EU GDPR

Klaus Lenssen, Chief Security Officer - Cisco Deutschland

www.cisco.de/trustoffice

Disclaimers :

- Ich bin kein Jurist …
- … noch machen wir irgendeine Form der Rechtsberatung.
- Diese Folien sind keine offizielle Cisco Position bzgl. EU GDPR oder der Adaption der GDPR im Unternehmen
- Diese Folien sind ein Überblick und Interpretation der EU GDPR und sind als Einstieg in das Thema gedacht.
- Dies ist eine informelle Informationsveranstaltung und KEIN formelles Training

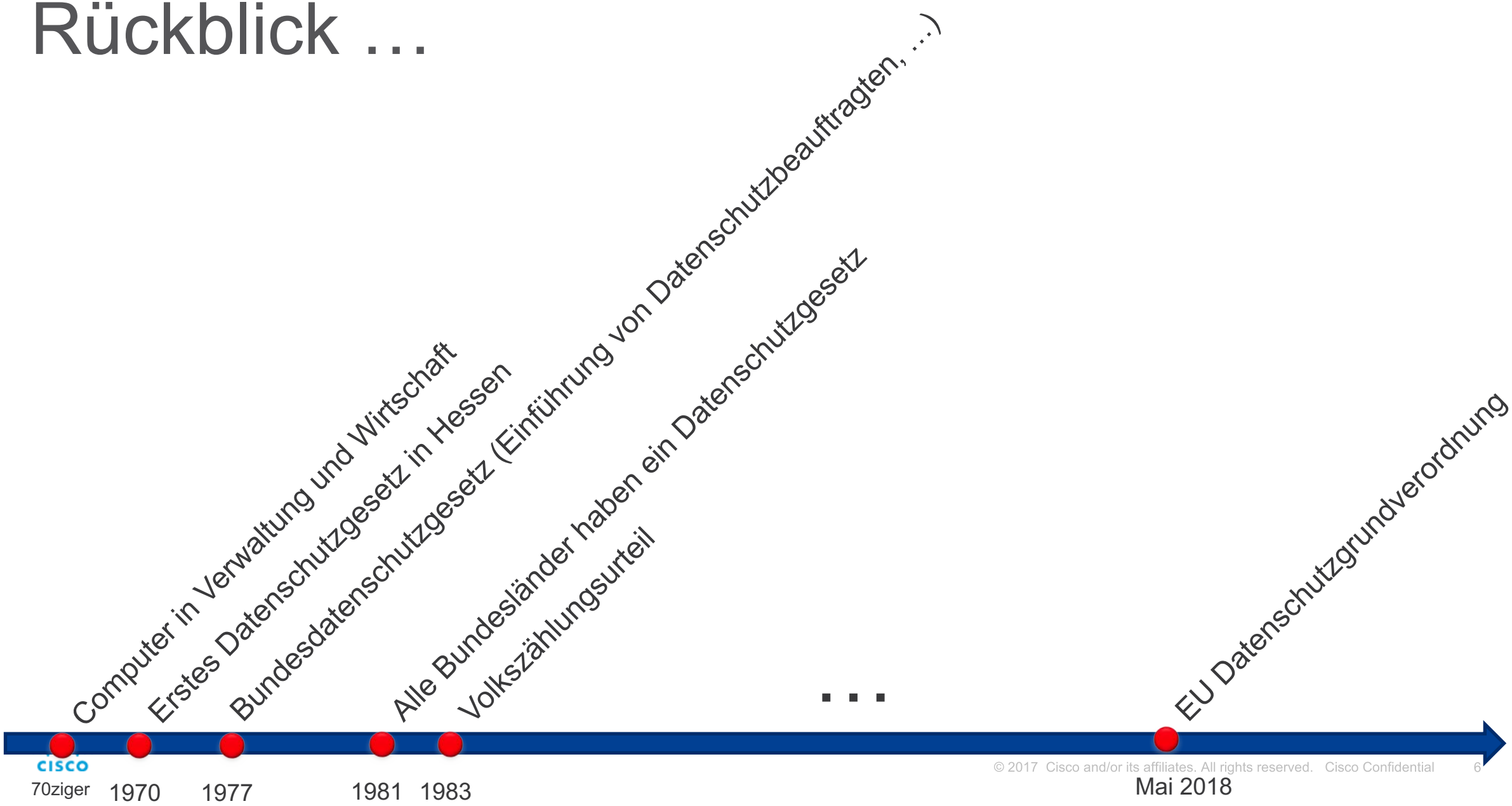
Warum Datenschutz?

Warum Datenschutz?

Warum Datenschutz?

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Rückblick …



Informationelle Selbstbestimmung

Herleitung des Grundrechts

- Art. 1, Abs. 1 GG: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.„
- Art. 2, Abs. 1 GG: "Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

Inhalt der Informationellen Selbstbestimmung

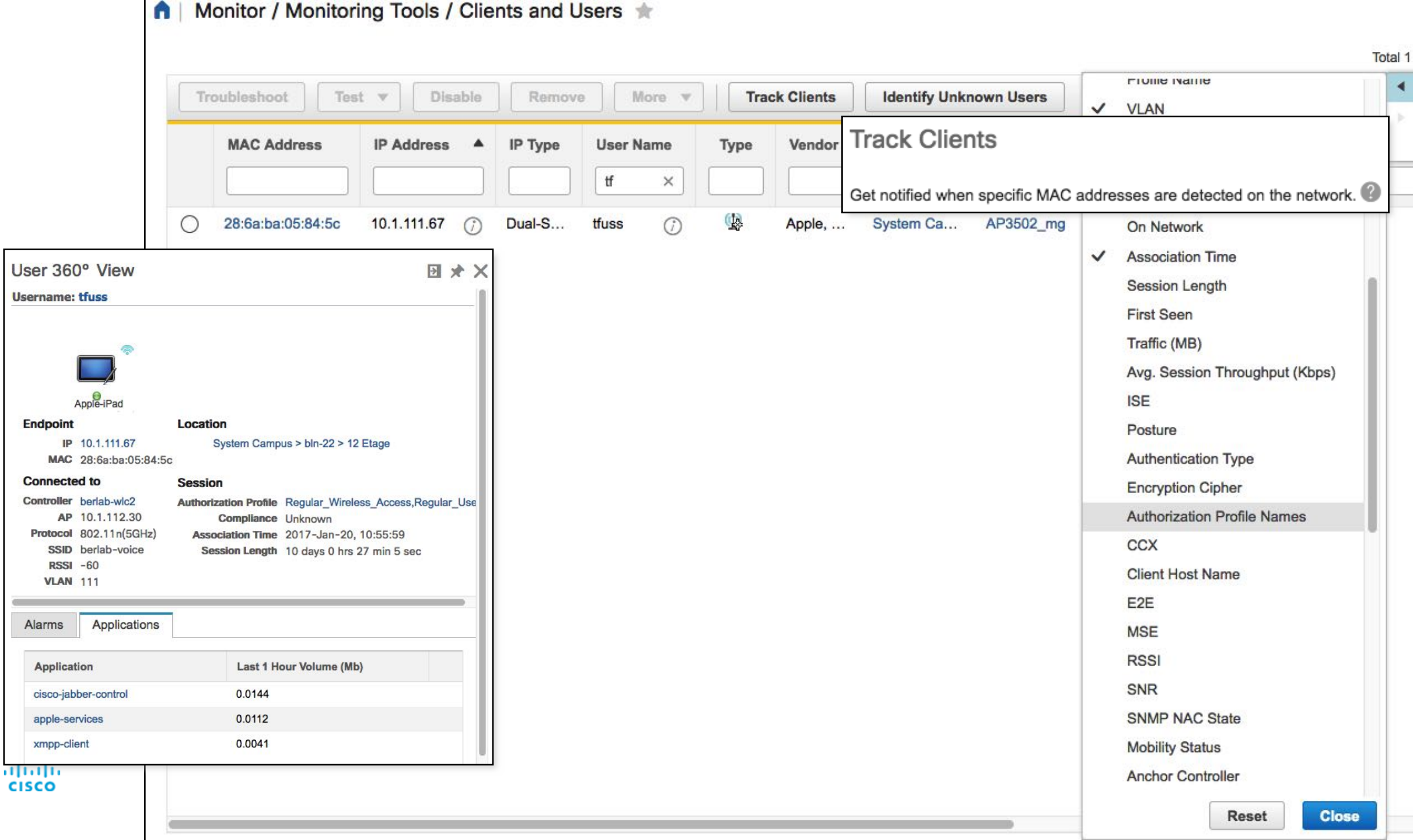
1. Recht der Selbstbestimmung über die Preisgabe und Verwendung eigener Daten zu bestimmen
2. Schutz der Privatsphäre
3. Freie Entfaltung der Persönlichkeit
4. Aufrechterhaltung fairer Kommunikationsverhältnisse

Personenbezogene Daten § 3 BDSG

- Natürliche Person
  - Kein Schutz für juristischer Personen mangels Menschenwürde.
    Aber: Schutz der natürlichen Person hinter der juristischen Person (Unternehmer)
    Ggf. postmortales Persönlichkeitsrecht?
- Einzelangaben über persönliche oder sachliche Verhältnisse
  - Es gibt kein belangloses Datum unter den Bedingungen der automatischen Datenverarbeitung (Volkszählungsurteil).
    Alle Informationen, die über die Bezugsperson etwas aussagen.
- Bestimmte oder bestimmbare Person (Betroffener), § 3 BDSG
  - Aus den Angaben muss sich ergeben, dass sie sich auf Person beziehen.

Personenbezogene Daten § 3 BDSG

- Name, Geburtsdatum, Geburtsort, Telefonnummer – **sind das personenbezogene Daten?**
- Reicht es, wenn ich das zum Beispiel durch eine IP-Adresse verschleiere damit sie nicht mehr zuzuordnen sind – Pseudonymisierung?
- Was bedeutet Anonymisierung, damit ich meine Daten ohne die starken Einschränkungen des Datenschutzes verarbeiten kann?
  - Verändern von personenbezogenen Daten derart, dass Einzelangaben über persönliche oder sachliche Verhältnisse nicht oder nur unter unverhältnismäßig großem Aufwand an Zeit, Kosten, Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet werden können
  - Kein Personenbezug mehr!

