maschinen (VMs), um Bereitstellung, Management und Wartung als eine einzige Einheit zu ermöglichen.
AMI	Ein Amazon Machine Image (AMI) ist eine spezielle Art von virtueller Appliance und wird für die Erstellung von VMs in der Amazon Elastic Compute Cloud® (AMAZON EC2) verwendet.
Azure VM	Eine Azure VM ist eine skalierbare On-Demand-Computing-Ressource, die auf Azure bereitgestellt wird.
Auto-Scaling	Eine im Cloud-Computing verwendete Methode, bei der die Rechenkapazitäten einer Server-Farm (in der Regel gemessen an der Anzahl aktiver Server) automatisch gemäß der Belastung der Farm skaliert werden.
AWS Security Group	AWS Security Groups (SGs) sind EC2-Instanzen zugeordnet und bieten Sicherheit auf der Protokoll- und Port-Zugriffsebene.
Azure Network Security Group	Über Network Security Groups kann der Datenverkehr zu und von Azure Ressourcen in einem virtuellen Azure Netzwerk gefiltert werden. Eine Network Security Group umfasst Sicherheitsregeln, die ein- und ausgehenden Netzwerkdatenverkehr für verschiedene Arten von Azure Ressourcen erlauben oder blockieren.

Was ist Cloud-Migration?

- **Cloud-Migration** ist der Prozess der Verlagerung von Daten, Applikationen und anderen Business-Elementen in eine **Cloud**-Computing-Umgebung, wie zum Beispiel AWS, Azure oder Google Cloud™. Unternehmen können eine Cloud-Migration auf unterschiedliche Arten vollziehen. Ein verbreitetes Modell ist der Transfer von Daten und Applikationen von einem lokalen On-Premise-Rechenzentrum in die Public **Cloud**.

CLOUD-MIGRATION: RECHTE BOX

SCHLÜSSELFRAGEN:

- Was wollen sie durch eine Migration in die Cloud erreichen? Kosteneinsparungen, verbesserte Agilität, Rechenzentrum muss erneuert werden?
- Sind sie mit dem Modell der geteilten Verantwortung für Cloud-Sicherheit vertraut?
- Nutzen aktuell bereits Teams oder BUs die Cloud für den Betrieb von Applikationen oder die Datenspeicherung?
- Was planen sie, in die Cloud zu verlagern? Daten oder Applikationen?
- Ist Automation wichtig?

POSITIONIERUNG:

- Deep Security unterstützt bei der Umsetzung der geteilten Sicherheitsverantwortung in der Public Cloud. Herkömmliche Sicherheitsprodukte für Rechenzentren helfen hier nicht weiter (z.B. fehlende Unterstützung für Linux Kernel und Auto-Scaling).
- Deep Security gewährleistet Sichtbarkeit sowie die automatische Erkennung und Durchsetzung von Sicherheitsregeln für Cloud-Instanzen. Dies unterstützt bei der Compliance.
- Trend Micro Sicherheit erstreckt sich auch auf Modernisierungen mit Containern in der Cloud.
- Mit API-first und Security-as-Code-Werkzeugen können große Mengen von Daten und Applikationen einfach und automatisiert in die Cloud migriert werden. Außerdem sind konsistente Sicherheitsregeln gewährleistet.
- Unterstützung bei der Compliance.
- Deep Security as a Service ist ein Level One Service Provider gemäß PCI DSS.
- Deep Security ist validiert nach Common Criteria Evaluation Assurance Level 2 (EAL2) und Federal Information Processing Standard (FIPS) 140-2.

STICHWORTE IM GESPRÄCH:

- Kosteneinsparungen, beschleunigte Bereitstellung, verbrauchsbasierte Abrechnung
- Fehlendes Bewusstsein für die geteilte Sicherheitsverantwortung
- Geringes Vertrauen in das Sicherheitsprofil der Public Cloud
- Teams verwenden bereits die Cloud; Besorgnis wegen Schatten-IT ohne Sichtbarkeit und Kontrolle.
- „Lift and Shift" für Applikationen oder neue Cloud-Initiativen, bei denen Sicherheit essentiell ist.
- Automation ist wichtig.
- Transformation von Applikationen, modernisierte App-Architektur und Container-Bereitstellung
- Stark regulierte Branche (Finanzen, Handel, Gesundheitswesen, Behörden)

VORTEILE:

- Automation ermöglicht reibungslose Sicherheit in verschiedenen und sich permanent verändernden Umgebungen.
- Geteilte Sicherheitsverantwortung in der Cloud erfüllen.
- Konzipiert für AWS, Azure und Google Cloud, vollständige Integration
- Sichtbarkeit für die gesamte Hybrid Cloud über ein einziges Werkzeug
- Konsistente Sicherheitsregeln, Verwaltung und Compliance über die gesamte Hybrid Cloud hinweg

VERTRIEBSHINWEISE

- Sobald Sie die Cloud-Strategie des Kunden verstanden haben, sollte das nächste Gespräch den Cloud-Architekten (oder ähnliche Rolle) einbeziehen. Wurden im Gespräch bereits Entwicklerwerkzeuge erwähnt, kann auch die Einladung von Entwicklern bzw. Engineers ratsam sein.
- Diese zusätzlichen Fragen sollen Ihnen ein besseres Verständnis der internen Arbeitsprozesse ermöglichen.
- Die Fragen richten sich in erster Linie an Personen der rechten Box.

CLOUD-MIGRATION: LINKE BOX

SCHLÜSSELFRAGEN:

- Wie sieht ihre Cloud-Strategie für die nächsten 12 Monate bzw. zwei Jahre aus? Ist ihr Ziel die komplette Verlagerung in die Cloud? Wer ist verantwortlich für Cloud-Projekte?
- Welche Public Cloud Provider ziehen sie in Erwägung?
- Welche Plattformen verwenden sie, z.B. Windows, Linux oder Container?
- Welche Werkzeuge setzen sie derzeit ein (Orchestrierung, Automation)?
- Müssen Sie interne oder externe Compliance-Anforderungen erfüllen?

POSITIONIERUNG:

- Deep Security ermöglicht konsistente Sicherheit für physische, virtuelle und Cloud-Workloads und schützt Windows, viele Linux Builds sowie Computing-Architekturen wie Container.
- Deep Security schützt Workloads unabhängig davon, in welcher Public Cloud sie ausgeführt werden.
- Herkömmliche Sicherheitsprodukte für Rechenzentren helfen nicht weiter (z.B. fehlende Unterstützung für Linux Kernel und Auto-scale).
- Deep Security unterstützt Organisationen bei der Erfüllung von Compliance-Anforderungen durch Regularien wie DSGVO, IT-SiG, NIS, PCI DSS, HIPAA, ISO und NIST 800-53.
- Mit API-first und Security-as-Code-Werkzeugen können große Mengen von Daten und Applikationen einfach und automatisiert in die Cloud migriert werden. Außerdem sind konsistente Sicherheitsregeln gewährleistet.
- AWS Quick Start ermöglicht schnelle und einfache Einrichtung der Cloud-Umgebung, NIST-konformer Quick Start verfügbar.
- Deep Security umfasst Firewalls, Antivirus, Schwachstellen- und Patch-Management, Kontrolle von Software-Änderungen, Log-Inspektion, Intrusion Detection / Intrusion Prevention Systeme (IDS/IPS) und File Integrity Monitoring (FIM).

