TeleManagement Forum TMF528
Principles for Security Compliance Audit Automation (SCA)
Who to achieve compliance without increasing risk?

TROOPERS 2012, Heidelberg, March 2012.

Life is for sharing.

Management Summary

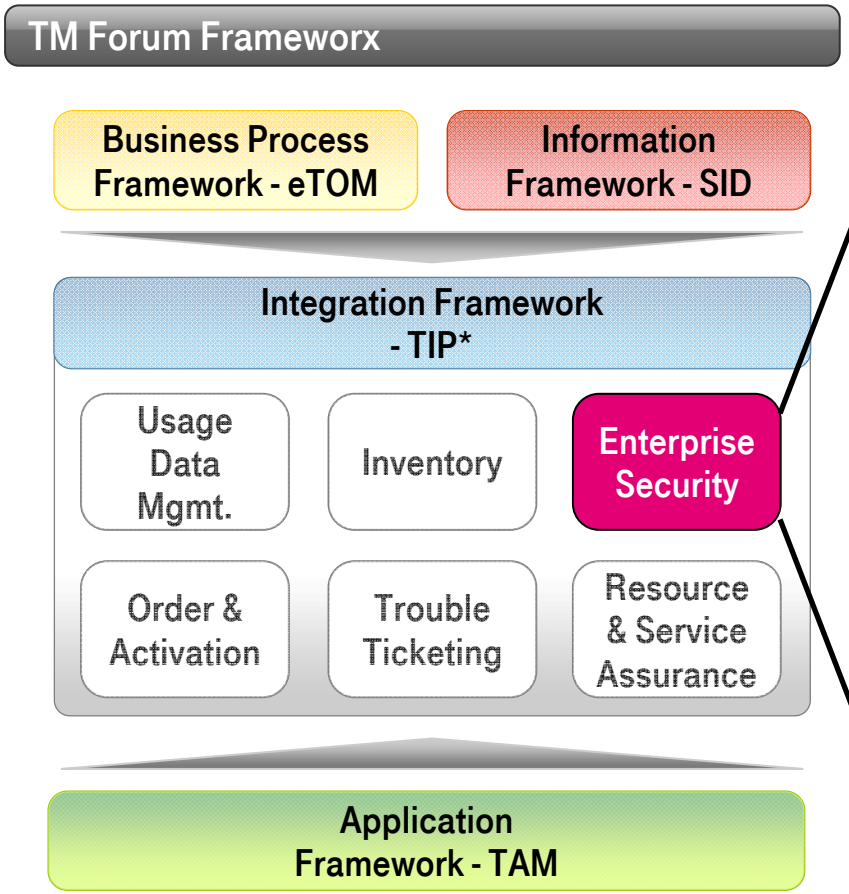
- The Enterprise Security team is part of the TM Forum Integration Program (TIP) and is currently working on three TMF standards: Operator User Management (OUM), Single Sign-On (SSO) and Security Compliance Audit Automation (SCA).
- This document describes the DTAG contribution to Security Compliance Audit Automation.
- The SCA standard is currently under development. It describes data, data formats and transfer protocols required to audit the compliance to security policies.
- Currently security-related log data is determined, queried and transferred in a proprietary, service provider- and vendor-specific way. Existing data formats are generally proprietary and not suitable for easy security analysis. The SCA standard is meant for solving these issues.
- Currently the standardization work focuses on security log data. This appears to be not sufficient. Consequently this contribution suggest to broaden the SCA scope for config and telemetry data.
- In addition two fundamental interface characteristics are proposed:
  - The SCA interface should use a central SCA repository – all managed elements implementing SCA must actively push the information to the SCA Management System (southbound).
  - To SCA Management System provides view based access to a unique information repository for management systems (northbound)– without direct interaction to the production infrastructure.

Overview on TeleManagement Forum.