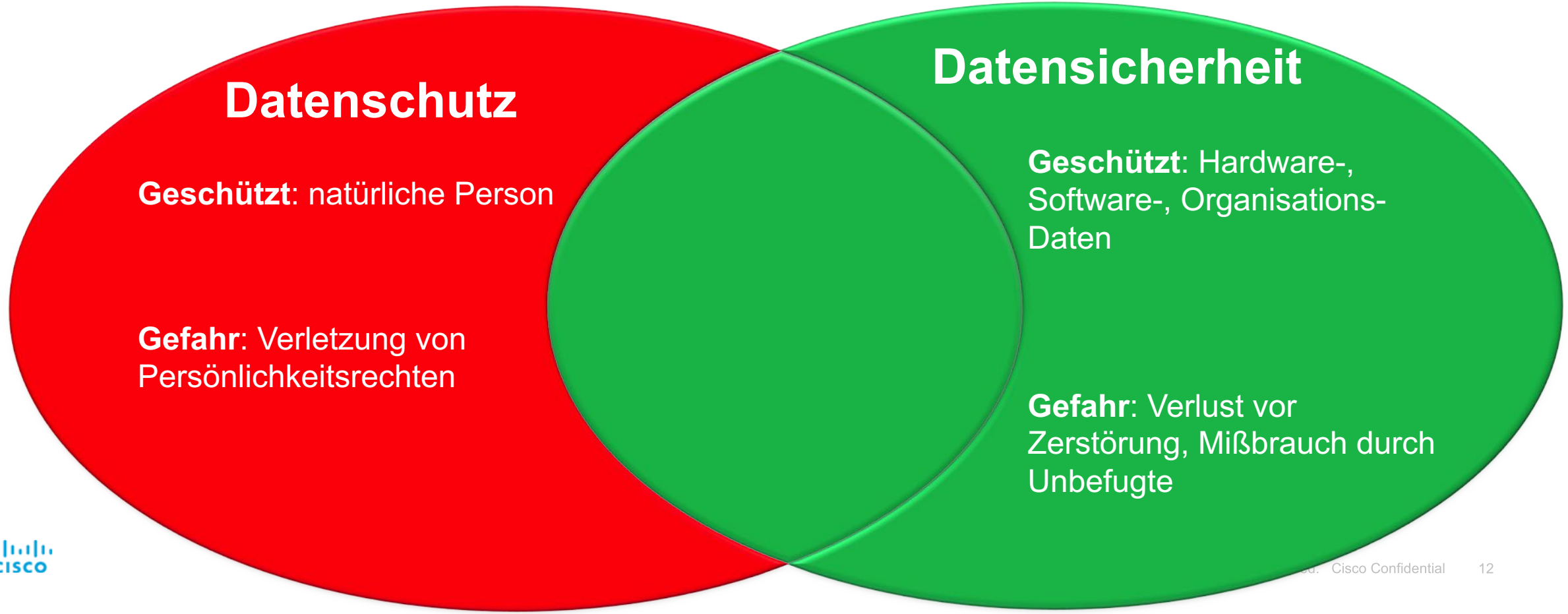

Monitor / Monitoring Tools / Clients and Users
Total 1
Troubleshoot
Test
Disable
Remove
More
Track Clients
Identify Unknown Users
MAC Address
IP Address
IP Type
User Name
Type
Vendor
tf
28:6a:ba:05:84:5c
10.1.111.67
Dual-S…
tfuss
Apple, …
System Ca…
AP3502_mg
Track Clients
Get notified when specific MAC addresses are detected on the network.
VLAN
On Network
Association Time
Session Length
First Seen
Traffic (MB)
Avg. Session Throughput (Kbps)
ISE
Posture
Authentication Type
Encryption Cipher
Authorization Profile Names
CCX
Client Host Name
E2E
MSE
RSSI
SNR
SNMP NAC State
Mobility Status
Anchor Controller
Reset
Close
User 360° View
Username: tfuss
Apple-iPad
Endpoint
IP 10.1.111.67
MAC 28:6a:ba:05:84:5c
Location
System Campus > bln-22 > 12 Etage
Connected to
Controller berlab-wlc2
AP 10.1.112.30
Protocol 802.11n(5GHz)
SSID berlab-voice
RSSI -60
VLAN 111
Session
Authorization Profile Regular_Wireless_Access,Regular_Use
Compliance Unknown
Association Time 2017-Jan-20, 10:55:59
Session Length 10 days 0 hrs 27 min 5 sec
Alarms
Applications
Application
Last 1 Hour Volume (Mb)
cisco-jabber-control 0.0144
apple-services 0.0112
xmpp-client 0.0041

Datenschutz vs Datensicherheit

- Was Bedeutet der Begriff Datenschutz?
  - Schutz von Daten ⇒ Schutz der Person, deren Daten verarbeitet werden!

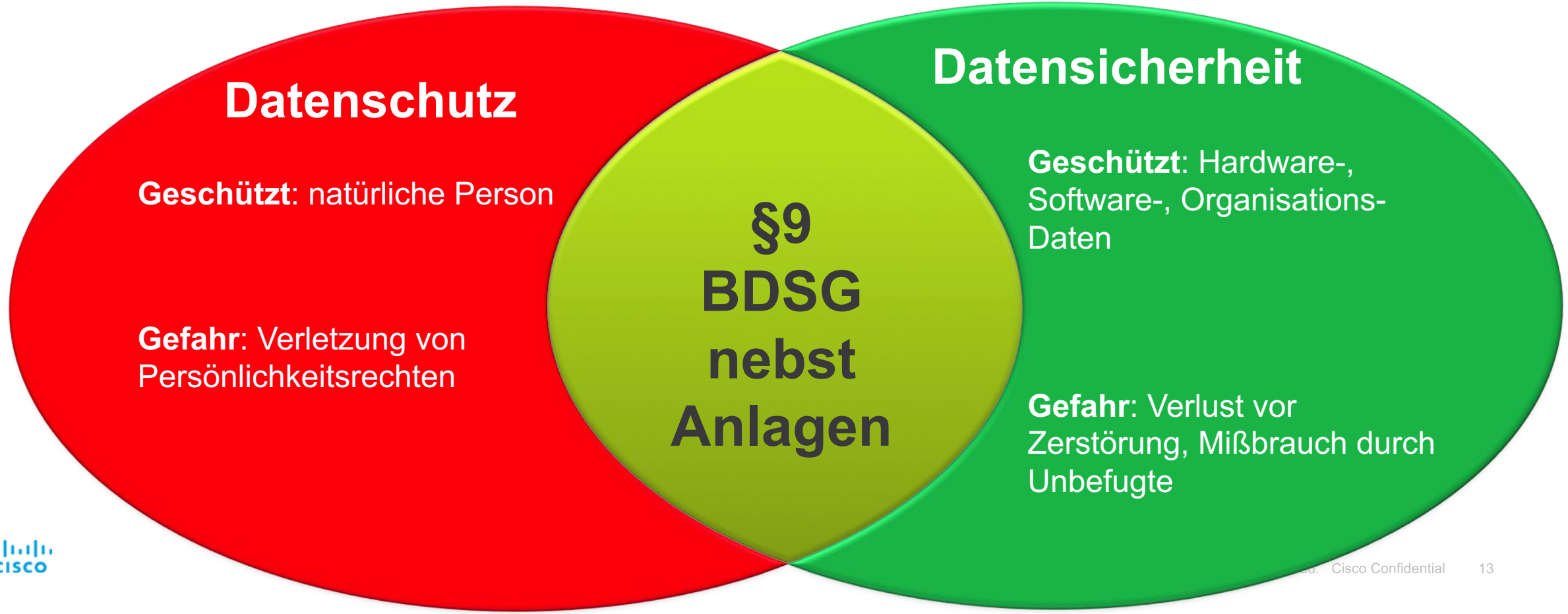
Datenschutz vs Datensicherheit

- Was Bedeutet der Begriff Datenschutz?
  - Schutz von Daten ⇒ Schutz der Person, deren Daten verarbeitet werden!



Datenschutz vs Datensicherheit

- Was Bedeutet der Begriff Datenschutz?
  - Schutz von Daten ⇒ Schutz der Person, deren Daten verarbeitet werden!



Wie funktioniert Datenschutz?
Sieben Goldene Regeln

Rechtmäßigkeit
- Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung

Einwilligung
- Informiert und freiwillig

Zweckbindung
- Verwendung nur für Erhebungszweck

Erforderlichkeit und Datensparsamkeit
- Verarbeitung nur soweit für Erhebungszweck erforderlich

Transparenz und Betroffenenrechte
- Unterrichtung über Verwendung, Auskunfts-/Berichtigungs-/Löschrechte

Datensicherheit
- Technische und organisatorische Maßnahmen

Kontrolle
- Interner / externer Datenschutzbeauftragter
- Audit

Rechtmäßigkeit

- **Kern**: Datenverarbeitung ist verboten, sofern nicht erlaubt in Gesetz oder via Einwilligung
  - § 4 Bundesdatenschutzgesetz
    - „(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“

EU Perspektive

- Harmonisierung der nationalen Vorschriften
- Bisher Datenschutz-Richtlinie 95/46/EG
- Nationale Vorschriften müssen mindestens an die Datenschutz Richtlinie angepasst werden
- Weitergehende Harmonisierung gewünscht, daher Arbeit an Verordnung von 2012-2017

EU Menschenrechtskonvention

- **Artikel 8 Schutz personenbezogener Daten**
  - (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
  - (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
  - (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Grundrecht auf Datenschutz
EU Grundrechtecharta

- Art. 7 EuGRCh – Achtung des Privat- und Familienlebens
  - Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.
- Art. 8 EuGRCh – Schutz personenbezogener Daten
  - (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
  - (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlichen legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
  - (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

EU GDPR
Anwendungsbereich / Grundprinzipien

- Verarbeitung von personenbezogenen Daten
  - **Art. 2 Abs. 1 GDPR** eröffnet den sachlichen Anwendungsbereich bei einer ganz oder teilweise automatisierten Verarbeitung oder eine nicht automatisierte Verarbeitung von personenbezogenen Daten stattfindet.
  - Ausnahmen regelt **Art. 2 Abs. 2 GDPR.**

- **Grundsätze bleiben unverändert:**
  - Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - Zweckbindung
  - Richtigkeit
  - Erforderlichkeit (Speicherbegrenzung)
  - Integrität und Vertraulichkeit - Datensicherheit
  - Verantwortlichkeit (Rechenschaftspflicht)
  - NEU: Datenminimierung

EU GDPR
Übermittlung in Drittstaaten

- Zulässig, wenn Verantwortliche und Auftragsverarbeiter die niedergelegten Bedingungen erfüllen und die sonstigen Bestimmungen der GDPR erfüllt sind
- Wenn die EU Kommision festgestellt hat, dass ein angemessenes Datenschutzniveau besteht
- Wenn Verantwortliche und Auftragsverarbeiter geeignete Garantien vorgesehen hat und durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen
  - Hierzu gehören auch ”Binding Corporate Rules”
  - Oder Standarddatenschutzklauseln, die von der Kommision oder der Aufsichtsbehörde angenommen werden
- Weitere Sonderfälle vorgesehen

Cisco Systems, Inc.

● Active Participant

Other Covered Entities

Industries

Participation

Privacy Policy

Dispute Resolution

Other Covered Entities

- Acano Federal LLC
- Acano LLC
- Cisco OpenDNS LLC
- Cisco Systems Capital Corporation
- Cisco Systems, Inc.
- Cisco WebEx LLC
- CliQr Technologies LLC
- CloudLock LLC
- Jasper International Services LLC
- Jasper Technologies LLC
- Neohapsis International LLC
- Neohapsis, Inc.
- One Mainstream LLC
- ParStream LLC
- Scientific-Atlanta LLC

Privacy Shield

Cisco Systems, Inc.