STICHWORTE IM GESPRÄCH:

- Strategie für Hybrid Cloud oder komplette Cloud-Verlagerung?
- Geschäftsführung erhöht den Druck hinsichtlich Cloud- und Cloud-first-Strategien.
- Migration zu AWS, Azure, Google Cloud und Oracle Cloud
- Verwendung von Windows, Linux, Containern und Legacy-Plattformen
- Erwähnung von Werkzeugen für Orchestrierung, Analytics, Security Information and Event Management (SIEM), Jenkins, Github usw.
- Bedenken hinsichtlich der Compliance beim Übergang von On-Premise in die Cloud
- Aktive Formulierung der Cloud-Strategie oder Nachzügler?

VORTEILE:

- Automation ermöglicht reibungslose Sicherheit in verschiedenen und sich permanent verändernden Umgebungen.
- Sichtbarkeit für die gesamte Hybrid Cloud über ein einziges Werkzeug
- Konsistente Sicherheitsregeln, Verwaltung und Compliance über die gesamte Hybrid Cloud hinweg
- Unterstützung für interne Compliance-Initiativen verbessert Sichtbarkeit interner Netzwerkaktivitäten. Außerdem Unterstützung für Compliance mit DSGVO, IT-SiG, NIS, PCI DSS, HIPAA, ISO und NIST 800-53.
- Detaillierte, Audit-fähige Reports dokumentieren abgeschirmte Schwachstellen, erkannte Angriffe und den Compliance-Status der Sicherheitsregeln.
- Reduziert Zeit und Aufwand für die Vorbereitung auf Audits durch zentralisierte Sicherheitskontrollen und konsolidiertes Reporting.

VERTRIEBSHINWEISE

- Verwenden Sie diese Informationen, um herauszufinden, ob Cloud-Migra-tion für Ihren Gesprächspartner / das Unternehmen ein relevantes Thema ist.
- Die Schlüsselfragen helfen Ihnen dabei, besser zu verstehen, wie die Cloud-Strategie des Unternehmens aussieht, welche Cloud-Angebote verwendet werden, welche Plattformen geschützt werden müssen, ob Automation eingesetzt werden soll (DevOps Transition) und ob Compliance-Anforderungen zu erfüllen sind.
- Die Fragen richten sich in erster Linie an Personen der linken Box, können aber auch Informationen über möglicherweise relevante Personen der rechten Box liefern.
- Nachdem Sie den Interessenten mithilfe der Fragen näher kennengelernt haben, können die Gespräche telefonisch oder persönlich weitergeführt werden. Dabei sollten dann relevante Personen der rechten Box anwesend sein und die entsprechenden Rechte-Box-Fragen zur Vertiefung verwendet werden.

CLOUD-MIGRATION: EINWANDBEHANDLUNG

EINWAND:
Wir verwenden Cloud-native Werkzeuge zum Schutz unserer Umgebung, warum benötigen wir zusätzliche Sicherheit (z.B. „AWS Sicherheit ist doch gut genug“)?

REAKTION:
- Diskutieren Sie das Modell der geteilten Sicherheitsverantwortung in der Cloud.

EINWAND:
Wir setzen weder AWS noch Azure für unsere Cloud-Plattform ein.

REAKTION:
- Erläutern Sie die Integration mit AWS WAF, GuardDuty, SNS, CloudTrail und die Zusammenarbeit mit Azure Security Center.

EINWAND:
Wir sehen Trend Micro eher als traditionellen Sicherheitshersteller.

REAKTION:

- Deep Security kann in jeder Cloud auf allen unterstützen Betriebssystemen eingesetzt werden. Sie profitieren auf jeden Fall von leistungsstarker, mehrschichtiger und automatisierter Sicherheit.

EINWAND:
Ist Trend Micro ein relevanter bzw. strategischer Partner von AWS / Azure / Google?

REAKTION:
- **Geben Sie einen Überblick zu unserer großartigen AWS Story:** https://aws.amazon.com/partners/success/trend-micro/

EINWAND:
Wir haben bereits ein ELA mit Wettbewerber XYZ und werden die bestehende Lösung in die Cloud erweitern.

REAKTION:
- Kann ihnen der Wettbewerber vollständige Sichtbarkeit ihrer Cloud Accounts bieten? Wird automatische Provisionierung unterstützt, um Auto-Scaling zu ermöglichen? Ist der Wettbewerber ein strategischer Partner von AWS, Azure oder Google? Trend Micro ist bereits strategischer Partner von AWS und Azure. An der Erweiterung der Partnerschaft auf Google wird gearbeitet.

EINWAND:
Wir wünschen uns Sichtbarkeit der Cloud Posture.

REAKTION:
- Dies wird heute noch nicht von Trend Micro angeboten, aber wir sind immer daran interessiert, mehr über ihre Bedürfnisse zu erfahren.

VERTRIEBSHINWEISE

- Sobald Sie die Cloud-Strategie des Kunden verstanden haben, sollte das nächste Gespräch den Cloud-Architekten (oder ähnliche Rolle) einbeziehen. Wurden im Gespräch bereits Entwicklerwerkzeuge erwähnt, kann auch die Einladung von Entwicklern bzw. Engineers ratsam sein.
- Diese zusätzlichen Fragen sollen Ihnen ein besseres Verständnis der internen Arbeitsprozesse ermöglichen.
- Die Fragen richten sich in erster Linie an Personen der rechten Box.
- Nachdem Sie den Interessenten mithilfe der Fragen näher kennengelernt haben, können Sie die zusätzlichen Fragen für weitergehende Gespräche verwenden.

CLOUD-MIGRATION: ASSETS UND ANWENDERGESCHICHTEN

ASSETS (STUFE 1 BIS 5)

- **Stufe 1 bis 3 (Prospektierung)**
  - **Gartner CWPP Market Guide:** www.trendmicro.com/de_de/business/products/hybrid-cloud.html?modal=6dba25
  - **Hybrid Cloud Security Webseite:** https://www.trendmicro.com/de_de/business/products/hybrid-cloud/cloud-security.html
  - **AWS Microsite (englisch):** https://trendmicro.com/aws
  - **•Azure Microsite (englisch):** https://trendmicro.com/azure
  - **Trend Micro Compliance-Webseite:** https://www.trendmicro.com/de_de/business/capabilities/solutions-for/compliance.html
- **Stufe 4 (Relevanz bestätigt)**
  - **Hybrid Cloud Security Explainer-Video (englisch):** https://www.youtube.com/watch?v=ZBYIr83n1OY
  - **Hybrid Cloud Security Solution Brief (englisch):** https://community-trendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=069U0000002PsIvIAC
- **Stufe 5 (Einschätzung der technischen Lösung)**
  - **AWS Quick Start Deep Security:** https://aws.amazon.com/quickstart/architecture/deep-security/
  - **Video: Automatisierte Sicherheit in der Hybrid Cloud (englisch):** https://youtu.be/0x8qHN32MWA

ANWENDERGESCHICHTEN (STUFE 6+)