Short intro

- Website: http://www.tmforum.org Logo: tmforum
- TeleManagement Forum is a global, non-profit industry association of service providers and their suppliers
- focused on simplifying the complexity of running a service provider's business.
- the Forum serves as a unifying force, enabling more than 850 companies to solve critical business issues through access to a wealth of knowledge, intellectual capital and standards.
- founded as OSI/Network Management Forum in 1988 by eight companies (AT&T, HP, British Telecom, ..)
- DTAG's NGSSM is based on TMF's NGOSS
- TMF published the Business Process Framework eTOM (enhanced Telecom Operations Map) –(good/best practice standard (like ITIL or (ISO (more generic))))
- TMF providing catalysts (PoCs), best practices, case studies, standards and interfaces spec. (TMFxxx) within the TMF Collaboration Program

The Security Compliance Audit Automation (SCA) interface is currently specified by the Enterprise Security team (ESEC)



Enterprise Security team (ESEC)

Security Compliance Audit Automation (SCA)

- Standardize data, message formats and transfer mechanisms for automated security compliance verification
- Business Agreement (BA) TMF528 currently in development, TMF619 (IA) and TMF900 (IIS) will follow

Single Sign-On (SSO)

- Replace “multi sign-on/off” by "single sign-on/off“ mechanisms
- Until now BA TMF523 released.

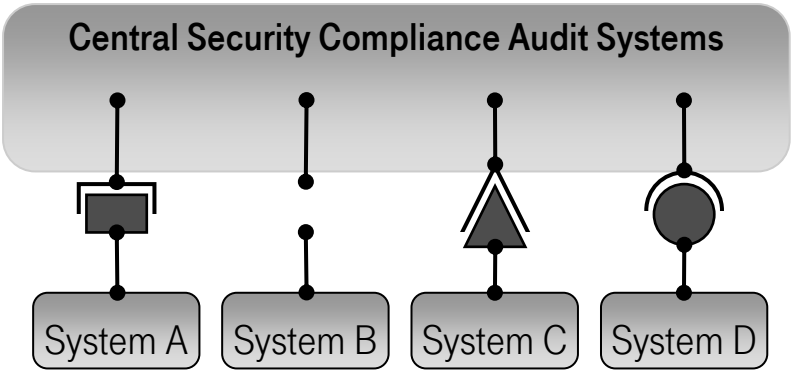
Operator User Management (OUM)

- Interoperable, consistent and secure management of OSS operators' credentials and entitlements, reducing integration and operational costs
- Centralized OSS operator provisioning and support for specific OSS operator entitlements based on local situation
- Consists of BA TMF520, IIS TMF615, IA TMF873

*only interface integration & delivery teams are listed

The importance of standardized log data for security analysis is commonly understood.

As-is Situation



- Proprietary log interfaces and log message formats, not suitable for easy security analysis.
- Supplier depended semantic and syntax
- In case specifications exist, they are independent and overlapping
- Log data only partially transferred if at all

Business problem (Log data)

- The ability to audit the compliance of OSS systems and their users to security directives is key to the security and proper operation of OSS system
- Current attempts to verify the compliance to security directives trigger a cumbersome data interpreting process.
- Currently security-related log data is usually determined, queried and transferred in a proprietary, service provider- and vendor-specific way.

To answer all necessary security compliance questions, log data alone appears not to be sufficient.

Security questions from practical experience

- Which bash-processes out there listens on TCP port 2 (rootkit)?
- Which SSH daemons have password authentication activated?
- Which Apache servers are still in version 2.2.3?
- Which systems run with a printer daemon?
- Does a process cause 100% processor load?
- Which Apache servers use a workaround for CVE-2011-3192? (rewrite rule active?)
- Is anywhere a weak SSH public key installed (s. CVE-2008-0166)?
- ...

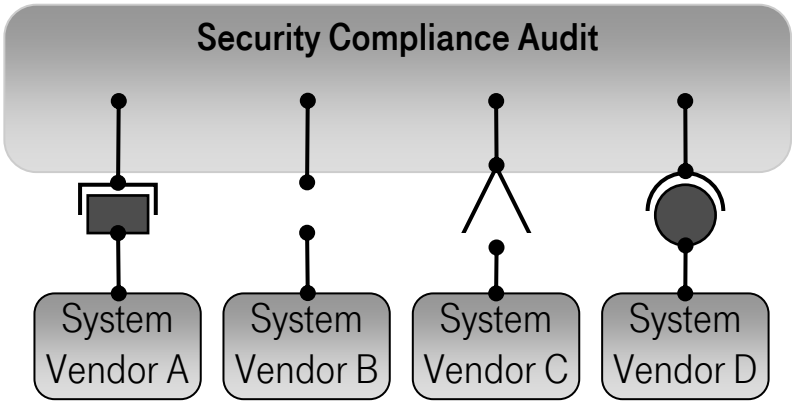
There is no efficient and secure way for continues collection of infrastructure information covering config, telemetry.