● Active Participant

Other Covered Entities

Industries

Participation

Privacy Policy

Dispute Resolution

Industries

- Information and Communications Technology
  - Computer Hardware
- Information and Communications Technology
  - Computer Software
- Information and Communications Technology
  - Computer Systems
- Information and Communications Technology
  - Cybersecurity
- Information and Communications Technology
  - Information Technology Services
    - Computer Services

- One Mainstream LLC
- ParStream LLC
- Scientific-Atlanta LLC

Privacy Shield

Cisco Systems, Inc.

● Active Participant

Participation

EU-U.S. PRIVACY SHIELD FRAMEWORK FRAMEWORK: ACTIVE

Original Certification Date:
10/27/2016

Next Certification Due Date:
10/27/2017

Industries

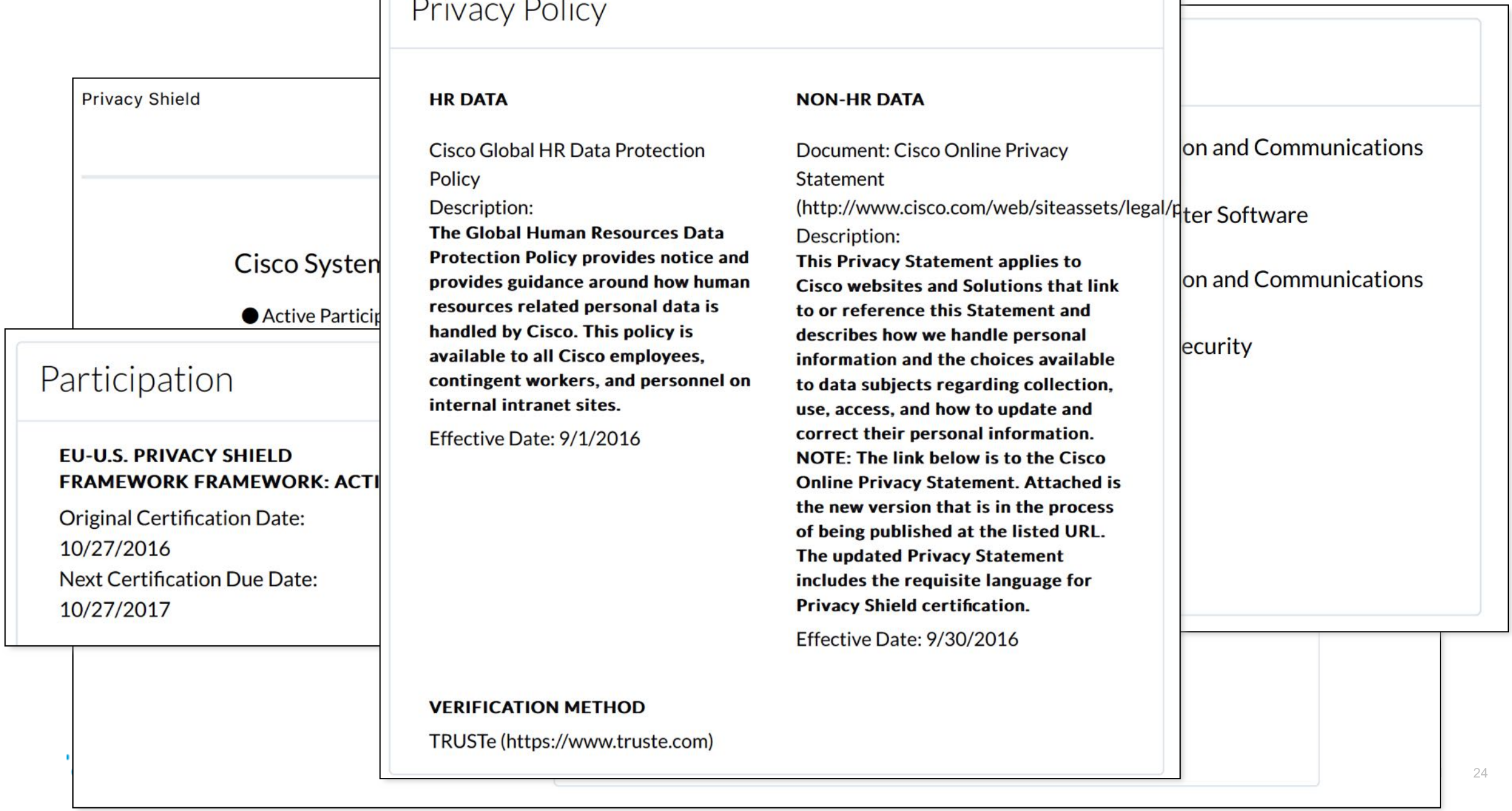
- Information and Communications Technology
  - Computer Hardware
- Information and Communications Technology
  - Computer Software
- Information and Communications Technology
- Information and Communications Technology
  - Cybersecurity

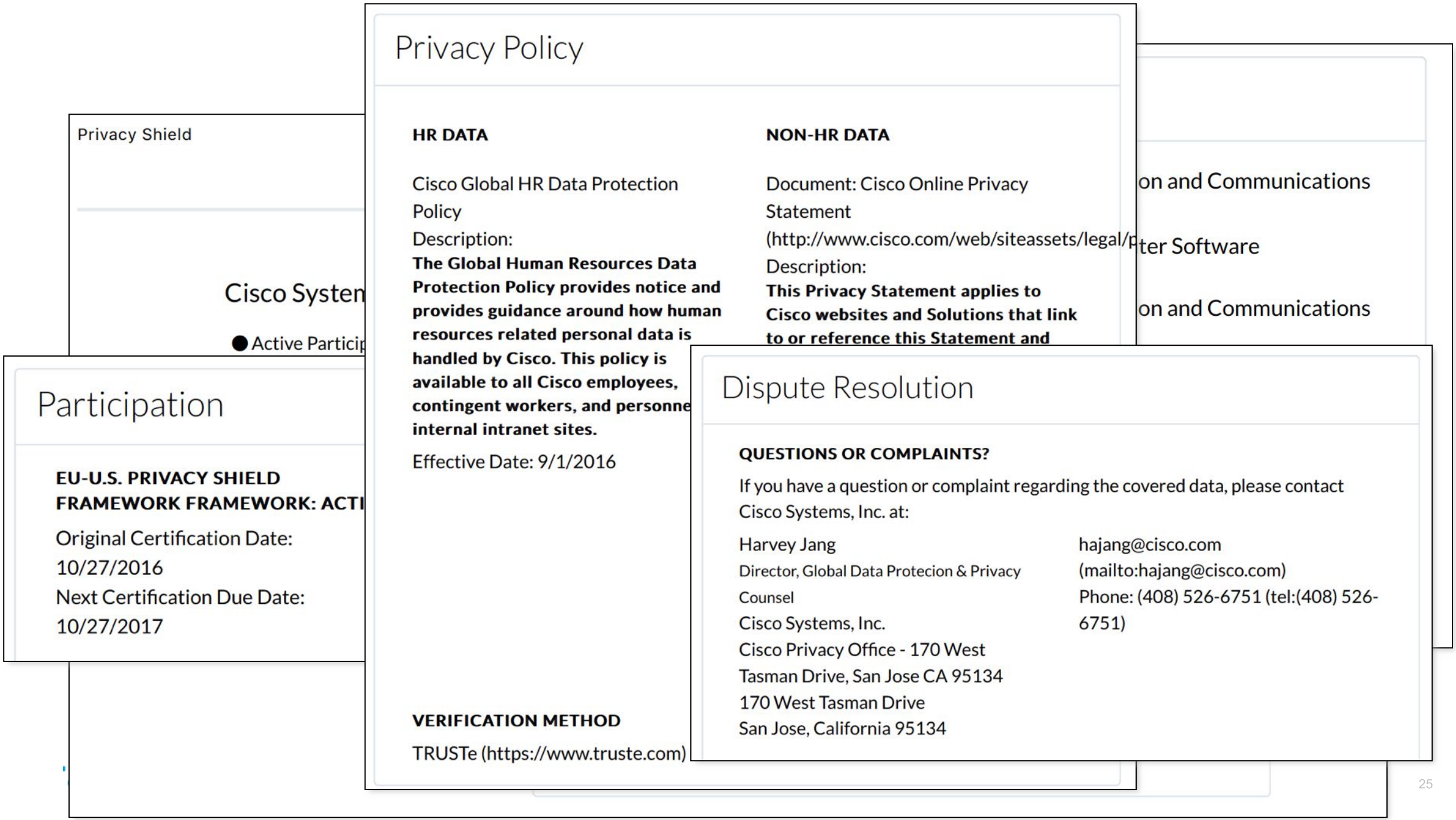
munications

logy

es

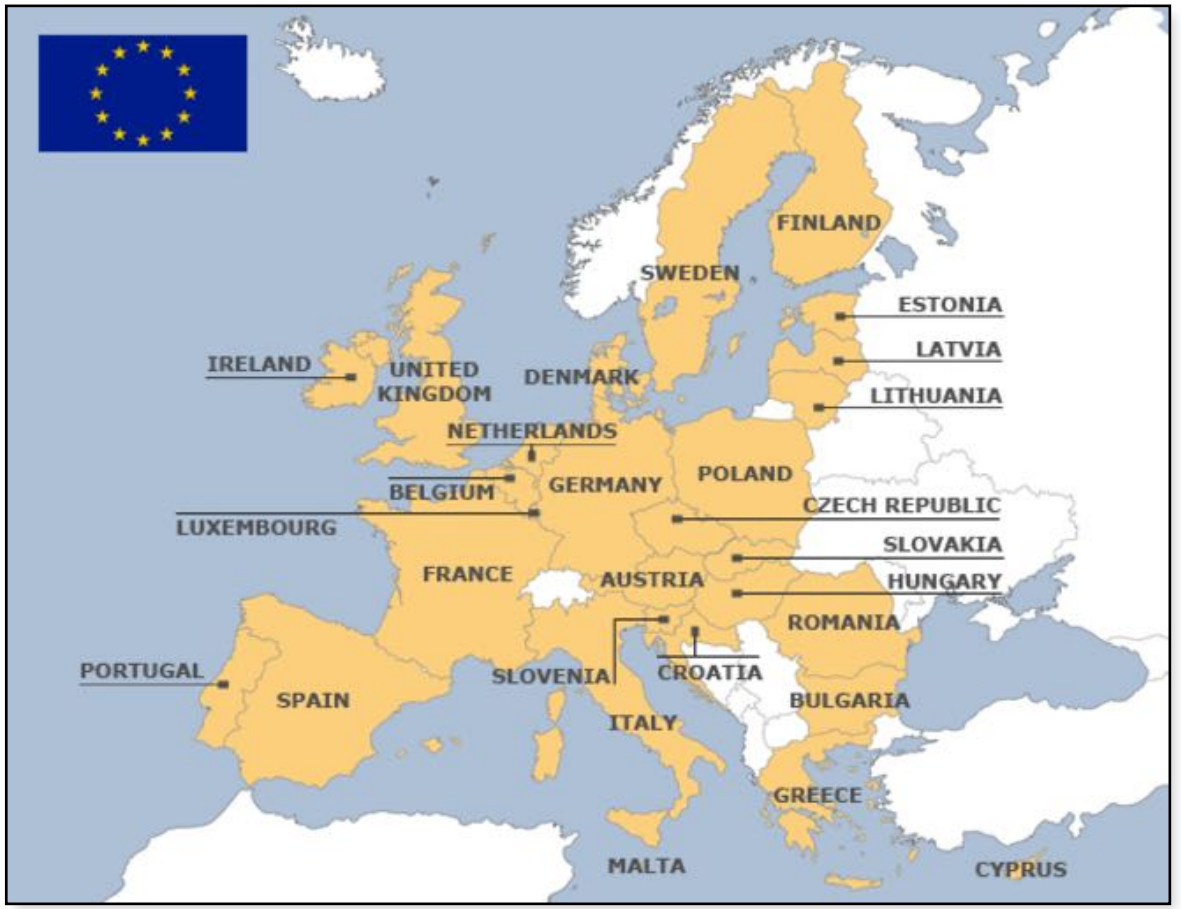
- One Mainstream LLC
- ParStream LLC
- Scientific-Atlanta LLC


