Post-Quantum

Cryptography Conference

Practical Insights from Following NIST SP 1800-38B

In this session, Dr. Alexander Löw from Data-Warehouse will share real-world experiences from the National Cybersecurity Center of Excellence (NCCoE) regarding the implementation of NIST SP 1800-38B. Alexander will delve into the practical application of public key application discovery tools within the context of transitioning to PQC. Participants will gain insights into the step-by-step process outlined in SP 1800-38B, including identifying public key cryptographic algorithms in use, assessing their vulnerability to quantum attacks, developing a migration strategy, and implementing new PQC algorithms. By walking through the challenges encountered, attendees gain insights into what to expect during their transition, and learn about the role and benefits of Cryptographic Agility, Cryptographic Inventory, Cryptographic Bill of Material (CBOM), Software Bill of Material (SBOM), and Cryptographic Governance, providing comprehensive insights based on real-world experiences from following the National Cybersecurity Center of Excellence (NCCoE).

Alexander Löw
CEO at Data-Warehouse

SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

January 15 and 16, 2025 - Austin, TX (US) | Online

PKI Consortium

Data-Warehouse GmbH
Cybersecurity

Practical Insights from Following NIST SP 1800-38B

Alexander Loew

Theoretical aspects

Action Blocks 1-5

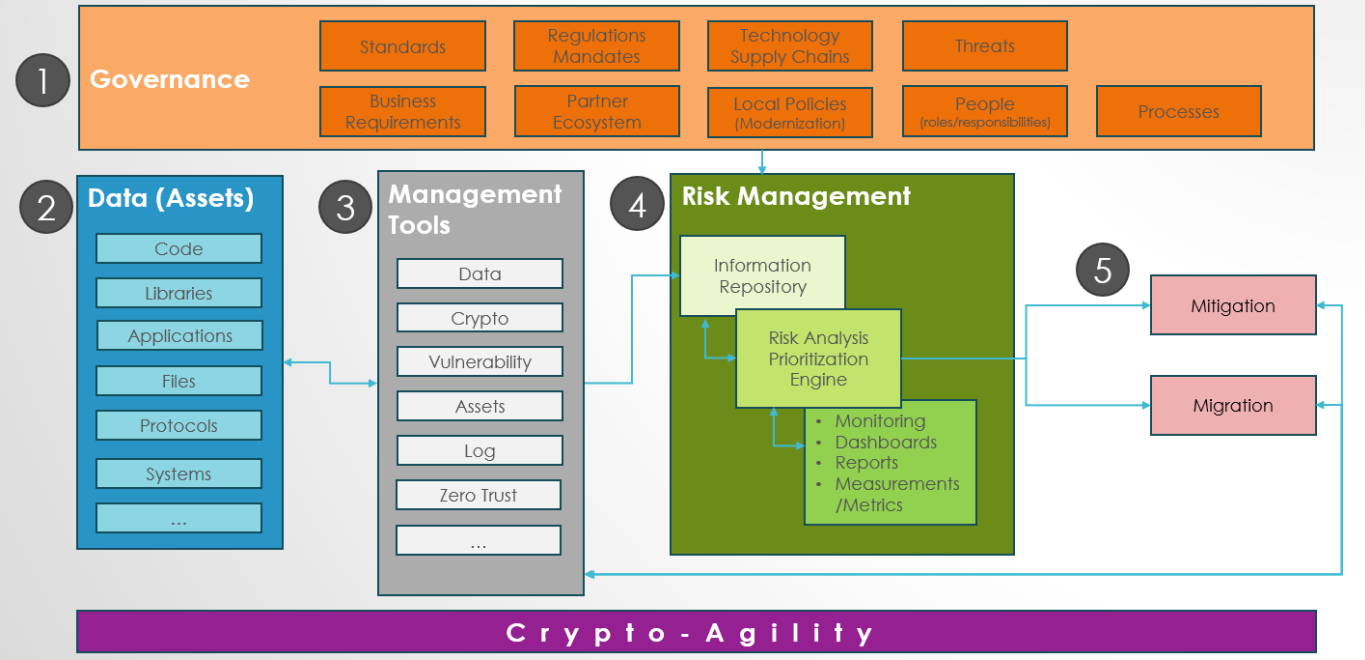
1 understanding the enterprise

2 collect data

3 manage the environment

4 perform risk management

5 perform the migration



Takeaways and learnings from the WG

- Working on a standard is plenty of formal work
  - Many participants with different approaches / goals / motivations
  - Harmonization needs formal processes which are handled in Working Groups and Subgroups

- It is essential to generalize
  - Put away the product glasses and judging and be open to other ideas
  - Especially for techies a challenge ;-)
  - NIST must provide tech neutral guidelines

- If you like to participate plan enough ressources to contribute
  - Even listening and learning from existing solutions and discussions bring new insights and ideas.