- **Healthdirect Australia (englisch):** https://www.trendmicro.com/de_de/about/customer-stories/healthdirect-australia.html
- **MEDHOST (englisch):** https://www.trendmicro.com/de_de/about/customer-stories/medhost.html
- **XentIT und NASA (englisch):** https://www.trendmicro.com/de_de/about/customer-stories/xentit.html
- **Essilor (englisch):** https://www.trendmicro.com/de_de/about/customer-stories/essilor.html

DEVOPS AND AUTOMATION: TERMINOLOGIE

CI/CD Pipeline	Continous Integration / Continous Delivery ist das Rückgrat moderner DevOps-Umgebungen und schließt die Kluft zwischen Entwicklungs- und Betriebsteams durch Automation der Entwicklung, Tests und Bereitstellung von Applikationen.
Agil	Agile Software-Entwicklung bezieht sich auf eine Gruppe von Methodiken für die Software-Entwicklung. Basis ist die iterative Entwicklung, bei der Anforderungen und Lösungen im Rahmen eines kooperativen Prozesses zwischen sich selbst organisierenden und cross-funktionalen Teams entstehen.
Git/Github	GitHub ist eine webbasierte Kollaborationsplattform mit Versionskontrolle für Software-Entwickler. Git ist eine generische Sprache die auch von Organisationen genutzt werden kann, die nicht GitHub verwenden.
Jenkins/Bamboo	Jenkins ist ein Open-Source-Software-Werkzeug für Continous Integration. Das Werkzeug ist in der Programmiersprache Java® geschrieben und ermöglicht Tests und Reporting isolierter Änderungen in einer größeren Code-Basis in Echtzeit. Bamboo® ist ein ähnliches Werkzeug wie Jenkins.
Chef	Chef ist eine Engine für die Infrastruktur-Automation in modernen Software-getriebenen Organisationen.
Puppet	Puppet ist ein Open-Source-Werkzeug für das Software-Konfigurationsmanagement.
Ansible	Ansible ist ein Open-Source-Werkzeug für Software-Provisionierung, Konfigurationsmanagement und Applikationsbereitstellung.
AWS OpsWorks	AWS OpsWorks ist ein Cloud-Computing-Service von AWS, der Infrastruktur-Bereitstellungen für Cloud-Administratoren verwaltet. Der Service automatisiert Bereitstellungen, Konfigurationen und Betriebsaufgaben für verteilte Applikationen.
Salt/SaltStack	Salt (manchmal auch SaltStack Plattform genannt) ist ein Werkzeug für Konfigurationsmanagement und Orchestrierung.
Powershell	PowerShell ist ein automatisiertes Task-Framework von Microsoft. Ein Kommandozeilen-Interface und eine Skriptsprache sind in das .NET-Framework integriert, das in andere Applikationen eingebettet werden kann. Dies ermöglicht Batch-Verarbeitung und die Generierung von Werkzeugen für das Systemmanagement.
Serverless / Server-los	Serverless Computing ist ein Cloud-Computing-Ausführungsmodell, in dem der Cloud Provider den Server betreibt und die dynamische Zuweisung von Maschinenressourcen verwaltet.
Lambda	AWS Lambda ist ein Serverless-Computing-Service, der die Ausführung von Code in Reaktion auf Events ermöglicht und der das Management der zugrundeliegenden Computing-Ressourcen übernimmt.
Azure Functions	Azure Functions ist eine Lösung für die einfache Ausführung kleiner Code-Teile oder „Functions" in der Cloud.
Container	Ein Container ist eine Software-Standardeinheit, in der Code inklusive aller Abhängigkeit paketiert wird, sodass die Applikation schnell und zuverlässig in verschiedenen Umgebungen ausgeführt werden kann.

Was ist DevOps?

- DevOps ist eine Kultur bzw. ein Verfahren für Software-Entwicklung und Engineering. Ziel ist eine effizientere Kommunikation zwischen Entwicklung (Produkt-verantwortliche, Entwickler, Q/A-Tester) und dem IT-Betrieb. Der Fokus des Verfahrens liegt auf der Automation aller Ebenen der Software-Entwicklung, bis hin zur Bereitstellung im Betrieb. DevOps soll kürzere Entwicklungs- und Bereitstellungszyklen ermöglichen, um Kunden- bzw. Unternehmensanforderungen schneller mit stabileren Software Releases zu erfüllen, gemäß der CI/CD Pipeline Methodik.

DEVOPS UND AUTOMATION: RECHTE BOX

SCHLÜSSELFRAGEN:

- Können sie Time-to-Market-Ziele nicht erreichen, weil Sicherheit nur schwer implementiert oder automatisiert werden?
- Sind ihre Sicherheitswerkzeuge für die Cloud und ihre Pipeline optimiert?
- Verwenden sie Container?
- Setzen sie auf Serverless Computing (z.B. Lambda oder Azure Functions)?

POSITIONIERUNG:

- Deep Security bietet RESTful APIs, die eine kontinuierliche Überwachung und integrierte Sicherheit für die DevOps Toolchain ermöglichen. So zum Beispiel für Pipeline-Management- und Bereitstellungswerkzeuge wie GitHub, Jenkins, Chef, Puppet, Ansible, AWS OpsWorks, SaltStack, Kubernetes und Powershell.
- Deep Security reduziert die Komplexität von Tests und Bereitstellung. Durch die Erkennung von Malware, Schwachstellen und vertraulichen Informationen zur Build-Zeit werden gleichzeitig auch die Kosten für die Problembehebung bei Applikationen reduziert.
- Ein einziger Sicherheitsagent mit breiter Unterstützung für Plattformen und führende Cloud Provider schützt Laufzeit-Applikationen.
- Das Deep Security Automation Center bietet Best Practices, Skript-Beispiele und Dokumentationen, die DevOps Teams bei der Automation manueller Prozesse helfen.

STICHWORTE IM GESPRPÄCH:

- Steigende Sicherheits- und Compliance-Anforderungen verursachen ungeplanten Mehraufwand.
- Sicherheit darf sich nicht negativ auf die Geschwindigkeit auswirken.
- Inkompatible Werkzeuge, die nicht für die Cloud oder das Bereitstellungsmodell optimiert sind.
- Microservice-Entwicklung für Applikationen
- Pipeline-Management- und Bereitstellungswerkzeuge wie GitHub, Jenkins, Chef, Puppet, Ansible, AWS OpsWorks, SaltStack, Kubernetes und Powershell.

VORTEILE:

- Die Integration der Sicherheit als Code mittels APIs und Skripts reduziert die Anzahl benötigter Builds. Darüber hinaus bietet Deep Security konsistenten Schutz für die CI/CD Pipeline und stellt damit Sicherheits- und Compliance-Teams zufrieden.
- Konzipiert für Integration mit DevOps Orchestrierung
- Konzipiert für kontinuierliches Monitoring. Ermöglicht Automation, wodurch die Mitarbeiterproduktivität gesteigert werden kann. Ein einziger Agent reduziert den Testaufwand und verkürzt die Time-to-Market.
- Deep Security wurde speziell für die Automation konzipiert und integriert sich in bestehende Toolchains.