Privacy Shield
Cisco Systen
Active Particip
Participation
EU-U.S. PRIVACY SHIELD FRAMEWORK FRAMEWORK: ACTI
Original Certification Date: 10/27/2016
Next Certification Due Date: 10/27/2017
Privacy Policy
HR DATA
Cisco Global HR Data Protection Policy
Description:
The Global Human Resources Data Protection Policy provides notice and provides guidance around how human resources related personal data is handled by Cisco. This policy is available to all Cisco employees, contingent workers, and personnel on internal intranet sites.
Effective Date: 9/1/2016
NON-HR DATA
Document: Cisco Online Privacy Statement
(http://www.cisco.com/web/siteassets/legal/p
Description:
This Privacy Statement applies to Cisco websites and Solutions that link to or reference this Statement and describes how we handle personal information and the choices available to data subjects regarding collection, use, access, and how to update and correct their personal information. NOTE: The link below is to the Cisco Online Privacy Statement. Attached is the new version that is in the process of being published at the listed URL. The updated Privacy Statement includes the requisite language for Privacy Shield certification.
Effective Date: 9/30/2016
VERIFICATION METHOD
TRUSTe (https://www.truste.com)
on and Communications
ter Software
on and Communications
ecurity


Privacy Shield
Cisco Systen
Active Particip
Participation
EU-U.S. PRIVACY SHIELD FRAMEWORK FRAMEWORK: ACTI
Original Certification Date: 10/27/2016
Next Certification Due Date: 10/27/2017
Privacy Policy
HR DATA
Cisco Global HR Data Protection Policy
Description:
The Global Human Resources Data Protection Policy provides notice and provides guidance around how human resources related personal data is handled by Cisco. This policy is available to all Cisco employees, contingent workers, and personne internal intranet sites.
Effective Date: 9/1/2016
VERIFICATION METHOD
TRUSTe (https://www.truste.com)
NON-HR DATA
Document: Cisco Online Privacy Statement
(http://www.cisco.com/web/siteassets/legal/p
Description:
This Privacy Statement applies to Cisco websites and Solutions that link to or reference this Statement and
on and Communications
ter Software
on and Communications
Dispute Resolution
QUESTIONS OR COMPLAINTS?
If you have a question or complaint regarding the covered data, please contact Cisco Systems, Inc. at:
Harvey Jang
Director, Global Data Protecion & Privacy Counsel
Cisco Systems, Inc.
Cisco Privacy Office - 170 West Tasman Drive, San Jose CA 95134
170 West Tasman Drive
San Jose, California 95134
hajang@cisco.com
(mailto:hajang@cisco.com)
Phone: (408) 526-6751 (tel:(408) 526-6751)

EU GDPR Marktortprinzip

- größte Änderung gegenüber bisherigen Regelungen
- **Art. 3 GDPR**:
  - Unerheblich ob Datenverarbeitung in Europa stattfindet
  - Unabhängig vom Sitz der verarbeitenden Stelle



EU GDPR
Meldepflichten

- Erweiterung der bestehenden allgemeinen Meldepflichten
- Jede Verletzung des Schutzes personenbezogener Daten, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, zu einer Meldepflicht an die Aufsichtsbehörde (Art. 33).
- Unverzügliche Meldung = ohne schuldhaftes Zögern (Frist 72 Std.)
- Direkte Benachrichtigung der Betroffen bei hohem Risiko (Art. 34)
- Pflicht der Dokumentation der Verletzung.

Sanktionen vermeiden:
Bis zu 20 Mio oder 4% des Jahresumsatzes – je nachdem welcher Betrag höher ist.

Wo können wir unterstützen ?

- Technische Maßnahmen
- Technik oder datenschutzfreundliche Voreinstellungen

… ergibt aus den geforderten TOMs:

- 1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
- 2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
- 3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),
- 4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
- 5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
- 6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
- 7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
- 8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

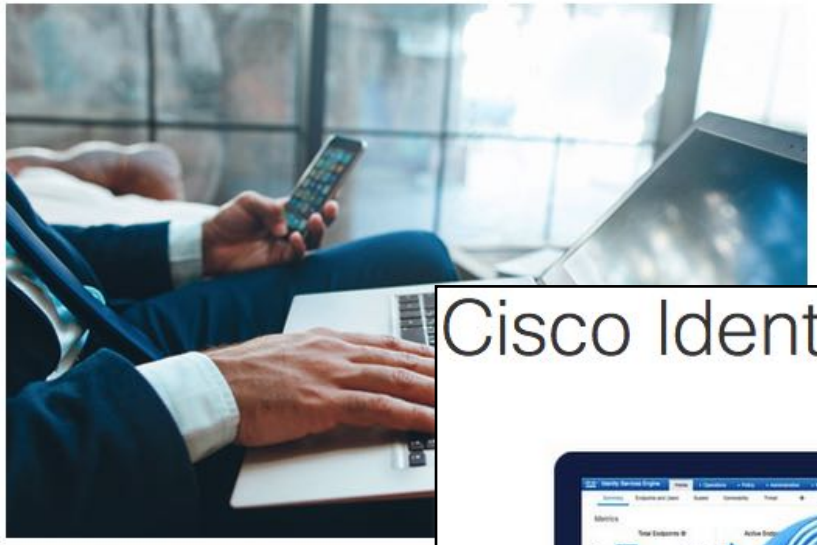
… ergibt aus den geforderten TOMs:

- 1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
- 2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
- 3. zu g… Zugrif… …zung und nach …
- 4. zu g… …r ihrer Speich… …d festge… …rtragung vorgesehen ist (**Weitergabekontrolle**),
- 5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
- 6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
- 7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
- 8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

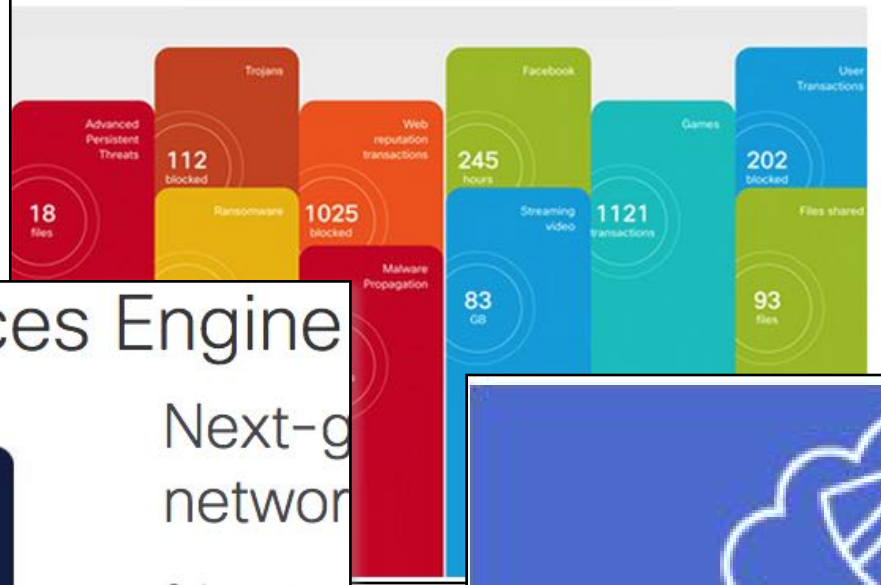
… insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Security Produkte (Beispiele)

Cisco Email Security



Cisco Web Security

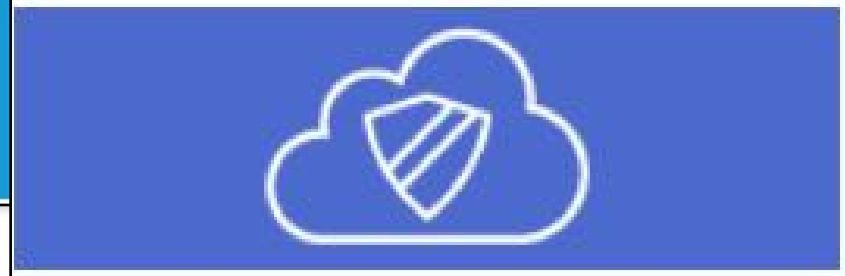


Cisco Identity Services Engine

Next-g
networ

Gain awarene
access consis
complex acce

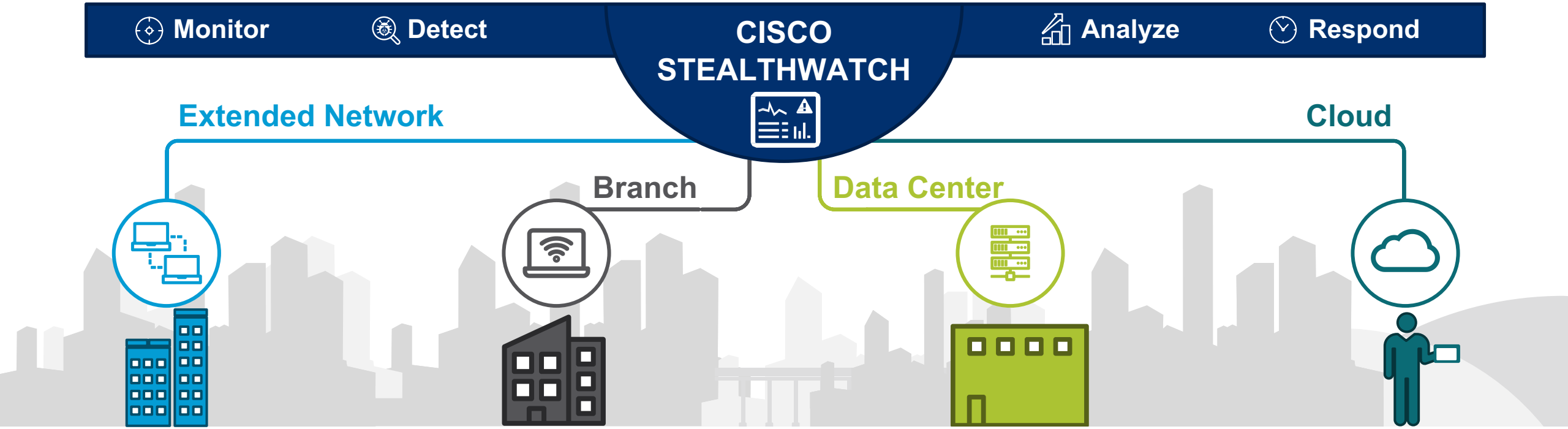
ISE in 3



OpenDNS Umbrella

Use our cloud-delivered network security service to protect any device, anywhere.