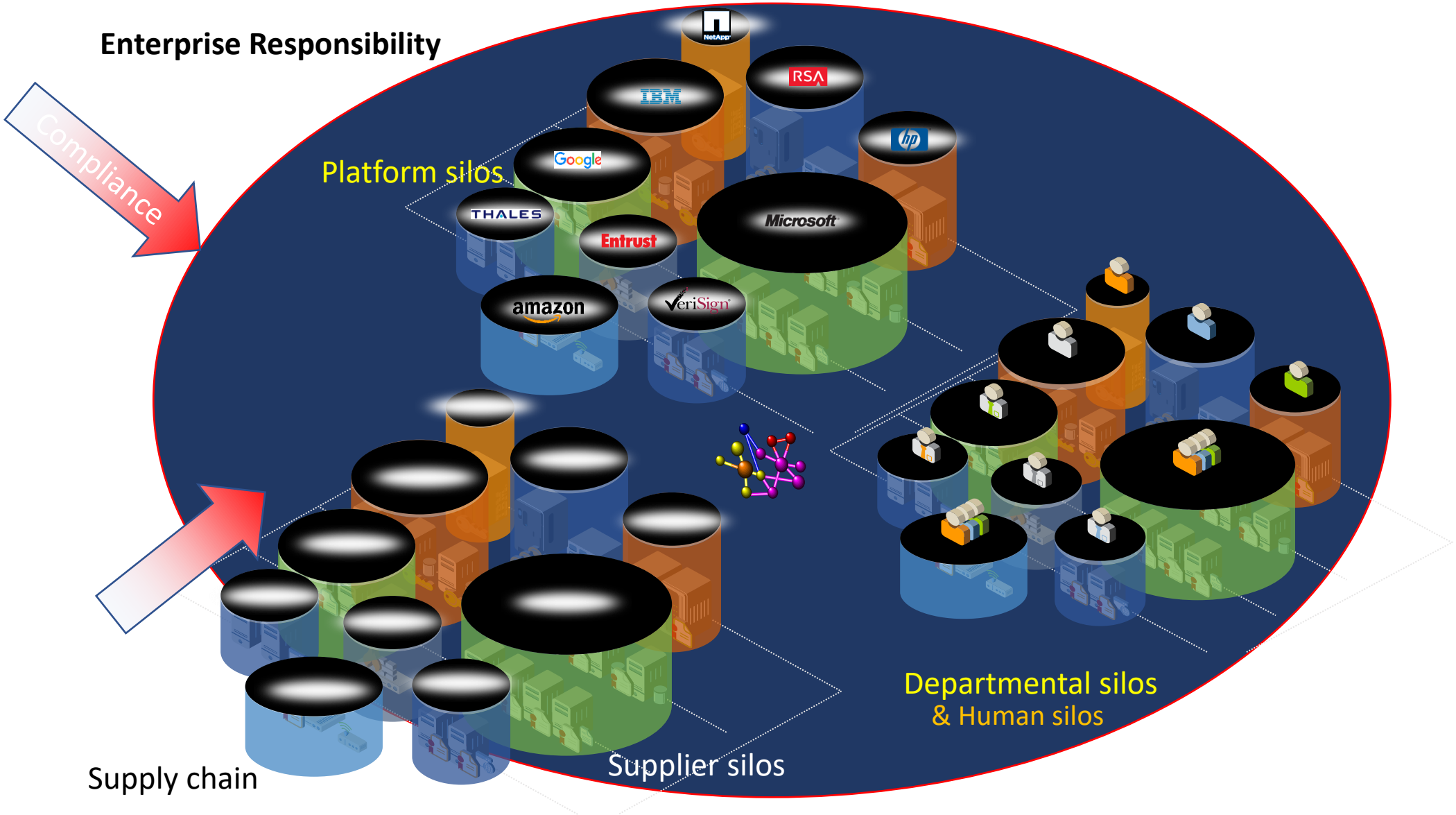
Give aways about stepping into PQM

Data-Warehouse GmbH
Cybersecurity

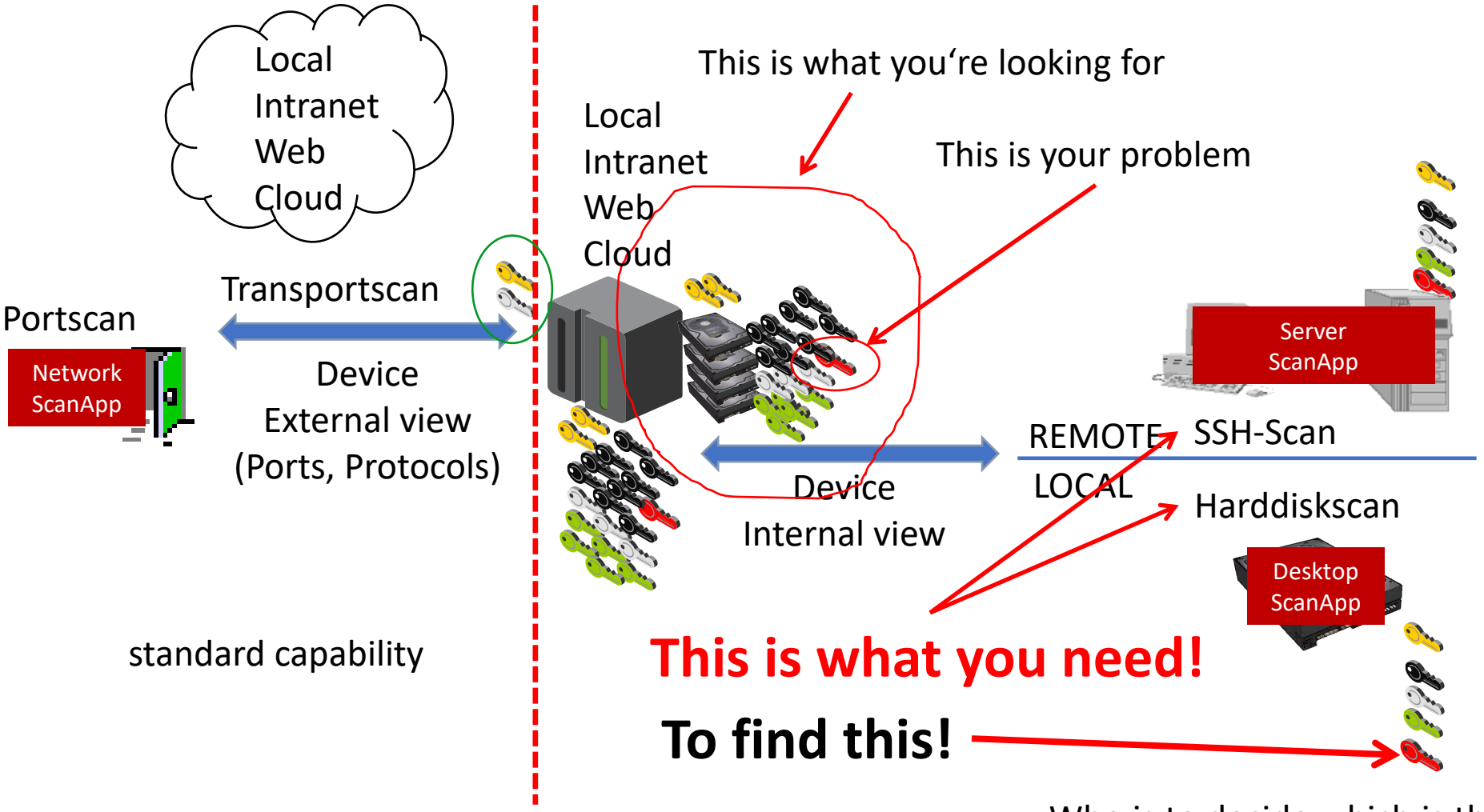
- Visibility - know your infrastructure
- Strategy - know your business traps, compliance and frameworks
- Legality - operate in a legal status and be able to proof it
- Interoperability - be able to interface with as many as possible stakeholders
- Flexibility - be able to adapt to any business and technological change
- Exchangeability - be able to transfer the current solution and data to another platform
- Automation - reduce manual and human interaction to a maximum within compliance