Business problem (Config and Telemetry data)

- Service Providers have to **evaluate and verify the compliance of their infrastructure** and services to corporate security directives and legal guidelines.
- Compliance verification needs config data and telemetry **data centralized at hand without manual, time-consuming operator activity**
- **Current attempts** to verify the compliance to security directives trigger a **cumbersome data gathering process**.
- **Often powerful access rights** and credentials are assigned to the OSS System **only to collect data**.

Solving the business problem leads to significant security, efficiency and quality gains

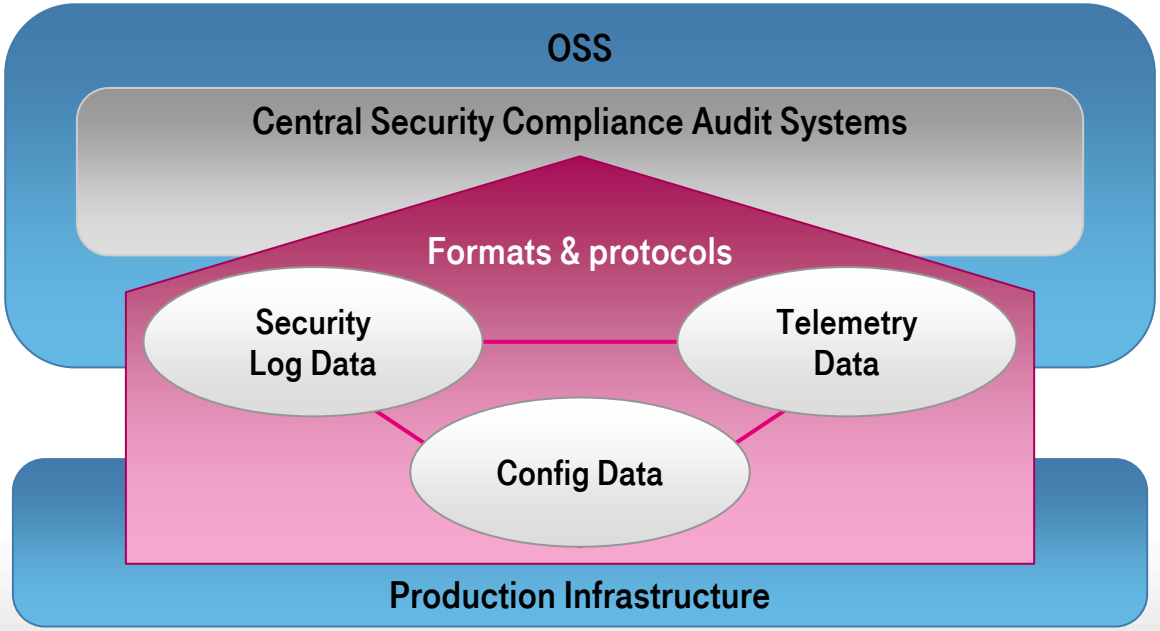
...because of lacking or proprietary interfaces



- Required data only partially transferred if at all
- Interface adaptation to suite our needs are costly
- In case solutions exist, they are vendor specific
- Support of vendor is normally lost when deploying 3rd party (compliance) solutions on telco systems (much more easy on IT systems)

