PCI DSS v4.0 Cryptographic Activity Monitoring

Case study of how a Swedish bank perform PCI DSS v4.0 monitoring of cryptographic cipher suites & protocols in use

PCI Security Standards Council

Vui Huang Tea

Swedbank, Sweden

Swedbank

PCI DSS v4.0: Requirement 12

Support Info Security with Organizational Policies & Programs

- 12.3 Risks to the cardholder data environment are formally identified, evaluated & managed.
  - 12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following:
    - An up-to-date inventory of all cryptographic cipher suites & protocols in use, including purpose & where used.

- Protocols and encryption strengths may quickly change or be deprecated due to identification of vulnerabilities or design flaws. In order to support current and future data security needs, entities need to know where cryptography is used and understand how they would be able to respond rapidly to changes impacting the strength of their cryptographic implementations.

PCI DSS v4.0: Requirement 12.3.3

An up-to-date inventory of all cryptographic cipher suites & protocols in use…

- The defined approach testing procedures in 12.3.3 is:
  - *Examine documentation for cryptographic suites and protocols in use and interview personnel to verify the documentation and review is in accordance with all elements specified in this requirement.*
- However, it is challenging to get cryptographic info from software vendors, and time-consuming to document & maintain an up-to-date inventory. For example, there may be half a dozen instances of cryptography in 20,000+ lines of code.
- There is also a risk of inaccurate or incomplete data:

	Algorithm	Key Size	Purpose
1	RSA	?	?
2	?	512	?
3	?	?	Encrypt

PCI Security Standards Council

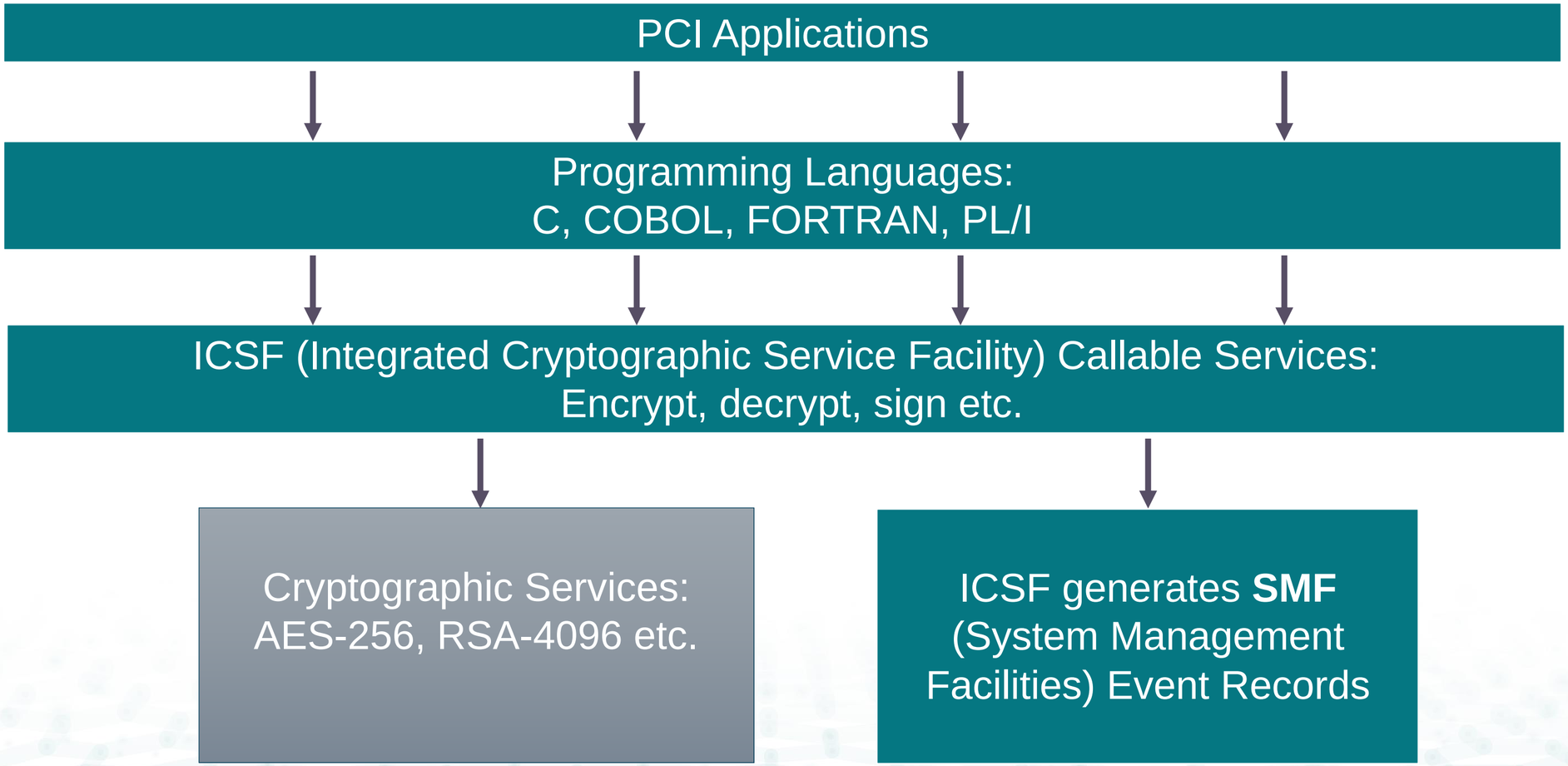
PCI DSS v4.0: Requirement 12.3.3

An up-to-date inventory of all cryptographic cipher suites & protocols in use…

- Another approach is to track the cryptographic usage & activities from the logs.
- On Mainframes, there is an API (Application Programming Interfaces) that works with hardware cryptographic features to provide secure, high-speed cryptographic services. This works as a single gateway interface by which the PCI applications (C, COBOL, FORTRAN, PL/I & Assembler) request the cryptographic services.