My understanding of the Challenge in trust silos and cryptography to be handled: why visibility?

Data-Warehouse GmbH
Cybersecurity



Visibility challenge: Cryptographic discovery (one IT driven-Device)



Who is to decide which is the red one?

Cryptographic-Lifecycle-Management

Discovery & Visibility

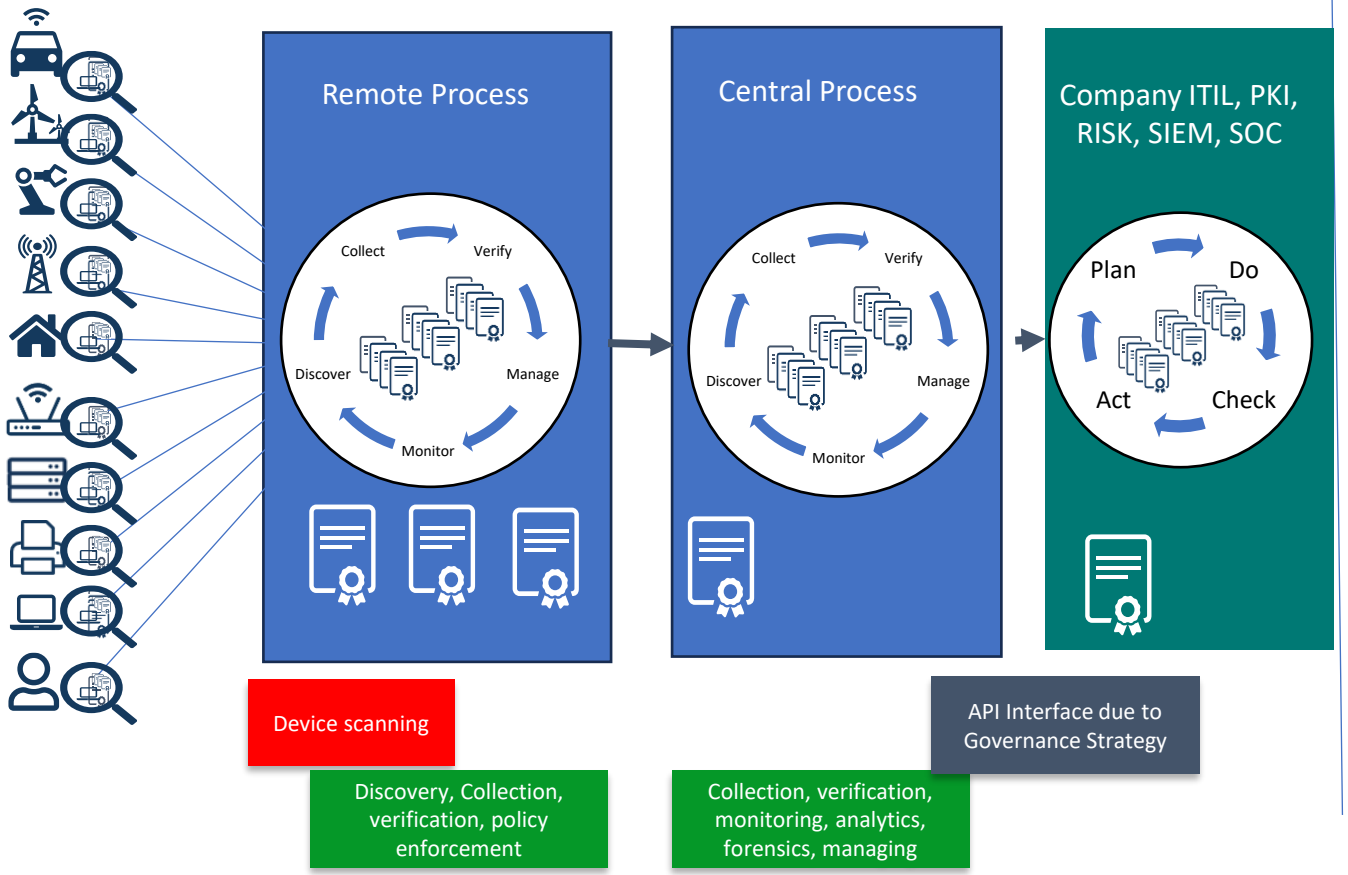
Single lens visibility of PKI with depth and breadth of your enterprise previously not achievable