VERTRIEBSHINWEISE

- Sobald Sie ein Verständnis für die DevOps- und Automationsstrategie des Kunden gewonnen haben, sollten Sie sicherstellen, dass an allen weiterführenden Diskussionen zumindest ein Entwickler oder Engineer (oder ähnliche Positionen) beteiligt ist. Falls in den bisherigen Gesprächen bereits Container-Werkzeuge erwähnt wurden, kann außerdem die Einladung von Container-Architekten ratsam sein.
- Diese zusätzlichen Fragen ermöglichen Ihnen ein besseres Verständnis der internen Arbeitsabläufe / Aufgaben beim Kunden.
- Diese Fragen richten sich an Personen der rechten Box.

DEVOPS UND AUTOMATION: LINKE BOX

SCHLÜSSELFRAGEN:

- Wie stellen sie heute neue Workloads bereit?
- Wissen sie, was ihre Teams tun, um die CI/CD Pipeline und Applikationen über Build- und Bereitstellungsumgebungen hinweg zu schützen?
- Wie sind sie in den Schutz dieser Workloads oder Umgebungen involviert? Haben sie ein DevOps Team?
- Wie verfahren sie mit Sicherheits- und Compliance-Anforderungen im Hinblick auf DevOps Teams und die CI/CD Pipeline?
- Scannen sie Code oder Applikationen auf Schwachstellen?

POSITIONIERUNG:

- Deep Security bietet Sicherheit für alle Entwicklungs- und Betriebsprozesse durch Container Image Scanning zur Build-Zeit und Workload-Schutz zur Laufzeit auf dem Host sowie für Kubernetes® und Docker Plattformen.
- Deep Security stellte umfangreiche RESTful APIs bereit, mit denen Sicherheit gewährleistet werden kann, ohne die Bereitstellung zu verlangsamen.

STICHWORTE IM GESPRÄCH:

- Automatisierte Workflows oder automatisierte Prozesse
- Unsicherheit hinsichtlich der Sicherheitsaktivitäten von Teams
- Vorgeschriebene Sicherheit für die Organisation
- Docker, Kubernetes, ECS oder Amazon Elastic Container Service for Kubernetes (EKS), Google Cloud Kubernetes Service (GKS) oder Microsoft Azure Container Services (ACS)
- Microservice-Architektur, häufig in Verbindung mit Containern
- Automation, DevOps, CI/CD Pipeline, agile Entwicklung
- Unsicherheit hinsichtlich Container-Sicherheit oder Verwendung eines Mitbewerbers (Twistlock®, Aqua Security™)
- Werkzeuge für Code Scanning und die Suche nach Schwachstellen in Applikationen, wie zum Beispiel Coverity®, Fortify oder Signal Sciences

VORTEILE:

- Optimiert für Umgebungen wie AWS, Azure, Docker, VMware und traditionelle Rechenzentren. Breiteste Plattformunterstützung (Windows, Linux usw.) ermöglicht flexible Beschaffung und Lizenzierung – verbrauchsbasierte Abrechnung.
- Reduziert Kosten durch reduzierte Werkzeugsets (ein einziger Agent)
- Reduziert Kosten durch frühzeitige Identifikation von Schwachstellen in der Build Pipeline.
- Gewährleistet konsistente Sicherheit, ohne die Time-to-Market zu verlängern.

VERTRIEBSHINWEISE

- Verwenden Sie diese Informationen, um herauszufinden, ob der Schutz von DevOps und Automation für Ihren Gesprächspartner / das Unternehmen relevante Themen sind.
- Die Schlüsselfragen helfen Ihnen dabei, besser zu verstehen, wie die DevOps- und Automationsstrategie des Unternehmens aussieht, ob Container eingesetzt werden und ob ein Wettbewerbsprodukt zu Deep Security genutzt wird.
- Die Fragen richten sich in erster Linie an Personen der linken Box, können aber auch Informationen über möglicherweise relevante Personen der rechten Box liefern.
- Nachdem Sie den Interessenten mithilfe der Fragen näher kennengelernt haben, können die Gespräche telefonisch oder persönlich weitergeführt werden. Dabei sollten dann relevante Personen der rechten Box anwesend sein und die entsprechenden Rechte-Box-Fragen zur Vertiefung verwendet werden.

DEVOPS UND AUTOMATION: EINWANDBEHANDLUNG

EINWAND:
Die Integration der Sicherheit in unsere Umgebung ist einfach zu komplex und aufwändig.

REAKTION:
- Deep Security wurde speziell konzipiert, um die Automation und Integration in bestehende Toolchains zu ermöglichen.

EINWAND:
Umgebungen ändern sich konstant oder werden neu aufgebaut. Wir benötigen keine Sicherheit.

REAKTION:
- Die Integration der Sicherheit als Code mittels APIs und Skripts reduziert die Anzahl benötigter Builds. Darüber hinaus bietet Deep Security konsistenten Schutz für die CI/CD-Pipeline und stellt damit Sicherheits- und Compliance-Teams zufrieden.

EINWAND:
Sicherheit ist eine Hürde für die Entwicklung.

REAKTION:
- Deep Security nutzt einen einzigen Agenten mit einem einzigen Set von APIs. Das hilft dabei, den Aufwand für das Werkzeug-Management zu reduzieren und vereinfacht die Integration der Sicherheit in die Pipeline.

EINWAND:
Was ist mit Serverless und Lambda Sicherheit?

REAKTION:
- Trend Micro untersucht Serverless und Lambda Sicherheit. Unser Produktmanagement würde gerne mit ihnen darüber sprechen, welche Anforderungen und Erwartungen sie an Sicherheit in diesen Umgebungen haben.

DEVOPS UND AUTOMATION: ASSETS UND ANWENDERGESCHICHTEN

ASSETS (STUFE 1 BIS 5)

- **Stufe 1 bis 3 (Prospektierung)**
  - **ESG DevOps Whitepaper (englisch):** www.trendmicro.com/en_us/business/products/hybrid-cloud.html?modal=s8f-btn-learn-f8c209
  - **DevOps Webseite:** https://www.trendmicro.com/de_de/business/products/hybrid-cloud/development-operations.html
  - **Sechs Schritte zu einer stabilen Sicherheit für Container:** https://www.trendmicro.com/de_de/business/campaigns/art-of-cybersecurity/devops/steps-to-container-security.html#
- **Stufe 4 (Relevanz bestätigt)**
  - **Hybrid Cloud Security for DevOps Solution Brief (englisch):** https://www.trendmicro.com/content/dam/trendmicro/global/en/business/products/hybrid-cloud/development-operations/sb_hybrid-cloud-security-dev-ops.pdf
  - **Automation Center—Integrate using API / SDK (englisch):** https://automation.deepsecurity.trendmicro.com/
  - **Trend Micro™ Deep Security™ Smart Check Lösungsseite (englisch):** https://www.trendmicro.com/en_us/business/products/hybrid-cloud/smart-check-image-scanning.html
- **Stufe 5 (Einschätzung der technischen Lösung)**
  - **Video: Deep Security Smart Check Container Image Scanning (englisch):** www.trendmicro.com/en_us/business/products/hybrid-cloud/smart-check-image-scanning.html?modal=s3a-icon-demo-bc4a88
  - **Deep Security Smart Check und Deep Security Architekturdiagramme (englisch):** www.trendmicro.com/en_us/business/products/hybrid-cloud/smart-check-image-scanning.html?modal=s3c-icon-pdf-0f8733
- **ANWENDERGESCHICHTEN (STUFE 6+):**
  - **MEDHOST (englisch):** https://www.trendmicro.com/en_us/about/customer-stories/medhost-aws.html
  - **TRC Solutions (englisch):** https://www.trendmicro.com/en_us/about/customer-stories/trc-solutions.html
  - **Works Application (englisch):** https://www.trendmicro.com/en_us/about/customer-stories/works-applications.html
  - **Pivvot (englisch):** https://www.trendmicro.com/en_ca/about/customer-stories/pivvot.html
  - **Cloudticity (englisch):** https://www.trendmicro.com/en_ca/about/customer-stories/cloudticity-container-security.html