Scope of SCA specification

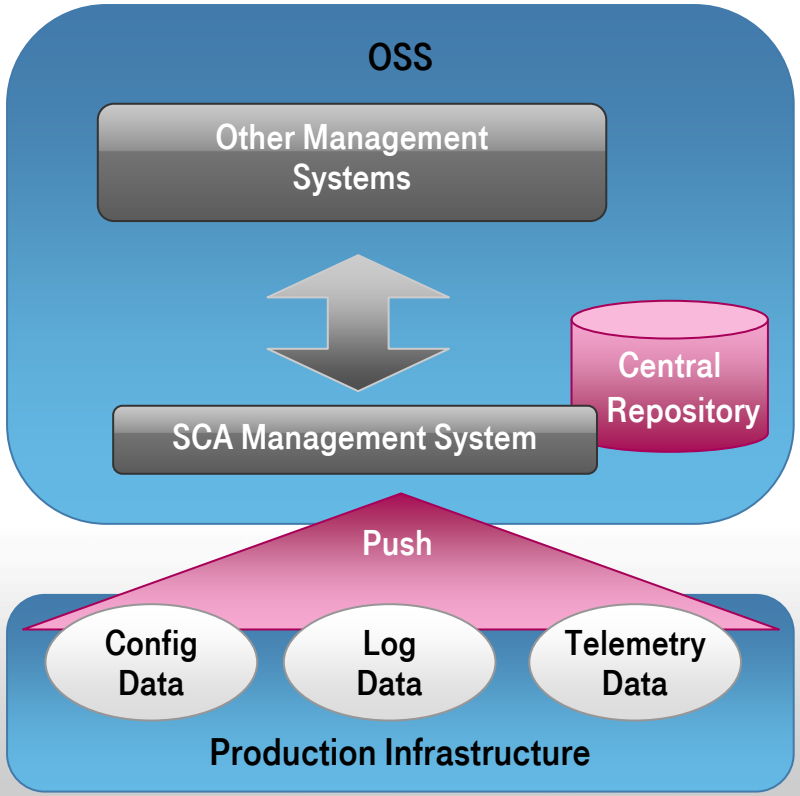
Proposed scope of SCA standardization



- Security Log Data - Authentication-Log, Application-Log.
- Telemetry Data - observed activity - process table, open files and network listen sockets.
- Config Data – sshd.conf, "/etc/passwd", apache.conf.

The full picture includes a central repository and a message push mechanism for a simple and robust implementation.

SCA full scope

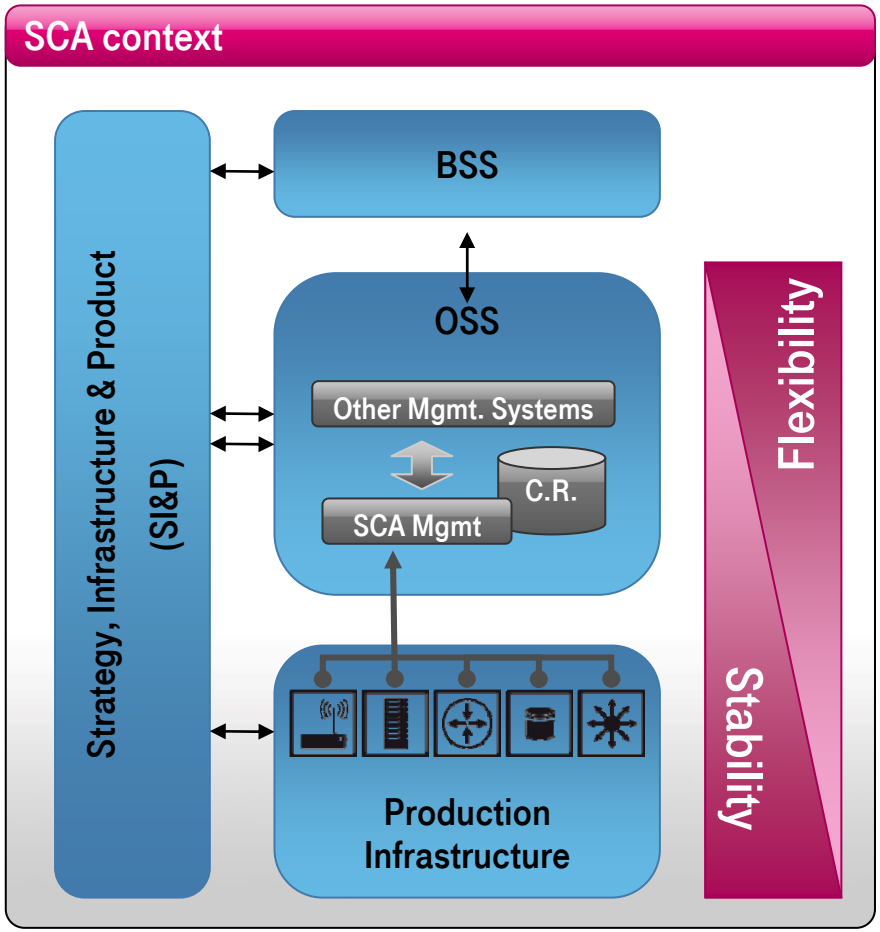


SCA basic approach

- The Devices will push the standardized log-, config- and telemetry data to the SCA Management System (Main scope: SCA as can opener for “closed devices”)
- The SCA Management System stores the collected data in the Central Repository
- The SCA Management System provides Views on the Central Repository to other Management Systems
- Other Management Systems access their data through views on the Central Repository and conduct security analysis.

- *Scope Phase 1: interface Device-to-SCA Management System (SCA-DI)*
- *Scope Phase 2: SCA Management System -to- Management Systems (SCA-MI)*

The central repository and message push mechanism enable management system flexibility and production stability.