Remediate & Manage

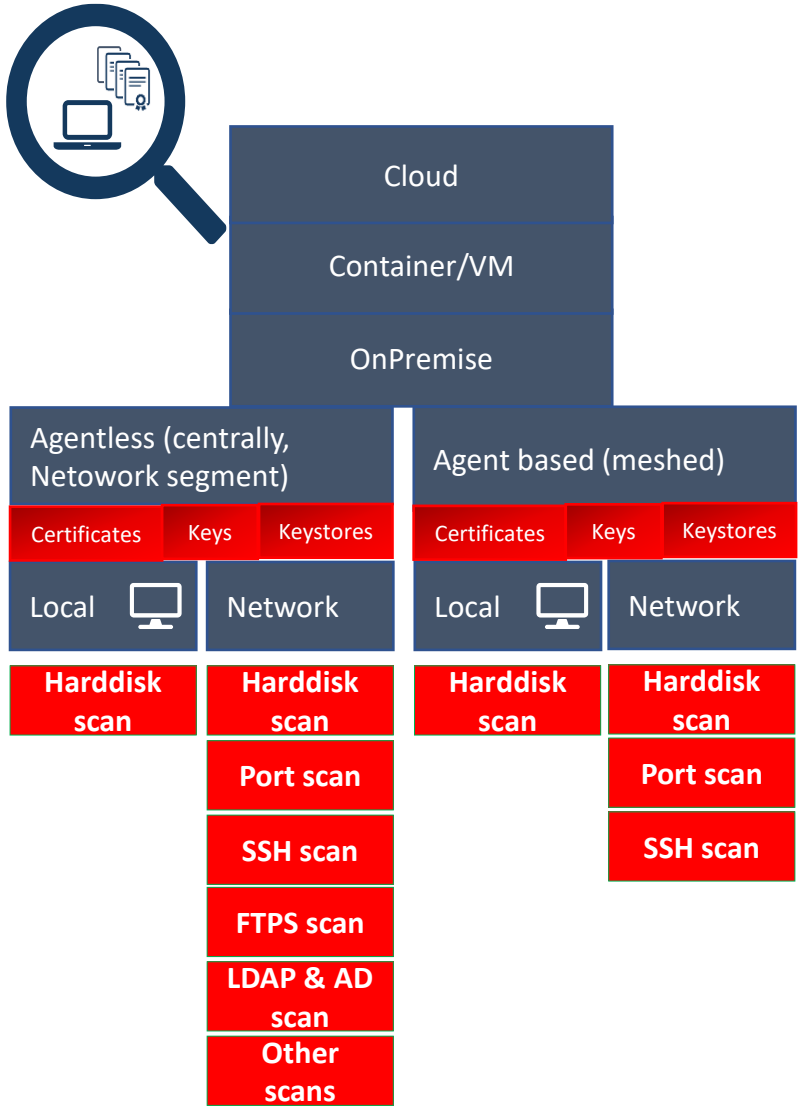
Policy based management drives auto remediation across the PKI lifecycle to support enterprise PKI processes

Monitor & Enforce

Remain compliant to policies and standards to ensure PKI hygiene and best practice



Discovery engines unveils the unknown unknowns to complete your infrastructure understanding