CONTAINER-SICHERHEIT: TERMINOLOGIE

Images	Ein Container Image ist eine unveränderliche, statische Datei, die aus mehreren Ebenen besteht. Zu den Ebenen gehören unter anderem der Anwendungscode, Datenbanken, Bibliotheken und Betriebssysteme, damit der Container als isolierter Prozess ausgeführt werden kann.
Registry	Eine Registry ist ein Repository für Container Images.
Docker	Docker ist eine Open-Source-Software-Plattform für die Generierung, Bereitstellung und Verwaltung virtualisierter Applikations-Container auf einem verbreiteten Betriebssystem. Dazu gehört ein Ökosystem verwandter Werkzeuge.
Kubernetes	Kubernetes (oftmals geschrieben als k8s) ist ein Open-Source-System für die Container-Orchestrierung. Bereitstellung, Skalierung und Management von Applikationen können mit Kubernetes automatisiert werden. Ziel ist eine „Plattform für automatisierte Bereitstellung, Skalierung und Betrieb von Applikationen über Cluster von Hosts hinweg".
Helm Chart	Helm verwendet ein Paketierungsformat namens Charts. Ein Chart ist eine Sammlung von Dateien, die ein relatives Set von Kubernetes Ressourcen beschreiben. Ein einzelner Chart kann verwendet werden, um einfache (Mem-cached Pod) oder komplexe Ressourcen (voller Web App Stack mit HTTP-Server, Datenbanken, Caches usw.) bereitzustellen.
ECS	Amazon Elastic Container Service (Amazon ECS) ist ein hoch skalierbarer und schneller Container-Management-Service, der es einfach macht, Docker Container auf einem Cluster auszuführen, anzuhalten und zu verwalten. ECS verwendet eine proprietäre Amazon Orchestrierungsschicht.
EKS	Amazon Elastic Container Service for Kubernetes (Amazon EKS) ist ein Managed Service für den einfachen Einsatz von Kubernetes auf AWS. Es muss keine eigene Kubernetes Control Plane betrieben werden. EKS verwendet die Kubernetes Standard-Orchestrierungsschicht.
GKE	Google Kubernetes Engine ist ein leistungsstarker Cluster-Manager sowie ein Orchestrierungssystem für die Ausführung von Docker Containern.
ACS	Azure Container Service (ACS) vereinfacht Erstellung, Konfiguration und Management von VM-Clustern, die für die Ausführung von Container-Applikationen vorkonfiguriert wurden.
Fargate	AWS Fargate® ist eine Computing Engine für Amazon ECS und ermöglicht die Ausführung von Containern ohne Server- oder Cluster-Management.
Microservices	Microservices sind eine Software-Entwicklungstechnik. Dabei handelt es sich um eine Variante der Service-orientierten Architektur (SOA), die eine Applikation als Sammlung lose verbundener Services strukturiert. In einer Microservice-Architektur sind die Services granular und die Protokolle schlank.

Was sind Container und warum benötigen sie Sicherheit?

- Container wickeln eine Software in eine komplettes System ein, das alle für die Ausführung benötigten Elemente enthält: Code, Laufzeit, Systemwerkzeuge und Systembibliotheken – alles, was auf einem Server installiert werden kann. Dadurch wird gewährleistet, dass die Software immer identisch ausgeführt wird, unabhängig von der Umgebung. Container laufen auf jeder Computer Hardware, in jeder Infrastruktur und in jeder Cloud. Am häufigsten werden sie aber in Verbindung mit Cloud-Infrastrukturen eingesetzt. Die Kommunikation des Containers muss ebenso wie die Host-Workloads geschützt werden. Container beinhalten Betriebssysteme und Host-Applikationen, die für Netzwerkangriffe und Bedrohungen anfällig sein können.

CONTAINER-SICHERHEIT: RECHTE BOX

SCHLÜSSELFRAGEN:

- Wie stellen sie heute neue Workloads bereit?
- Wissen sie, was ihre Teams tun, um die CI/CD Pipeline und Applikationen über Build- und Bereitstellungsumgebungen hinweg zu schützen?
- Wie sind sie in den Schutz dieser Workloads oder Umgebungen involviert? Haben sie ein DevOps Team?
- Wie verfahren sie mit Sicherheits- und Compliance-Anforderungen im Hinblick auf DevOps Teams und die CI/CD Pipeline?
- Scannen sie Code oder Applikationen auf Schwachstellen?

POSITIONIERUNG:

- Der Deep Security Agent sorgt für die Sicherheit laufender Container, indem Betriebssystem, Kubernetes, Docker und die Container-Applikation geschützt werden.
- Deep Security Smart Check durchsucht Images innerhalb der CI/CD Pipeline nach Schwachstellen, Malware, vertraulichen Informationen und Indicators of Compromise (IOCs).
- Deep Security Smart Check ist auf dem öffentlichen GitHub und kann als Kubernetes Helm Chart bereitgestellt werden.
- Automation über APIs

STICHWORTE IM GESPRÄCH:

- Docker, Kubernetes, EKS, ECS, ACS, GKS, Registry
- Kein Image Scanning – Deep Security Smart Check
- Falls Image Scanning eingesetzt wird, wie sieht es konkret aus? Diskussion möglicher Werkzeug-Konsolidierung.
- Keine Werkzeuge oder multiple Werkzeuge
- ECS (Nur Laufzeit-Schutz) und EKS (Deep Security Smart Check und Laufzeit-Schutz)
- Fargate ist ein Warnsignal (Diskussion über Deep Security Smart Check Pipeline, aber keine Laufzeit)
- Microservice-Architekturen, die häufig mit Containern genutzt werden.
- Wunsch nach Automation oder Integration der Sicherheit mit bestehendem Werkzeug-Set

VORTEILE:

- Ein einziger Agent schützt den kompletten Stack. Es müssen keine unterschiedlichen Agenten mehr für den Schutz von Hosts und Containern eingesetzt werden.
- Frühzeitige Erkennung und detaillierte Scan-Resultate ermöglichen Entwicklern die Behebung von Sicherheits-problemen, bevor sie zur Laufzeit auftreten.
- Scans können an jedem Punkt der Pipeline durchgeführt werden.