Cryptographic Usage on Mainframes

PCI applications use a high-level API to access cryptographic functions



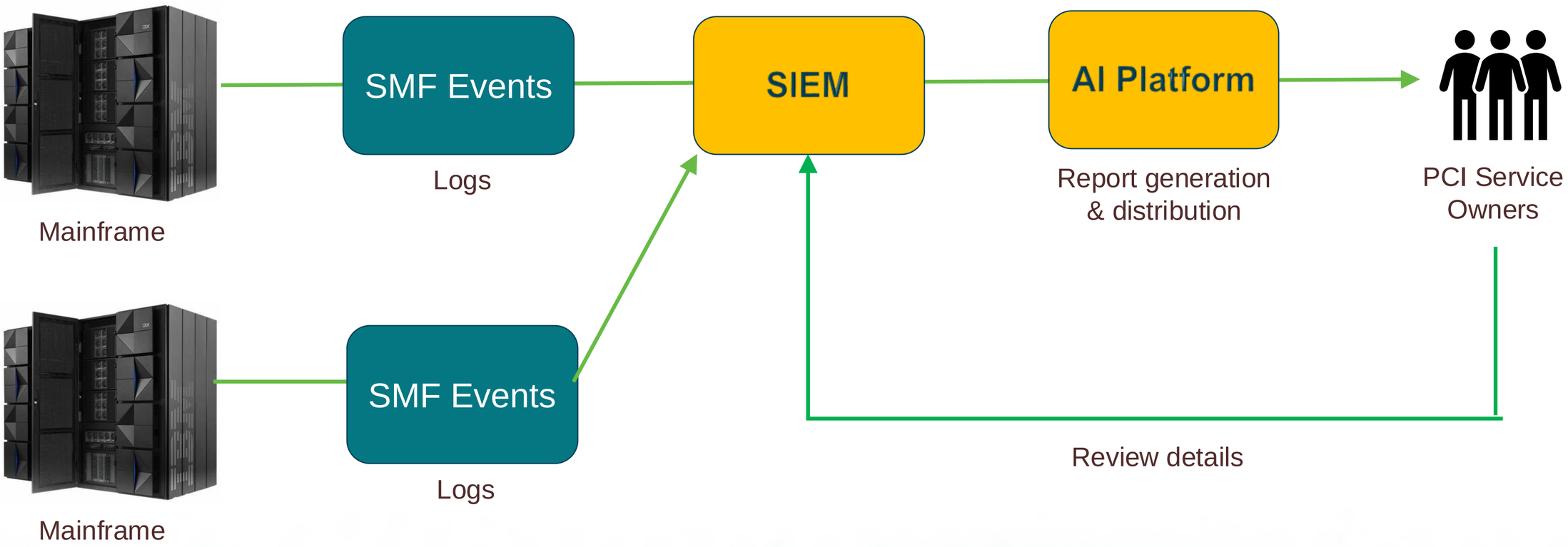
PCI Security Standards Council®

SIEM

Security Information & Event Management

- SIEM tools collect, aggregate, and analyze volumes of data from an organization’s applications, servers, and users in real-time so security teams can detect and block attacks.
- One of SIEM’s core function is log management. They gather vast amounts of data in one place and organizes it. Thus, we use the SIEM tool to collect and aggregate the Cryptographic API logs from all PCI-related Mainframes.
- Then we created custom notebooks & workbooks on an AI platform to analyze the SIEM logs for cryptographic usage to generate PCI DSS v4.0 compliance reports.

Cryptographic Activity Monitoring Overview



Machine Learning (ML) Pipeline Workflow

For orchestration & coordination

- A ML pipeline is an independently executable workflow of a complete machine learning task. Subtasks are encapsulated as a series of steps within the pipeline, and the pipeline service automatically orchestrates all the dependencies between pipeline steps.
- A well-defined ML pipeline can abstract a complex process into a multiple steps workflow, mapping each step to a specific task such that each team can work independently. All these steps built by different users are finally integrated into one workflow through the pipeline definition. The pipeline is a collaboration tool for everyone in the project.
- We deployed a ML pipeline that executes every week, each time generating the latest compliance report and then uploading it to a Cloud storage.

Automated Workflow

For email

- Automated workflow is used to manages the apps, data, services, and systems.
  It simplifies the connection of legacy, modern, and cutting-edge systems across hybrid cloud / on premises environments.
- Automated workflow is used to automate the scheduling & sending of email notifications when a new PCI DSS v4.0 report is generated, together with a link to the Cloud storage
- The PCI service owners can view the latest and past compliance reports, as well as refer to the SIEM for detailed log entries.

Sample Log Extraction Result

From Mainframes

- Cryptographic agility refers to the ability to monitor and manage the encryption and related verification technologies deployed across an organization.
- The finding on the right also shows how frequent the cryptographic operation is used in a given period.

```
Protocols / encryption strengths in-use:

897 x RSA-4096  PKA Key Import
383 x RSA-4096  PKCS #11 Private Key Structure Sign
228 x RSA-2048  PKA Key Generate
113 x RSA-2048  PKA Decrypt
 87 x RSA-2048  PKA Public Key Extract
 43 x RSA-2048  PKCS #11 Public Key Structure Verify
 21 x RSA-2048  PKCS #11 Private Key Structure Sign
```