Cryptographic inventory example

Data-Warehouse GmbH
Cybersecurity

Level	Priority	Serial No.	Valid from	Valid until	Revocation date	Algorithm	PubKeyType	PubKeyBits	Subject
pliant	9	4bab0582eb2339866580ed9d3aa27b75ed5eea2	09/16/2020	09/14/2050		SHA256withECDSA	EC	256	ST=California, O=Apple Inc., CN=Apple Accessories Certification Authority - 00000003
cal	9	4bbbe0d8257cd9711a1b57e6bb9c660f	07/06/2012	07/19/2015		SHA1withRSA	RSA	2048	CN="Sun Microsystems, Inc.", OU=Sun Microsystems, OU=Digital ID Class 3 - Microsoft Software Va
ium	9	4bcd77d6899133832fc144f642c9607c501d3d61	01/01/2015	01/01/2035		SHA256withRSA	RSA	2048	CN=xpcshell signed apps test root
cal	9	4be1ae04	04/28/2010	05/02/2020		SHA1withRSA	RSA	1024	CN=OpenVPN Update Root
ium	9	4be92a902784951dc13ac6ce37d230fe	02/24/2021	05/31/2027		SHA256withRSA	RSA	2048	CN=United Trust, O=United SSL Deutschland GmbH, C=DE
pliant	9	4c034bac67184c7faf44084d8296c7b2	11/18/2015	01/19/2038		SHA384withRSA	RSA	4096	CN=Network Solutions RSA Certificate Authority, O=Network Solutions L.L.C., L=Jacksonville, ST=FL
cal	9	4c0e646d	07/28/2010	07/28/2020		SHA1withRSA	RSA	2048	CN=Entrust Class 1 Client CA, OU="(c) 2010 Entrust, Inc.", OU=www.entrust.net/CPS is incorporated
pliant	9	4c1b960191fcabedcda9301a6cd78c3	12/15/2022	12/15/2032		SHA256withRSA	RSA	4096	CN=DigiCert Secure Site OV G2 TLS CN RSA4096 SHA256 2022 CA1, O="DigiCert, Inc.", C=US
ium	9	4c2b439be6d07a60ac676e51c73bd588	01/15/2015	01/15/2025		SHA384withRSA	RSA	2048	CN=TrustSign BR Certification Authority (DV) 2, O=TrustSign Certificadora Dig. & Soluções Seguran
cal	9	4c3	02/03/2014	02/03/2019		SHA1withRSA	RSA	2048	E=KoehlerT@iabg.de, CN=Koehler Tom, O=IABG, ST=Bayern, C=DE
pliant	9	4c462af6dbfbf7804f84c17cfea972b6	10/16/2014	10/16/2032		SHA256withRSA	RSA	4096	CN=TeliaSonera Server CA v2, O=TeliaSonera, C=FI
cal	9	4c50f334ad4d9931	11/14/2024	12/26/2024		SHA256withRSA	RSA	2048	C=US, O=Apple Inc., CN=Timestamp Signer NWK2
ium	9	4c7256a2663e5578e85bd2b6bb70c82	11/02/2017	11/02/2027		SHA256withRSA	RSA	2048	CN=AlwaysOnSSL TLS RSA CA G1, OU=Domain Validated SSL, O=CertCenter AG, C=DE
pliant	9	4c79b59a289c763164f58944d09102de	10/18/2012	12/02/2037		SHA384withECDSA	EC	384	CN=Symantec Class 3 Public Primary Certification Authority - G4, OU=Symantec Trust Network, O=
pliant	9	4c8a631da9638f05a2fb7614ff5ba2cd	02/19/2021	02/13/2045		SHA384withECDSA	EC	384	CN=HARICA Code Signing ECC Root CA 2021, O=Hellenic Academic and Research Institutions CA, C
pliant	9	4c8fc03a854eb98a09b02883c66a3c0	01/15/2021	01/15/2046		SHA384withRSA	RSA	4096	CN=DigiCert Client RSA4096 Root G5, O="DigiCert, Inc.", C=US
ium	9	4ca28f3bf96109b27d9a6197b7051bb	09/18/2024	10/19/2025		SHA256withRSA	RSA	2048	CN=*.statuspage.io
cal	9	4ca81f77d5e33f7	01/07/2016	02/07/2023		SHA256withRSA	RSA	2048	C=US, O=Apple Inc., CN=Apple Mac OS Application Signing
pliant	9	4caaf9cadb636fe01ff74ed85b03869d	01/19/2010	01/19/2038		SHA384withRSA	RSA	4096	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchest
cal	9	4caf150325af0001af00000	03/31/2015	03/31/2020		SHA1withRSA	RSA	1024	CN=iTunes.4CAF150325AF0001AF00000, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf160303af0001af000002	03/04/2016	03/05/2021		SHA1withRSA	RSA	1024	CN=CoreLSKD.4CAF160303AF0001AF000002, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf170210af0001af000001	02/10/2017	02/11/2022		SHA1withRSA	RSA	1024	CN=FPPineBoard.4CAF170210AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf190222af0001af000001	02/23/2019	02/24/2024		SHA1withRSA	RSA	1024	CN=FPStubCoreMediaPEM.4CAF190222AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
h	9	4caf200313af0001af000001	03/13/2020	03/14/2025		SHA1withRSA	RSA	1024	CN=MobileInstallation.4CAF200313AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
h	9	4caf201221af0001af000001	01/05/2021	01/06/2026		SHA1withRSA	RSA	1024	CN=StoreAgentStub.4caf201221af0001af000001, OU=Apple FairPlay, O=Apple Inc., C=US
h	9	4caf210203af0001af000001	02/03/2021	02/04/2026		SHA1withRSA	RSA	1024	CN=iBooks.4CAF210203AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
h	9	4caf220329af0001af000001	03/29/2022	03/30/2027		SHA1withRSA	RSA	1024	CN=iTunes.4CAF220329AF0001AF000001, OU=Apple FairPlay, O=Apple Inc., C=US
cal	9	4caf73421c8e7402	08/17/2006	08/14/2016		SHA1withRSA	RSA	4096	C=TR, O=EBG Bilişim Teknolojileri ve Hizmetleri A.Ş., CN=EBG Elektronik Sertifika Hizmet Sağlayıcıs
h	9	4cc7eaaa983e71d39310f83d3a899192	05/18/1998	08/02/2028		SHA1withRSA	RSA	1024	OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only", OU=Class 1 Pu
ium	9	4cd3f8568ae76c61bb0fe7160cca76d	10/01/2019	10/17/2030		SHA256withRSA	RSA	2048	CN=TIMESTAMP-SHA256-2019-10-15, O="DigiCert, Inc.", C=US
cal	9	4d1c00c5d7e6503b057dd1d5dba3555eac7	08/23/2024	11/21/2024		SHA256withRSA	RSA	2048	CN=cdn.live.ledger.com
pliant	9	4d2d3364d7e1c0da2a46046801adf36	03/24/2020	03/22/2028		SHA256withRSA	RSA	4096	CN=Ionian University TLS RSA SubCA R1, O=Hellenic Academic and Research Institutions CA, C=GR
cal	9	4d4edd7706ef6b3131d00b1c6791d0c1	11/05/2009	12/11/2010		SHA1withRSA	RSA	1024	CN=Adobe Systems Incorporated, OU=Information Systems, OU=Digital ID Class 3 - Microsoft Soft
cal	9	4d5d80c30ad9c700	07/21/2021	09/01/2021		SHA256withRSA	RSA	2048	C=US, O=Apple Inc., CN=Timestamp Signer MA2
cal	9	4d5f2c3408b24c20cd6d507e244dc9ec	02/08/2010	02/08/2020		SHA1withRSA	RSA	2048	CN=Thawte SSL CA, O="Thawte, Inc.", C=US
pliant	9	4d669cec0030600ed07b6fd36cd9900c56f82e09	03/30/2023	03/29/2053		SHA256withECDSA	EC	256	CN=GC01-TERM-CN-P
h	9	4d817ef4	03/17/2011	12/18/2065		SHA1withRSA	RSA	1024	CN=MobileGo, OU=MobileGo Studio, O=MobileGoStudio, L=Shenzhen, ST=Guangdong, C=CN
cal	9	4d819b64	03/10/2011	03/14/2021		SHA1withRSA	RSA	1024	CN=OpenVPN Web CA 2011.03.17 05:25:56 UTC ip-10-203-81-10
pliant	9	4d8247384adf541f88340f4928553224b6c48fe2	06/22/2020	06/22/2030		SHA384withECDSA	EC	384	CN=Cybertrust Japan SureServer CA G8, O="Cybertrust Japan Co., Ltd.", C=JP
pliant	9	4d8a4a1dabf126dac726fc663fab72a9	12/03/2018	01/01/2031		SHA384withECDSA	EC	256	CN=Sectigo ECC Domain Validation Secure Server CA 2, O=Sectigo Limited, L=Salford, ST=Greater M
h	9	4d8ba7b4df9e1153e1c80dee3e6f409a	03/13/2015	12/31/2030		SHA256withRSA	RSA	2048	CN=SHECA Extended Validation SSL CA, O=UniTrust, C=CN
ium	9	4d942c10d43be09409c5812d3a2b064f	11/02/2018	01/01/2031		SHA384withRSA	RSA	2048	CN=Sectigo RSA Client Authentication and Secure Email CA, O=Sectigo Limited, L=Salford, ST=Grea
cal	9	4da54fc7	04/06/2011	04/10/2021		SHA1withRSA	RSA	2048	CN=OpenVPN Update Root 2011.04
cal	9	4da54fc8	04/06/2011	04/10/2021		SHA1withRSA	RSA	2048	CN=OpenVPN Script Root 2011.04
cal	9	4da56a9b	04/06/2011	04/10/2021		SHA1withRSA	RSA	1024	CN=JY Private Root
pliant	9	4dd1c6d49937935c7c662428d193cf6	07/30/2014	07/30/2029		SHA384withRSA	RSA	4096	CN=NCC Group Secure Server CA G4, O=NCC Group, C=US
pliant	9	4dd7ecd8bfe3555392fa387b478e566f	03/14/2019	03/12/2027		SHA256withRSA	RSA	4096	CN=Ecclesiastical Academy of Vella SSL RSA SubCA R2, O=University Ecclesiastical Academy of Vell
ium	9	4ddcbc4d8baa006b1f321b00894f42ee	04/29/2015	04/29/2025		SHA384withRSA	RSA	2048	CN=Western Digital Technologies Certification Authority, O=Western Digital Technologies, L=Irvin
pliant	9	4df7309184c7b632b600b5d4a045e959	04/20/2022	04/20/2032		SHA384withECDSA	EC	256	CN=TrustAsia ECC OV TLS CA G3, O="TrustAsia Technologies, Inc.", C=CN

