PCert® Strategic: Prepare the next level of digitalization

A business incident caused by certificates generates around $ 3-5 million in damages (source Ponemon & Gartner). An enterprise typically experiences 3-5 incidents per year.

**Imagine you could just prevent one!** Or all of them?

Is your company running into incompliance? Like to verify?

Summary and USP: You are going digital, but are you secure? Unveil your unknown unknowns in your digital trust anchors is the comprehensive challenge of C-Suites today and business purpose of our product suite PCert® by Data-Warehouse with more than 25 years of research and 10 years of product experience in the field of cryptography handling. Helping your enterprise, vendors and customers in building a full scope automated cryptographic inventory enables to evolve to the next level in security with a transparent and minimal invasive integration to **enhance your existing** product and network structure with maximum automation and with new **capabilities**: **prepare, migrate to Post Quantum** Age (crypto agility), **verify and audit your company security processes, identify risks, products and supply chains (SBOM), ensure your product compliance and automate your management processes** such as handling of certificates or information exchange within your operations and business continuity team plus **reduce workload of your administration teams through automation**, **regardless of the use or the age of your technology infrastructure** and operational concept.

Your responsibility and challenge: Get rid of your cryptographic silos, enable a cryptographic inventory and build your SBOM

PCert® holistic approach makes it possible to investigate, discover, assess, automate and manage a very broad range of IT-trust relations regardless of whether they involve web services, products or devices. The PCert® approach is the identification of any certificate, key (like private, public, symmetric, ssh, pgp), keystore in any device for identifying vulnerabilities, weaknesses, human or systematic mistakes in order to **avoid infrastructure, program and product problems, prepare or perform transformation to new technologies (Post quantum is already on the horizon)**. Your

benefits with PCert® are not only bringing full transparency into your technical environment and Public Key Infrastructure (PKI), it also enhances your Cybersecurity as well as including your supply chain and proof of compliance against several standards (SOX, ISO,Fedramp, NIS 2 and more..).
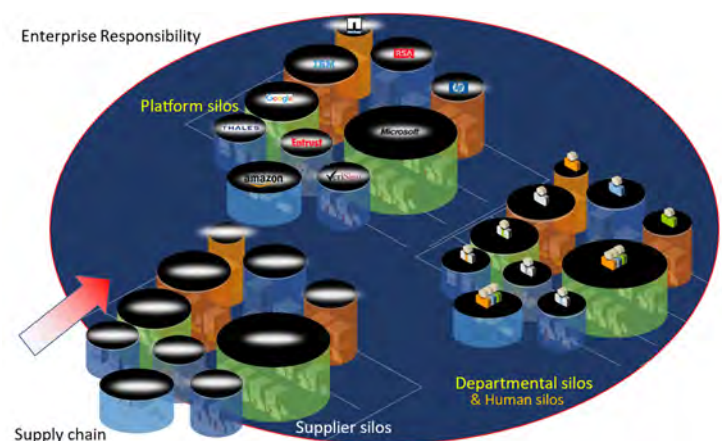
Your responsibility and challenge: Integrate the new compliance requirements into your Governance


Next level Governance
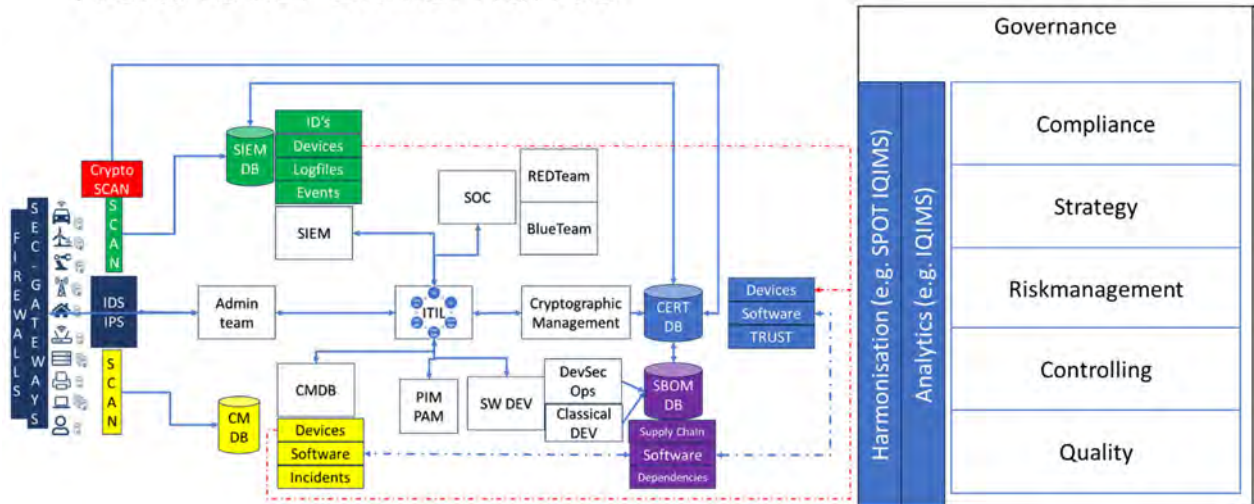
This also allows to verify the chains of trust, supplier and vendor security, supply chains and to identify risks when using products in your infrastructure.

Starting from sensors up to complex products, regardless if newest state of the art or legacy, if on premise or Cloud or hybrid, if your products, your infrastructure or your customers environments contain a seamless integration into your company processes, they enhance your strategic portfolio.

How does Cert Discovery interface into this world and what's new?
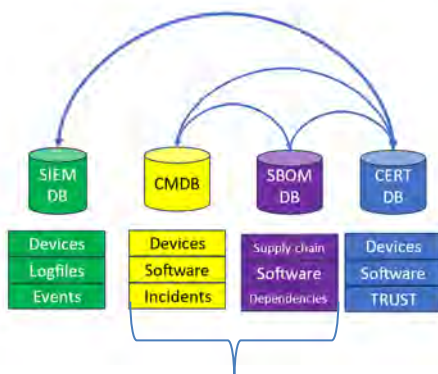
```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE data
[ <!ELEMENT data (certificate+)>
  <!ELEMENT certificate (idno, certno, scandate, scantime,
  origin, scanid, ipv4, ipv6, hostname, macaddress,
  portpath, filename, serialno, validfrom, validuntil,
  revocationdate, algorithm, pubkeytype, 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)>
```

PCert® with its flexible API's enables seamless integration into the customer's infrastructure, regardless of the interface type like XML, JSON, REST, SOAP, CSV and ensures the best possible information exchange and maximum use inside the process. This is also valid for the software itself as it needs minimum resources with minimum security exposure to prevent new vulnerabilities or integration topics. Regardless if on premise, Cloud or hybrid.

Book your independent PCert® test in the Post Quantum Migration Lab at
or any trusted Data-Warehouse partner
or talk to our experts to learn more about the strategic challenges