DOCKER UND KUBERNETES

Container und Container-Plattformen bieten im Vergleich zu traditioneller Virtualisierung viele Vorteile. Die Isolation erfolgt auf der Kernel-Ebene, ohne dass ein Betriebssystem benötigt wird. So sind Container wesentlich effizienter, schneller und schlanker. Die Verkapselung von Containern in eigenständigen Umgebungen führt zu einer Reihe von Vorteilen, darunter größere Parität zwischen Entwicklungsumgebungen. Docker ist derzeit die populärste Container-Plattform. Bei der Docker Engine handelt es sich um eine Laufzeit-Umgebung, die die Erstellung und Ausführung von Containern ermöglicht. Docker Hub ist ein Service für die Speicherung und gemeinsame Nutzung von Images. Insgesamt ist Docker eine Plattform und ein Werkzeug für Erstellung, Verteilung und Ausführung von Docker Containern. Mit Docker Swarm wird ein natives Clustering-Werkzeug angeboten, das für die Orchestrierung und Planung von Containern auf Maschinen-Clustern eingesetzt werden kann. Kubernetes ist ein Orchestrierungssystem für Docker Container, das über Docker Swarm hinausgeht. Fokus ist die effiziente Koordination von großangelegten Node-Clustern in der Produktion.

VERTRIEBSHINWEISE

- Sobald Sie ein Verständnis für die Container-Strategie des Kunden gewonnen haben, sollten Sie sicherstellen, dass an allen weiterführenden Diskussionen zumindest ein Container-Architekt (oder ähnliche Position) beteiligt ist. Falls in den bisherigen Gesprächen bereits Entwickler-Werkzeuge erwähnt wurden, kann außerdem die Einladung von Entwicklern bzw. Engineers ratsam sein.
- Diese zusätzlichen Fragen ermöglichen Ihnen ein besseres Verständnis der internen Arbeitsabläufe / Aufgaben beim Kunden.
- Diese Fragen richten sich an Personen der rechten Box.
- „Docker" ist der wichtigste Anbieter von Container-Software.

CONTAINER-SICHERHEIT: LINKE BOX

SCHLÜSSELFRAGEN:

- Verlagern sie ihre Workloads in die Cloud?
- Denken sie über Container nach oder sind sie bereits bei der Implementierung?
- Implementiert ihr Unternehmen neue DevOps- bzw. automatisierte Prozesse?
- Wie schützen sie heute ihre Container?
- Wer ist verantwortlich für Container-Projekte?
- Müssen sie Compliance-Anforderungen erfüllen?

POSITIONIERUNG:

- Deep Security schützt in der Build Pipeline vor Schwachstellen im Code, Malware aus öffentlichen Quellen, Verlust vertraulicher Informationen. Außerdem sorgt es für Compliance der Sicherheitsregeln (Deep Security Smart Check).
- Deep Security schützt zur Laufzeit vor Angriffen gegen laufende Container, Container-Plattformen oder das Betriebssystem, auf dem die Container gehostet werden (Deep Security).
- Deep Security unterstützt bei der Erfüllung von Compliance-Anforderungen.

STICHWORTE IM GESPRÄCH:

- Docker, Kubernetes, ECS, EKS, GKS oder ACS
- Microservice-Architektur, häufig in Verbindung mit Containern
- Automation, DevOps, CI/CD Pipeline, agile Entwicklung
- Unsicherheit hinsichtlich Container-Sicherheit oder Verwendung eines Mitbewerbers (Twistlock®, Aqua Security™)

VORTEILE:

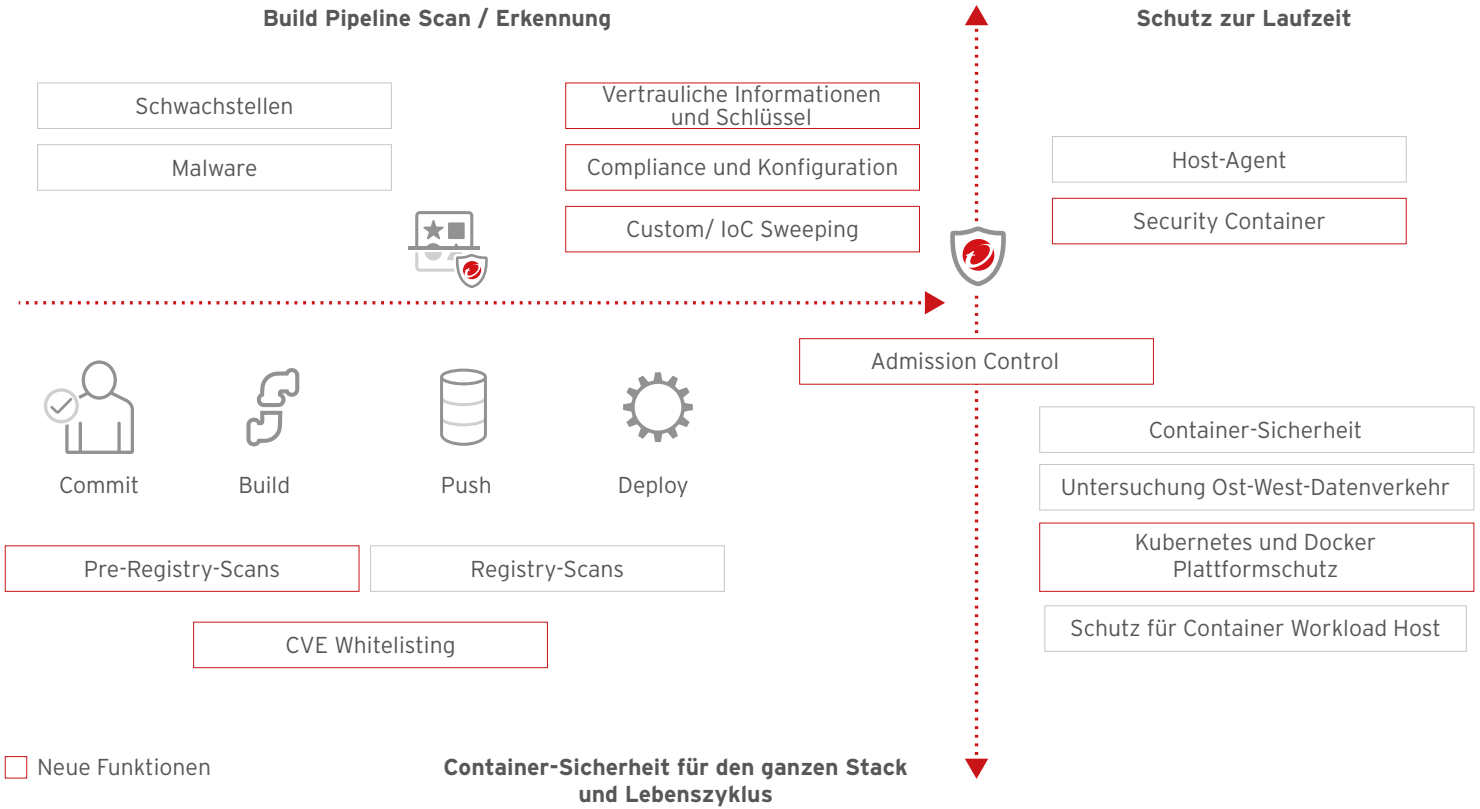
- Kontrolle von Schwachstellen in Hosts und Container-Applikationen
- Laufzeit-Funktionalität mittels eines einzigen Agenten für alle Workloads
- Bewährter Schutz durch führende globale Bedrohungsinformationen aus dem Trend Micro™ Smart Protection Network™, das kontinuierlich neue Bedrohungen identifiziert.
- Schutz vor unbekannten Bedrohungen und gezielten Angriffen
- Unterstützt bei der Compliance mit DSGVO, IT-SiG, NIS, PCI DSS, HIPAA, ISO, NIST 800-53 und anderen Regularien oder Richtlinien.