Like numbers? Mac Osx Highscore: currently 256.000, MS Windows 10: 369.000 Certs&Keys on one device

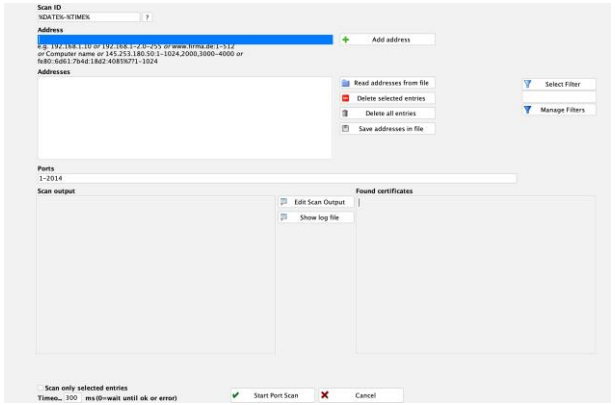
Risk Assessment option example

Data-Warehouse GmbH
Cybersecurity

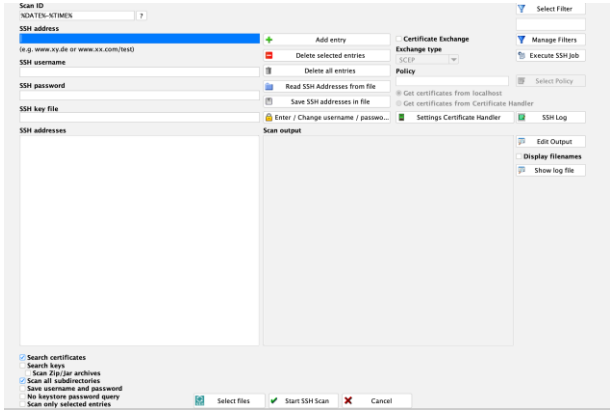
How to find them?