Stealthwatch enhances visibility across your entire business



- Gain unique visibility across your business
- Simplify segmentation throughout your networks
- Address threats faster

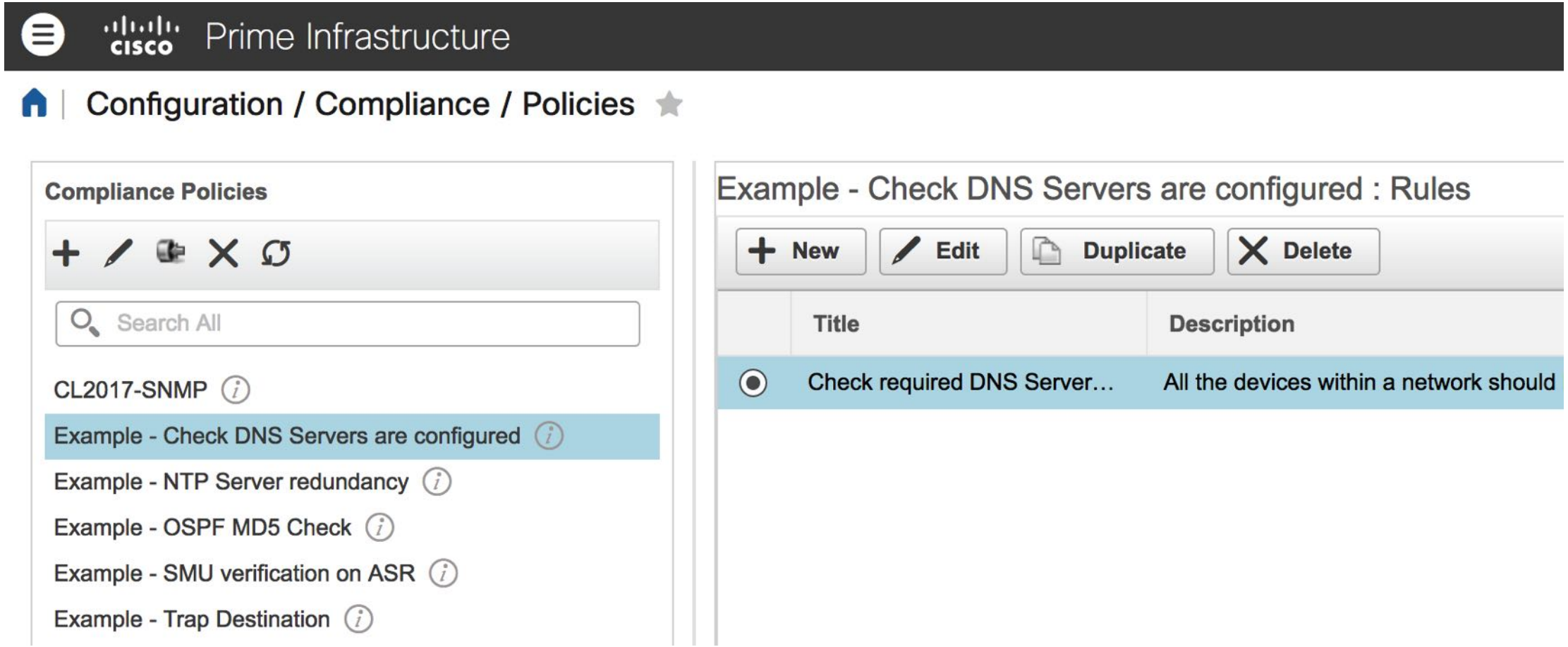
- Enable your network to take action
- Extend visibility and granular access control to your remote branches
- Prevent the lateral movement of threats

- Protect your critical information
- Simplify policy enforcement and data center segmentation
- Accelerate incidence response in the data center

- Gain enhanced visibility into the cloud
- Make the cloud a part of your segmentation strategy
- Identify threats quickly and take action