VERTRIEBSHINWEISE

- Verwenden Sie diese Informationen, um herauszufinden, ob Container-Sicherheit für Ihren Gesprächspartner / das Unternehmen ein relevantes Thema ist.
- Die Schlüsselfragen helfen Ihnen dabei, besser zu verstehen, wie die Container-Strategie des Unternehmens aussieht, welche Orchestrierungswerkzeuge eingesetzt werden und ob Automation geplant ist (DevOps Transition).
- Die Fragen richten sich in erster Linie an Personen der linken Box, können aber auch Informationen über möglicherweise relevante Personen der rechten Box liefern.
- Nachdem Sie den Interessenten mithilfe der Fragen näher kennengelernt haben, können die Gespräche telefonisch oder persönlich weitergeführt werden. Dabei sollten dann relevante Personen der rechten Box anwesend sein und die entsprechenden Rechte-Box-Fragen zur Vertiefung verwendet werden.
  - „Docker“ ist der wichtigste Anbieter von Container-Software.
  - „Kubernetes“ ist eine Open-Source-Software für die Container-Orchestrierung, die von größeren Unternehmen verwendet wird.

SCHUTZ DER CI/CD PIPELINE UND DOCKER LAUFZEIT

Anwendungsfälle für die rechte Box



- **Einen vollständigen Überblick zu den aufgeführten Funktionen finden Sie in der Kundenpräsentation:**

  https://community-trendmicro.force.com/Partner/GlobalSL_Download-Page?Id=0690B0000042KofQAE

CONTAINER SICHERHEIT: EINWANDBEHANDLUNG

EINWAND:
Wir verwenden weder Docker noch Kubernetes. Wir haben die Container-Plattform XYZ (z.B. Fargate, Pivotal®, Cloud Foundry, OpenShift usw.) im Einsatz.

Anmerkung: Diese Anforderungen stammen in der Regel aus einer BU. Nur weil eine BU etwas einsetzt, das wir heute noch nicht unterstützen, muss das nicht in anderen Teilen des Unternehmens genauso sein. Es kann sich lohnen, hier nachzufragen.

REAKTION:

- Wenn es ausschließlich um Container geht:
  - Trend Micro hat sich der Container-Sicherheit verpflichtet und unterstützt die derzeit führenden Plattformen Docker und Kubernetes. Wir treiben aber die Innovationen voran und werden auf verstärkte Nachfrage nach anderen Container-Plattformen reagieren.

- Wenn Container nur einen Teil der Diskussion bilden (mit breiteren Implikationen für die Rechenzentrumssicherheit):
  - Das Deep Security Produktmanagement würde sehr gerne über ihre Anforderungen sprechen.
  - Deep Security Smart Check scant alle populären Docker Registries, inklusive ECR, GCR, DTR, OpenShift, Azure Container Registry, Artifactory™, Nexus usw.
  - Fargate: Betonung von Deep Security Smart Check; nur sichere Images werden für die Ausführung in der Fargate Umgebung gezogen. Für Laufzeit-Schutz steht das Deep Security Produktmanagement bereit, um Anforderungen und Erwartungen zu diskutieren.

EINWAND:
Container sind flüchtig, deshalb benötigen wir keine Sicherheit.

Anmerkung: In Microservice-Architekturen haben flüchtige Container oftmals komplexe Abhängigkeiten und benötigen immer noch Schwachstellen-Scanning, um die nötige Zeit für Tests und Behebung sicherzustellen. Häufig sind Container weniger flüchtig (z.B. Migration von Legacy-Applikationen in Container) und der Wert des Schwachstellen-Scans ist unverändert relevant.

REAKTION:

- **Kennen sie die Docker Registry Cryptomining Images (englisch)?** https://techcrunch.com/2018/06/15/tainted-crypto-mining-containers-pulled-from-docker-hub/
- **Was ist mit der Kubernetes Privilege Escalation Schwachstelle (englisch)?:** https://duo.com/decipher/critical-kubernetes-bug-gives-anyone-full-admin-privileges
- Es ist irrelevant, wie lange die Images ausgeführt werden: Unternehmen sollten nicht das Risiko eingehen, dass Schwachstellen oder Malware enthalten sind. Viele Kunden „lift and shift" bestehende Applikationen in Container, die also nicht wirklich flüchtig sind.