Data-Warehouse GmbH
Cybersecurity

Ports / Networks / Segments



Remote Server



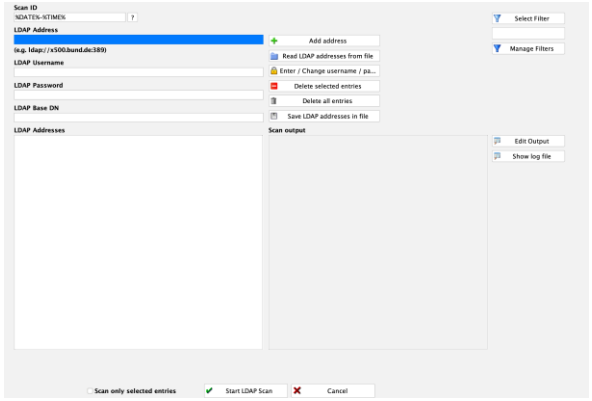
Questions asked:
Do you need agents?

Manually?

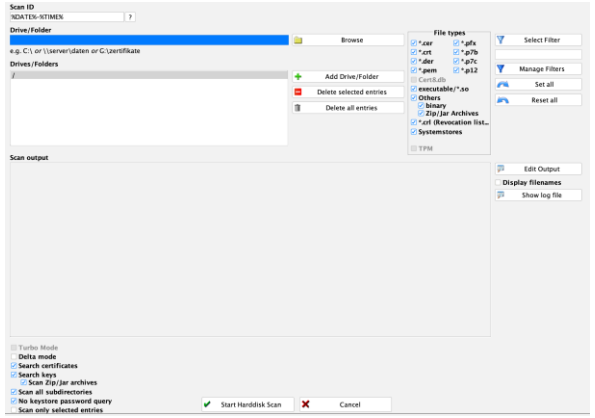
Both?

Automated?

Directories



Local

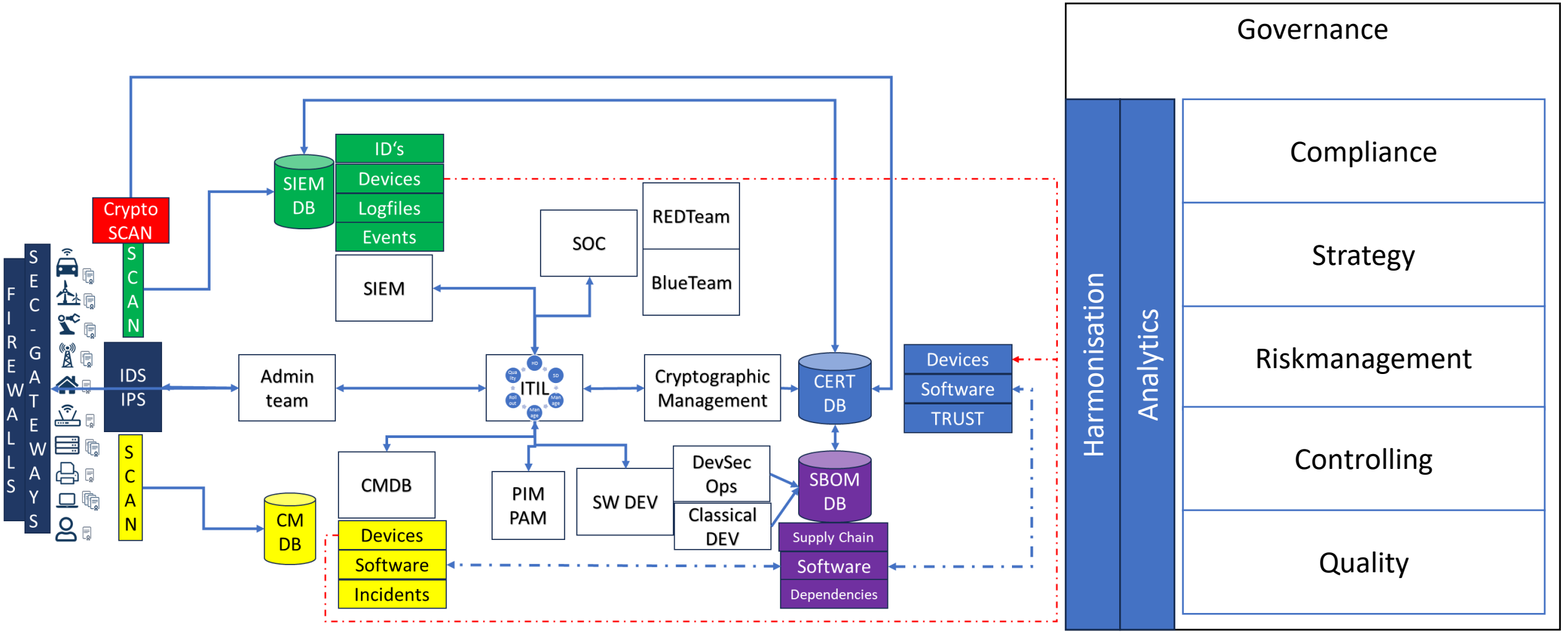


Do you ask the right questions?