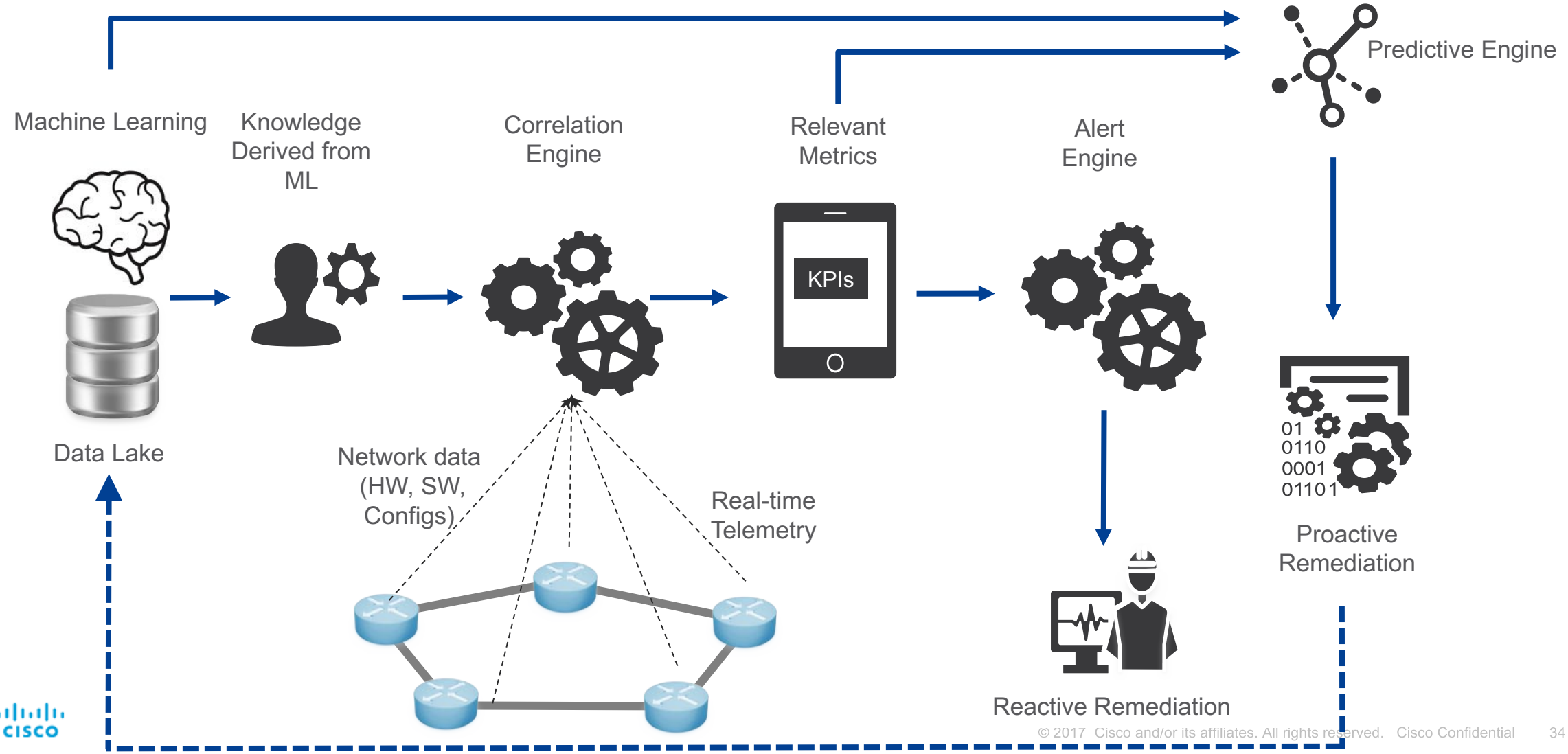
Cisco Services and Customer Success

Prime Infrastructure

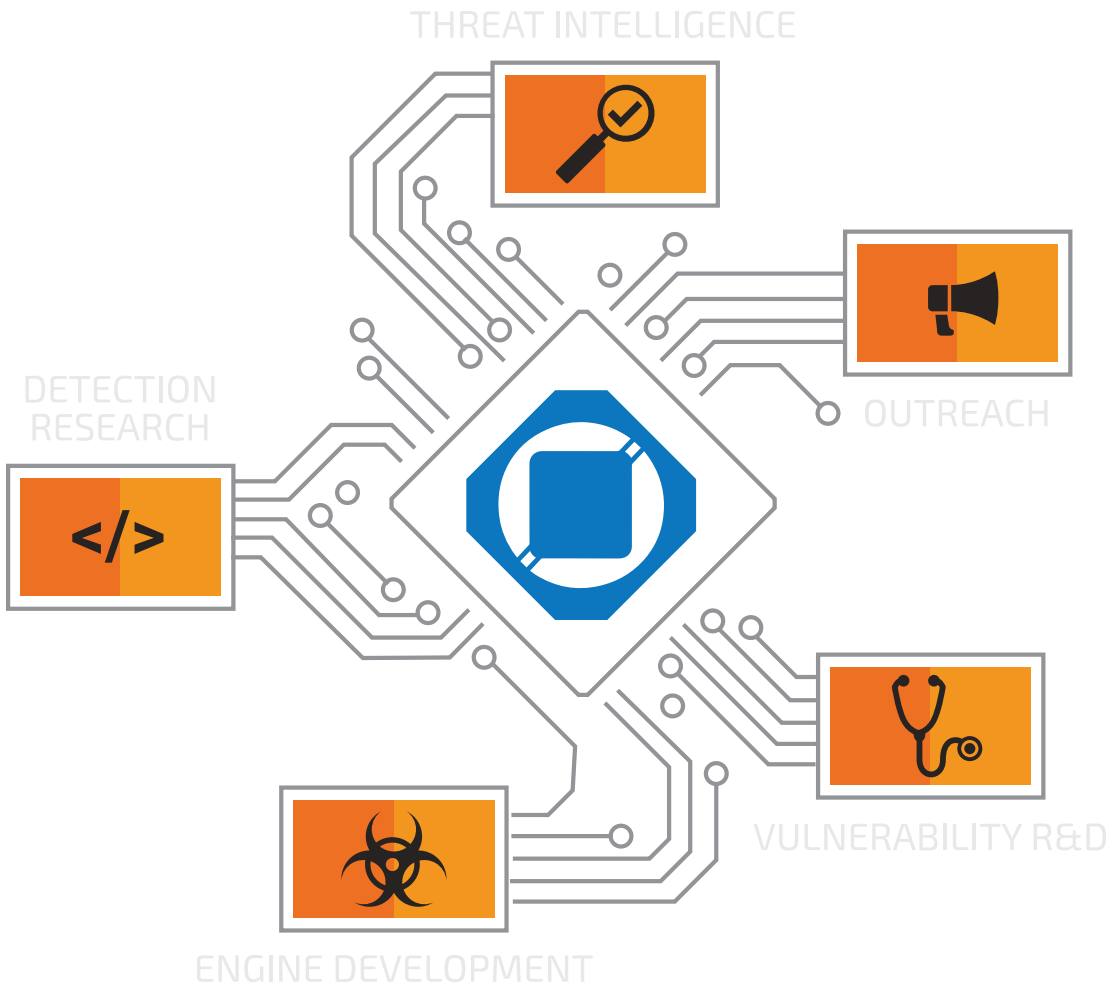


Moving from Reactive to Proactive Remediation

Pulse App – KPI's and Predictive Maint



Who is Talos

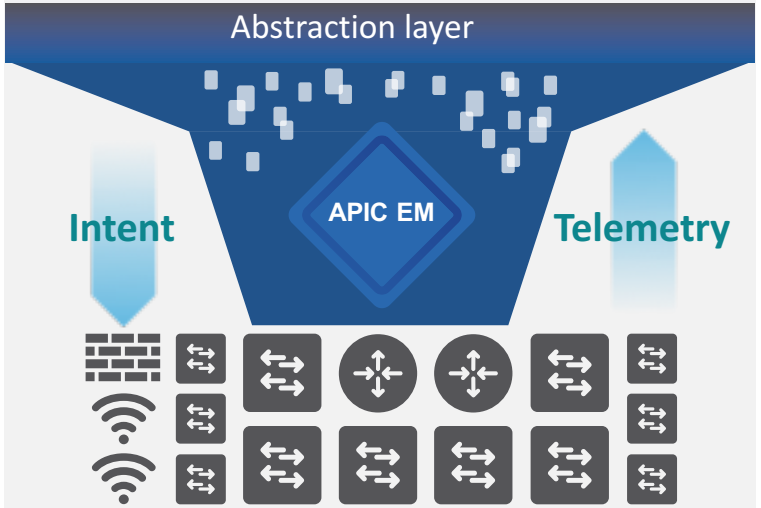


- **Cisco's threat intelligence organization**
  - Threat hunting
  - Malware analysis
- **5 groups** collaborating to produce threat intel
  - Reputation feeds, signatures, IOC
  - Security engines and tools
  - Threat reports and blogs
- **Who is behind Talos**
  - Cisco, Ironport, Sourcefire, ScanSafe,…
  - RevEng, Data Scientists, Spam -, Web-, DNS-, BGP-Experts, …

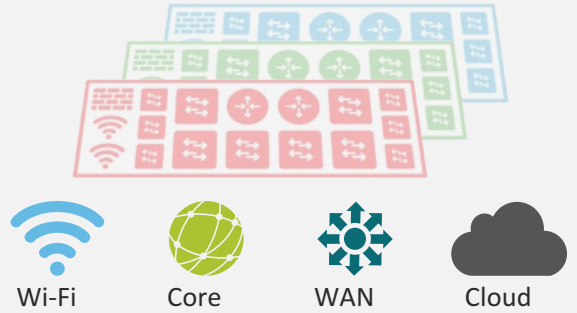
Network Requirements for the Digital Organization

- **Visibility** into Users behavior, Applications, Network performance
- Customer has the elements to **make decisions faster**

- Abstraction, Intent, Policy → **Automation**
- Verification of Desired Result → **Assurance**



Using the Network as a Sensor for security threats and then Enforce Compliancy through **Segmentation**

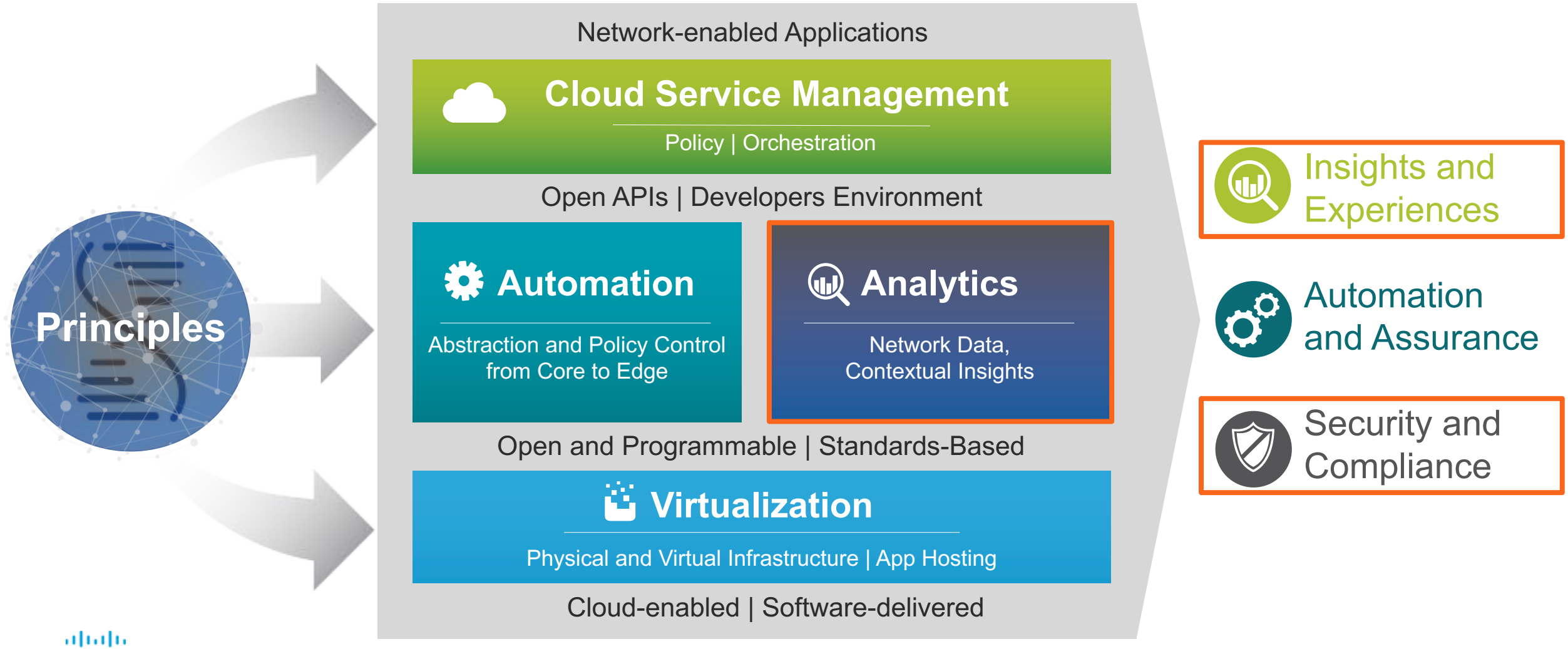


Drive Business Innovations

Speed, Simplicity & Visibility

Real-time and Dynamic Threat Defense

Cisco Digital Network Architecture



Deploy, Report, Measure, Adjust, Repeat

Digital Network Architecture

Network-enabled Applications

Cloud Service Management
Policy | Orchestration

Open APIs | Developers Environment

Automation
Abstraction & Policy Control from Core to Edge

Analytics
Network Data, Contextual Insights

Open & Programmable | Standards-Based

Virtualization
Physical & Virtual Infrastructure | App Hosting

Cloud-enabled | Software-delivered

Analytics

Apps Ecosystem
Customer Experience | Workforce Experience | Developer Experience

Network Data Graphs
Distributed | Structured | Correlated

Data Processing
Normalization | Curation | Contextualization

Data Ingestion
Identity | Location | Network Traffic | Applications

Network Elements

Developer Efficiencies: Multi-tenant cloud and on-premises support complete with standards-based APIs, Natural Language Processing, 3rd party integrations, and DevNet ecosystem

Analytics Efficiencies: leverage built-in 1) enrichment of network events with contextual metadata, 2) correlation across multiple data sources, and 3) situational context via knowledge-based databases and ML analytics

Single Source of Curated Network Data: Not just collector of raw logs and metrics, but normalizing and organizing data both in-motion and at-rest for real-time and batch processing

Telemetry Quotient: automatically assess network monitoring capabilities as well as provide Tesseract-orchestrated telemetry configuration and collector provisioning across the entire network fabric

Telemetry Efficiencies: eliminate unnecessary overhead on edge platforms by providing the right data - rich, low-bandwidth, pre-processed telemetry across switching, routing, and wireless systems

Cisco DNA Analytics

A highly flexible and modularized enterprise analytics tool which provides a 360 degree / end-to-end and granular view of the network and associated services