PCI Security Standards Council®

Sample Log Extraction Result

From Mainframes

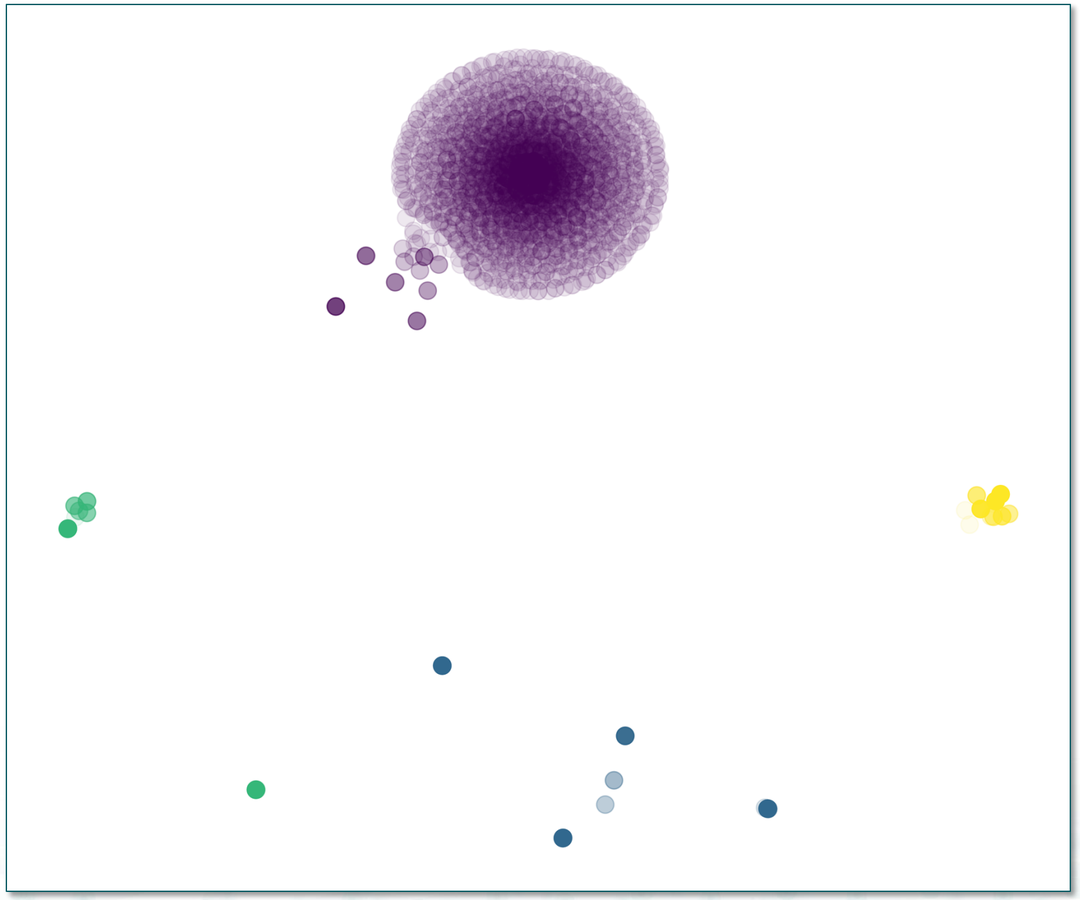
- Cryptographic agility is important to ensure an alternative to the original cryptographic primitive is available, with plans to upgrade to the alternative without significant change to system infrastructure.
- For example, if the entity is aware of when protocols or algorithms will be deprecated by standards bodies, it can make proactive plans to upgrade before the deprecation is impactful to operations.

Protocols / encryption strengths deprecated:

```
461 x DES-128  Import encrypted DES key
386 x DES-128  Encipher
290 x DES-128  Decipher
226 x DES-128  Unique Key Derive
117 x DES-64   Import encrypted DES key
 98 x RSA-512  PKA Encrypt
 86 x DES-64   MAC Generate
 74 x DES-64   MAC Verify
 73 x DES-128  Key Generate
 52 x DES-64   Encipher
 42 x DES-128  PKCS #11 Token Record
 32 x DES-128  Encrypted PIN Verify
```

Artificial Intelligence (AI)

Visualization of cryptographic cipher suites & protocols in use



- Clustering is an AI algorithm that organizes & classifies different data into clusters based on similarities. It can use just one or all features in the data (e.g., cipher algorithm, key size, purpose, frequency etc.).
- The visualization can be used to monitor ongoing cryptographic usage & **anomaly detection** by detecting which crypto activity are not contained within a cluster or are only weakly associated with a cluster

PCI Security Standards Council®

Security Standards Council®