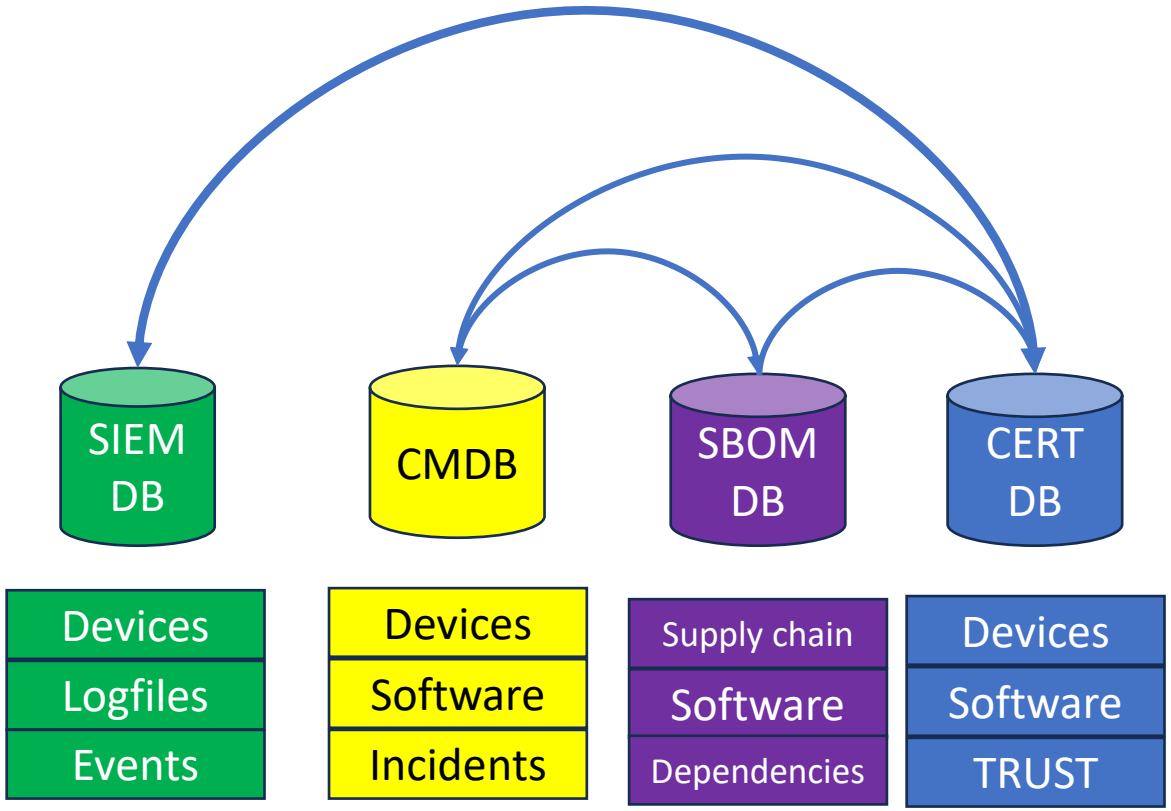
My one would be:
Can you allow to miss information?
How can we integrate it with minimal effords?
Can we support all our important processes?

Quantum migration ready Governance

Data-Warehouse GmbH
Cybersecurity



How does Cert Discovery interface into this world and what‘s new?




```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data
[ <!ELEMENT data (certificate+)>
  <!ELEMENT certificate (idno, certno, scandate, scantime,
origin, scanid, ipv4, ipv6, hostname, macaddress,
portpath, filename, serialno, validfrom, validuntil,
revocationdate, algorithm, pubkeytype, pubkeybits,
subject, issuer, ca, pathlength, selfsigned, fileformat,
alias, ocsp, trusted, subject_alternativenames,
thumbprint_sha1, thumbprint_sha256, certificate_pem)>
  <!ELEMENT idno (#PCDATA)>
  <!ELEMENT certno (#PCDATA)>
  <!ELEMENT scandate (#PCDATA)>
  <!ELEMENT scantime (#PCDATA)>
  <!ELEMENT origin (#PCDATA)>
  <!ELEMENT scanid (#PCDATA)>
  <!ELEMENT ipv4 (#PCDATA)>
  <!ELEMENT ipv6 (#PCDATA)>
```

Solutions necessary and adressed

Cryptographic inventory supports:

- CBOM
  - Building a Cryptrographic Bill of Material and consolidate it in enterprise context
- SBOM
  - Building a Software Bill of Material and consolidate it in enterprise context
- Crypto agility
  - Changing from one cryptographic provider (CA) to another with maximum automation
- Risk identification and monitoring
  - Identifying risk components or suppliers in the enterprise context

- Additional services like: Investigate cryptographic security
  - Eg. Keystore security, private and public key handling

Real world problems in enterprises

Data-Warehouse GmbH
Cybersecurity

- Computer Museum support
  - Support and include also older hardware/software into the inventory
- Information superiority
  - Define the level of management and independency of operation
- Automate and enable manual or identify not performed tasks
  - Automate certificate management (CLM) / reduce outages / enhance business continuity / react faster

Thanks for your attention

Dr. Alexander Löw (Loew)
Data-Warehouse GmbH
Ottobrunn/Germany
https://datawh.info/en/pcert

GE: +49 170 850 5050

PCert.com
US based company (MD) in Q1/2025
Howard County (MD), USA
offices:
Sarasota (FL), USA
Santa Monica (CA), USA
US: +1 646 821 7053