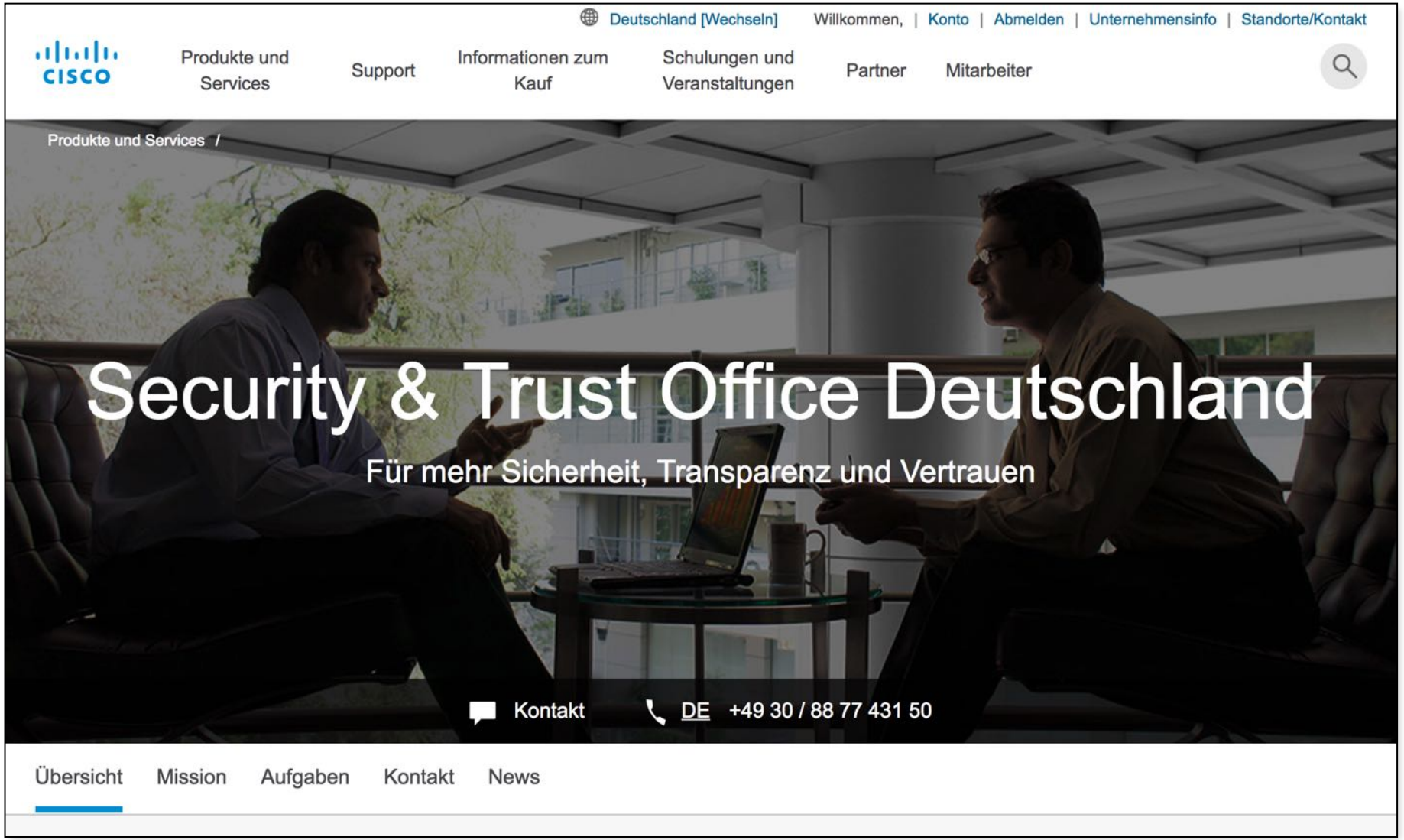
Security Advisory Services

Cisco Privacy Advisory Services: General Data Protection Regulation

Build Trust with your Clients

Trust and responsible information management practices are becoming business differentiators as consumers become more aware of the impact of data breaches and the potential misuse of personal information. This is especially true within the context of digital business initiatives that collect and analyze increasingly more information about customers and employees.

By 2018, organisations which hold data on EU citizens through which it is possible to identify an individual, must comply with the General Data Protection Regulation (GDPR).



www.cisco.de/trustoffice

Das Cisco Security & Trust Office Deutschland

Security-Fragen
zu Cisco-Produkten

Absolute Transparenz

Offene Zusammenarbeit

Ausbildung & Best-Practices

Fragen

Weiterführende Informationen

- **www.cisco.de/trustoffice**

- www.cisco.com/web/go/dataprotection
- http://www.cisco.com/go/ise
- http://www.cisco.com/go/primeinfrastructure
- www.cisco.com/web/go/dna
- www.cisco.com/web/go/opendns
- www.cisco.com/web/go/wsa
- www.cisco.com/web/go/esa

IT-Sicherheitsgesetz

IT Sicherheitsgesetz

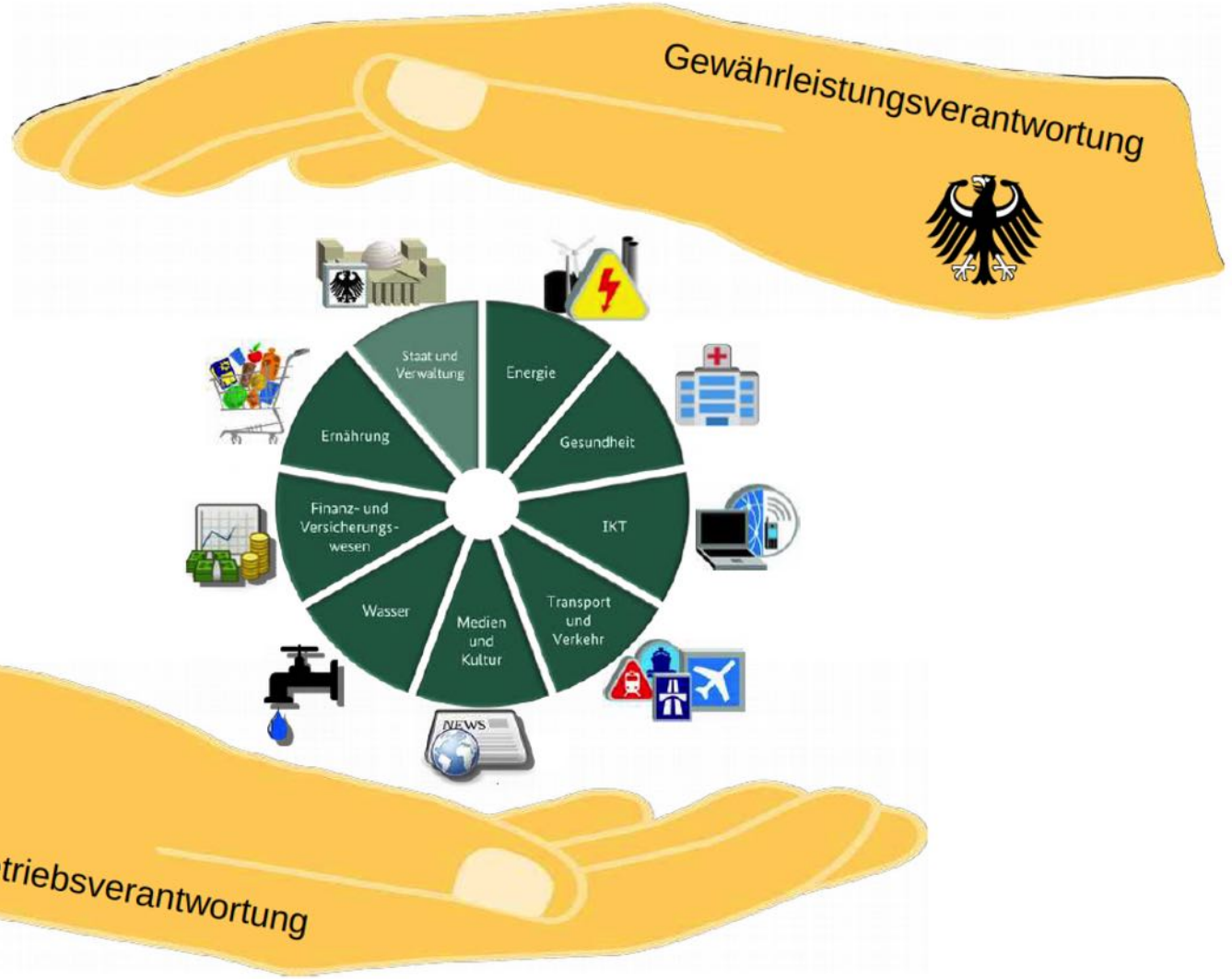
- *Sicherstellung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit informationstechnischer Systeme (IT-Sicherheit): Pflicht zur Einhaltung eines Mindestniveaus an IT-Sicherheit für Betreiber Kritischer Infrastruktur sowie zur Meldung erheblicher Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI), Gewährleistung des Fernmeldegeheimnisses, des Schutzes personenbezogener Daten sowie der Verfügbarkeit der Datenverarbeitungssysteme durch die Telekommunikationsanbieter, Überprüfung der Sicherheitskonzepte durch die Bundesnetzagentur, Benachrichtigung der Nutzer über Sicherheitsvorfälle, Vorlage eines Jahresberichts, Festschreiben des BSI als Zentralstelle für IT-Sicherheit, Stärkung des BKA im Bereich Cyberkriminalität; Änderung versch. § § von 8 Gesetzen; Verordnungsermächtigung*

TLP Green

Schutz Kritischer Infrastrukturen

- Schutzbedürfnis -

UP KRITIS



Bundesamt für Sicherheit in der Informationstechnik

Adressaten des Gesetzes

- Betreiber Kritischer Infrastrukturen
  - Energie
  - Informationstechnik und Telekommunikation
  - Wasser
  - Ernährung
  - Transport und Verkehr
  - Gesundheit
  - Finanz- und Versicherungswesen

IT-SIG Korb 2 - SCHWELLWERTE GESUNDHEIT

Entwurf 27. Feb 2017

- Krankenhäuser: ab 30.000 stationären Fällen pro Jahr
- Produktionsstätten und Abgabestellen für Medizinprodukte: ab einem Jahresumsatz von 90,6 Millionen Euro
- Produktionsstätten, Betriebs- und Lagerräume sowie Anlagen zum Vertrieb für verschreibungspflichtige Arzneimittel und Apotheken: ab 4,65 Millionen Packungen im Jahr
- Labore, Transportsysteme und Kommunikationssysteme zur Auftrags- oder Befundübermittlung: ab 1,5 Millionen Aufträgen im Jahr
- Anlagen oder Systeme zur Steuerung von Entnahme und Weiterverarbeitung von Blutspenden: ab 34‘000 Produkten im Jahr

Das Artikelgesetz IT-SiG

UP KRITIS

- Das IT-SiG umfasst Änderungen folgender Gesetze:
  - BSI-Gesetz
  - Atomgesetz
  - Energiewirtschaftsgesetz
  - Telemediengesetz
  - Telekommunikationsgesetz
  - Bundeskriminalamtgesetz