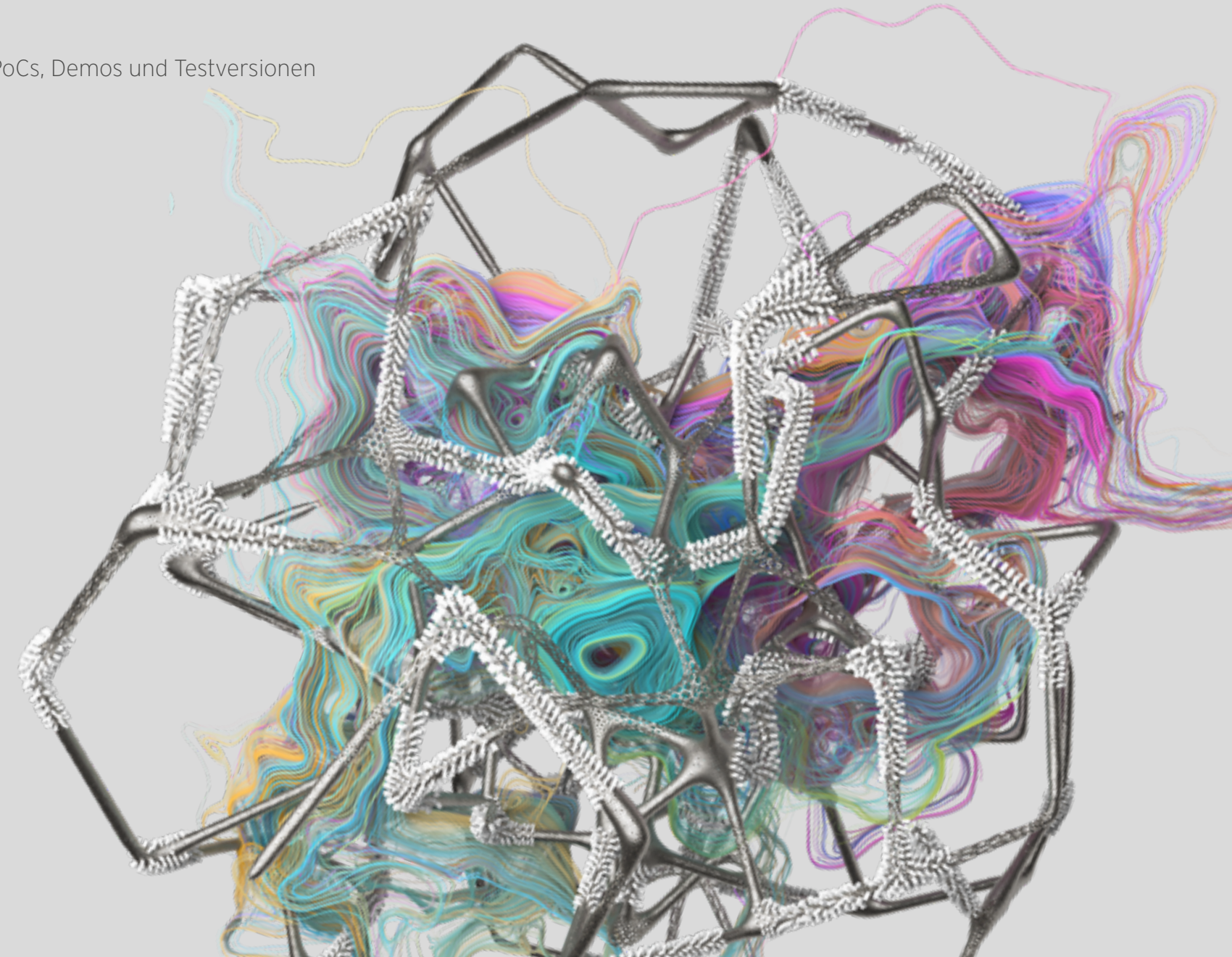
CONTAINER-SICHERHEIT: ASSETS UND ANWENDERGESCHICHTEN

ASSETS (STUFE 1 BIS 5)

- **Stufe 1 bis 3 (Prospektierung)**
  - **6 Steps to Comprehensive Container Security (englisch):** https://www.trendmicro.com/de_de/business/campaigns/art-of-cybersecurity/devops/steps-to-container-security.html#
  - **Container security Webseite (englisch):** https://www.trendmicro.com/en_us/business/products/hybrid-cloud/container.html
  - **Gartner CWPP Market Guide:** www.trendmicro.com/de_de/business/products/hybrid-cloud.html?modal=6dba25
- **Stufe 4 (Relevanz bestätigt)**
  - **Container-Sicherheit Explainer-Video (englisch):** https://www.trendmicro.com/de_de/business/products/hybrid-cloud.html?modal=s1b-hero-see-it-03bfd3
  - **Container-Sicherheit Kundenpräsentation (englisch):** https://community-trendmicro.force.com/Partner/GlobalSL_DownloadPage?Id=0690B0000042KofQAE
- **Stufe 5 (Einschätzung der technischen Lösung)**
  - **Automation Center – Integrate using API / SDK (englisch):** https://automation.deepsecurity.trendmicro.com/
  - **Proof-of-Concepts, Demos – siehe Anhang**
- **ANWENDERGESCHICHTEN (STUFE 6+)**
  - **MEDHOST (englisch):** https://www.trendmicro.com/en_us/about/customer-stories/medhost-aws.htm
  - **TRC Solutions (englisch):** https://www.trendmicro.com/en_us/about/customer-stories/trc-solutions.html
  - **Works Application (englisch):** https://www.trendmicro.com/en_us/about/customer-stories/works-applications.html
  - **Pivvot (englisch):** https://www.trendmicro.com/en_ca/about/customer-stories/pivvot.html
  - **Cloudticity (englisch):** https://www.trendmicro.com/en_ca/about/customer-stories/cloudticity-container-security.html

ANHANG

Wichtige Assets, Skripte, PoCs, Demos und Testversionen



DEEP SECURITY DEMO-UMGEBUNG

Deep Security Agent

- https://productcloud.trendmicro.com
- Dieses ist die Product Cloud. Sie benötigen ein AD-Login.
- Nutzen Sie das Login für Trend Micro Mitarbeiter mit AD. Wählen Sie dann unten „Deep Security".
- Inklusive Konnektoren für VMware, AWS und Azure

DEEP SECURITY UND DEEP SECURITY SMART CHECK TRIAL

Für Kunden:

- https://resources.trendmicro.com/DevOps-Trials.html

CONTAINER: BEISPIELSKRIPT FÜR DIE RECHTE BOX

WARUM RUFE ICH AN?

- **Soweit ich weiß, sind sie in ihrer Position verantwortlich für Container.**
- **Von Kollegen aus ihrem Fachbereich hören wir immer wieder:**
  - Traditionelle Sicherheit ist schwer zu implementieren und zu automatisieren. Deshalb ist Sicherheit ein Hindernis für Continous Integration und Bereitstellung.
  - Traditionelle Sicherheit lässt sich nur schwer mit Werkzeugen für CI/CD und DevOPs integrieren (z.B. Jenkis, GitHub, Container Registries).
  - Unternehmen unterliegen gesteigerten Anforderungen an Sicherheit und Compliance, die jetzt erfüllt werden müssen.
- **Stehen Sie auch vor diesen Herausforderungen?**
- **Wie würden ihnen gerne demonstrieren, wie sie:**
  - Sicherheit mit APIs automatisieren.
  - Sicherheit direkt in die Build Pipeline integrieren, um Continous Image Scanning zu ermöglichen und Container zur Laufzeit zu schützen.
  - Neue Risiken aus Compliance-Perspektive vermeiden, wie zum Beispiel Docker Hub Malware, Open-Source-Apps, Kubernetes Schwachstellen usw.

DEVOPS: BEISPIELSKRIPT FÜR DIE RECHTE BOX

Hallo Herr XYZ,

hier ist XXX von ABC. Haben sie zwei Minuten Zeit für mich?

Trend Micro ist der weltweit größte Cloud- und DevOps-Sicherheitsanbieter. Wir unterstützen Unternehmen beim Schutz ihrer CI/CD Pipeline und sorgen für die Einhaltung der Compliance-Anforderungen.

Unser Ziel ist, ihre Arbeit leichter zu machen und vielleicht sogar zu beschleunigen, indem wir Sicherheit direkt in die Pipeline integrieren. Dazu verwenden wir Continous-Integration-Werkzeuge wie Jenkins, Bamboo, Travis CI® und TeamCity™.

Wir haben mit anderen Entwicklern und DevOps-Profis gesprochen und dabei ist herausgekommen, dass übergreifende Sichtbarkeit benötigt wird, die sich gleichermaßen auf DevOPs und Sicherheit erstreckt. Wir wollen die Agilität ihres Unternehmens unterstützen und ihnen gleichzeitig die benötigte Sichtbarkeit und Sicherheit liefern, sodass sie die Compliance-Anforderungen erfüllen können.

Wie sieht ihre CI/CD Pipeline aus?

Viele unserer Kunden verwenden Open-Source-Software wie Jenkins. Wie schützen sie derzeit ihre Pipeline?

Verwenden sie noch andere Werkzeuge für Automation oder Orchestrierung?

Ich würde gerne mehr erfahren über ihre DevOps/App-Dev-Strategie und ihre aktuellen Herausforderungen. Vielleicht kann ich ihnen ein paar interessante Lösungsansätze zeigen. Haben sie Zeit für eine Demo am ..... um ..... ?