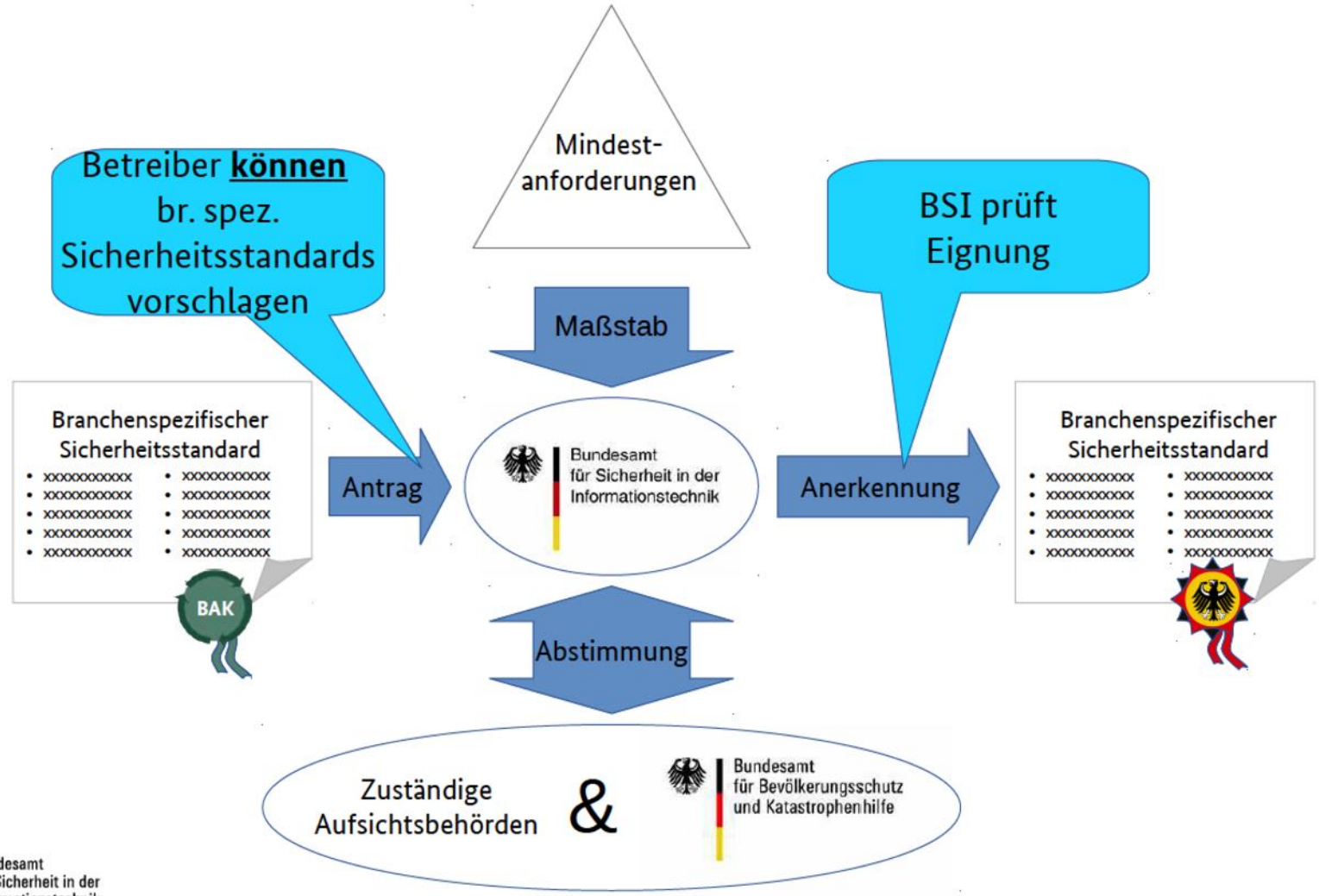
- § 8a: Sicherheit in der Informationstechnik Kritischer Infrastrukturen
- §8b: Bedrohungs- und Verfügbarkeitslagebild

Bundesamt für Sicherheit in der Informationstechnik

TLP Green

Sicherheit in der Informationstechnik Kritischer Infrastrukturen (§8a)

UP KRITIS

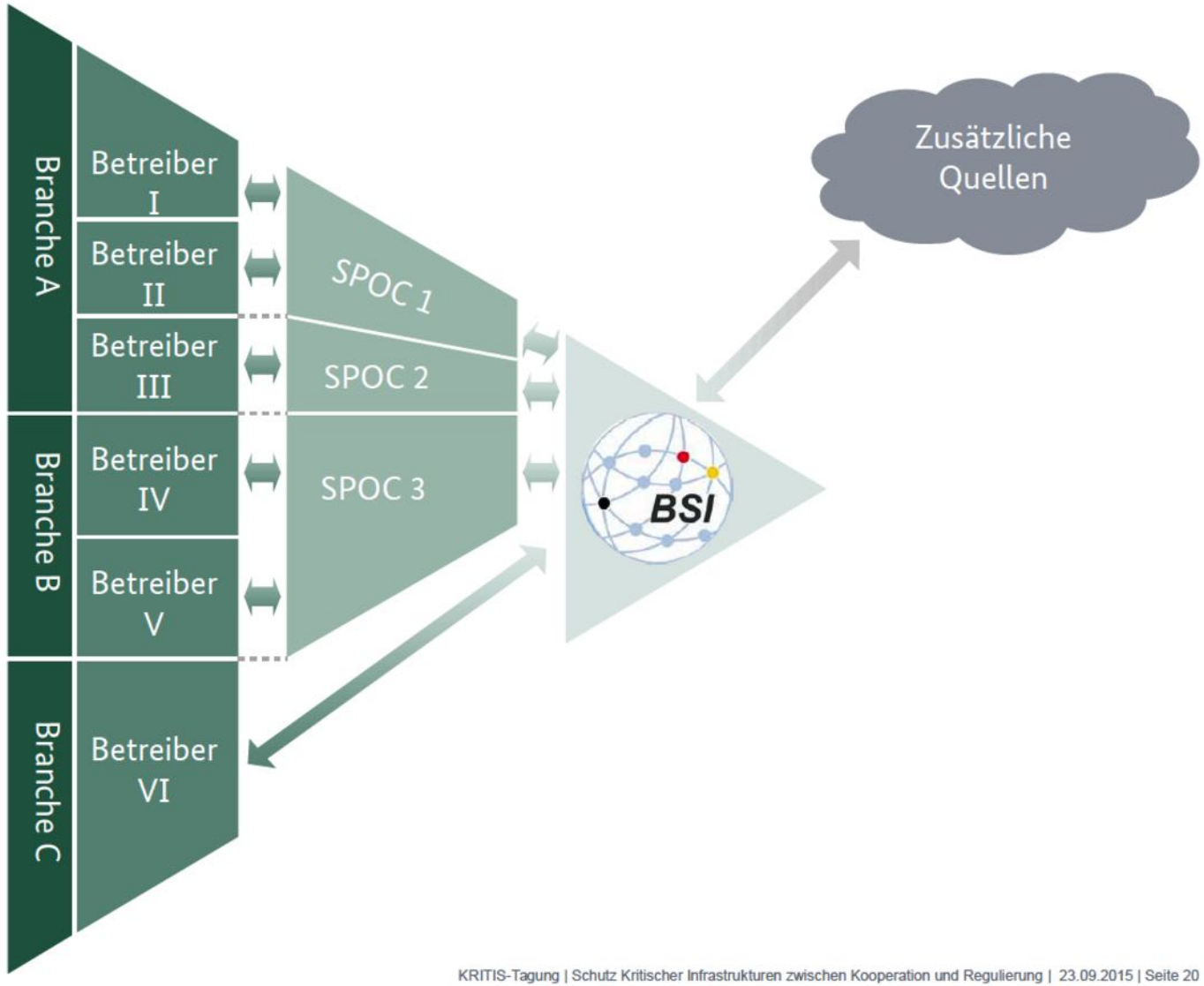


Bundesamt für Sicherheit in der Informationstechnik

TLP Green

Meldepflichten & Lagebilder
- Meldewege im UP KRITIS -

UP KRITIS



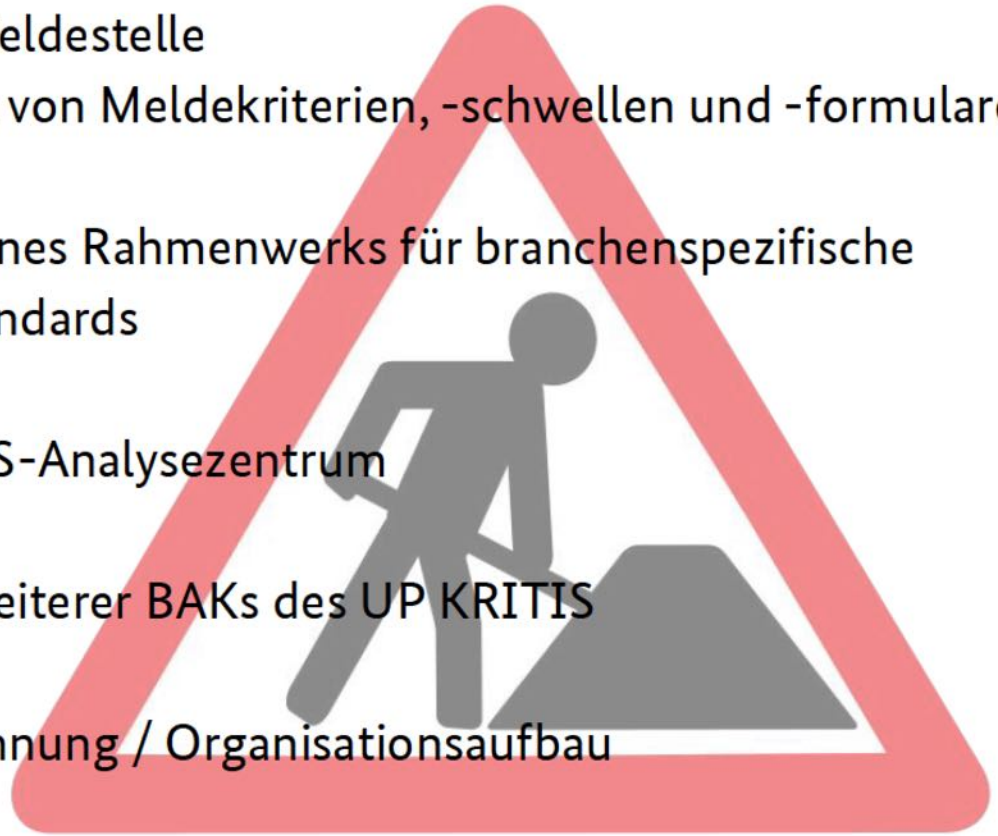
Bundesamt für Sicherheit in der Informationstechnik

TLP Green

Vorarbeiten zur Umsetzung des IT-Sicherheitsgesetzes im BSI

UP KRITIS

- Einrichtung Meldestelle
  - Definition von Meldekriterien, -schwellen und -formularen
- Erarbeitung eines Rahmenwerks für branchenspezifische Sicherheitsstandards
- Aufbau KRITIS-Analysezentrum
- Einrichtung weiterer BAKs des UP KRITIS
- Personalgewinnung / Organisationsaufbau



Bundesamt für Sicherheit in der Informationstechnik

Schutz vor Cyberattacken

- Schützen:
  - Ergreifen „angemessener organisatorischer und technischer Vorkehrungen“ zum Schutz der eigenen Infrastruktur vor Cyber-Angriffen auf Basis eines vom BSI abgenommenen branchenweiten Standards - § 8a (1)

Schutz vor Cyberattacken

- Kontrollieren:
  - Nachweisen der Erfüllung der Anforderungen aus dem ITSiG alle zwei Jahre; bei Feststellung von Sicherheitsmängeln kann das BSI im Einvernehmen mit der zuständigen Aufsichtsbehörde die Beseitigung dieser verlangen - § 8a (3)

Schutz vor Cyberattacken

- Erreichbarkeit:
  - Benennen einer Kontaktstelle, über die das Unternehmen jederzeit vom BSI erreichbar ist - § 8b (3)

Schutz vor Cyberattacken

- Informieren:
  - Unverzügliches Melden von Cyber-Angriffen mit erheblichen Auswirkungen an das BSI - § 8b (4)

Meldepflicht gilt für Betreiber kritischer Infrastrukturen erst nach Inkrafttreten der Rechtsverordnung

Schutz vor Cyberattacken

- Das Gesetz enthält auch Bußgeldvorschriften (§ 14). Diese sehen eine Sanktionierung der Unternehmen, die die neuen gesetzlichen Anordnungen nicht befolgen von bis zu 100.000 Euro vor.


CISCO