Management Flexibility

- Data mining on read only database (network telemetry data, config data, log data)
- Flexibility in network management while production stays stable
- Flexible policy definition without change to production
- Management functionality only in management layer

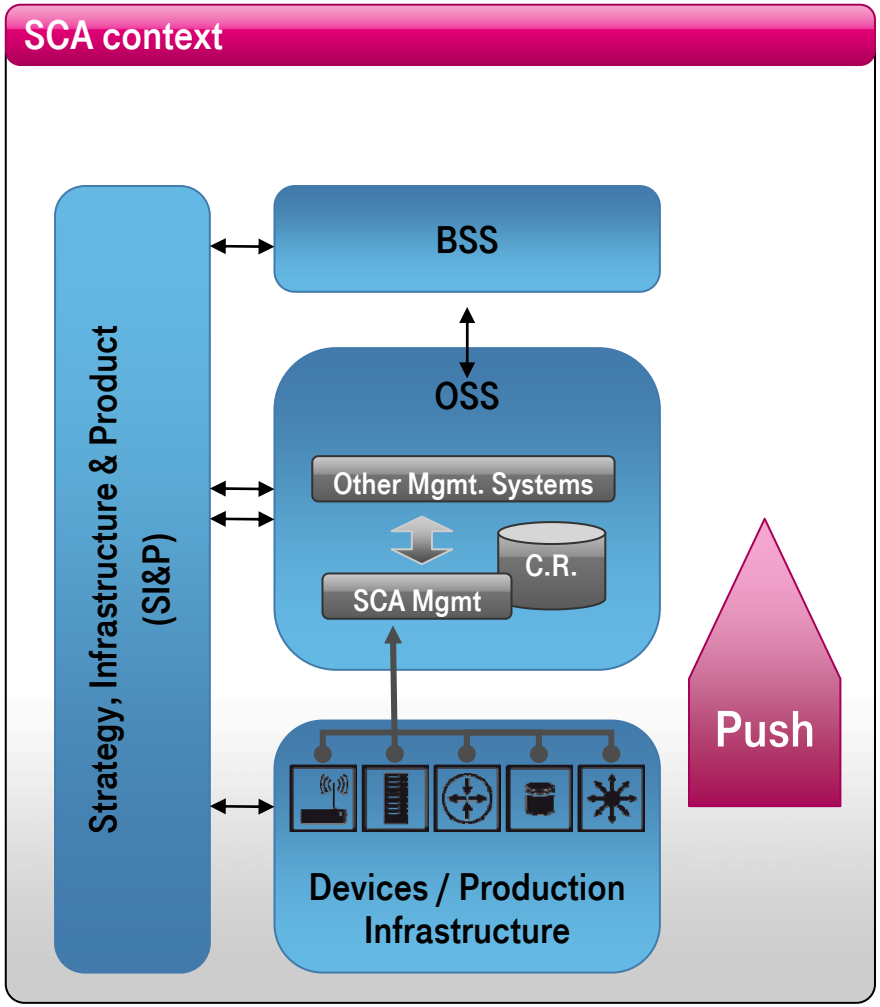
+

Production Stability

- Interactive scripts on production are avoided
- No additional attack vectors without interactive scripts
- Robust and simple pre-define standardized reports
- Data collection implemented, tested and approved by vendor
- All relevant data is delivered to management system

= **Best of both worlds**

The message push mechanism eliminates major security threats.



Eliminated security threats

- No risk, if central system is compromised
- No clear text passwords stored in the OSS for M2M communications
- No special users entitlements
- Firewall-friendly: Connection established by the Devices
- No network agents or shell logins on Devices
- No 3rd party software on Devices
- Vendor approved data collection

+

Simplicity

- No Customization & low Configuration
- Standardized message format
- Harmonized interfaces
- Supplier has implementation freedom

Overview of SCA Interfaces.

Management Systems

- Security Compliance Audit System, Patch-Management, CERT, License Mgmt, Vendor Support, ...

SCA-DP (Data Provider)

- Provides views on/ sends views of collected data
- Blacklisting / filter on critical or restricted information
- Access control

SCA-CR (Central Repository)

- Implementation e.g. file system / SVN / SQL
- Storage for
  - Log Data (e.g. auth.log, application-log), Config Data (e.g. apache.conf), Network & system telemetry data (observed activity) system status data (e.g. process table, netstat, lsof)
- Revision / history / house keeping

SCA-DR (Data Receiver)

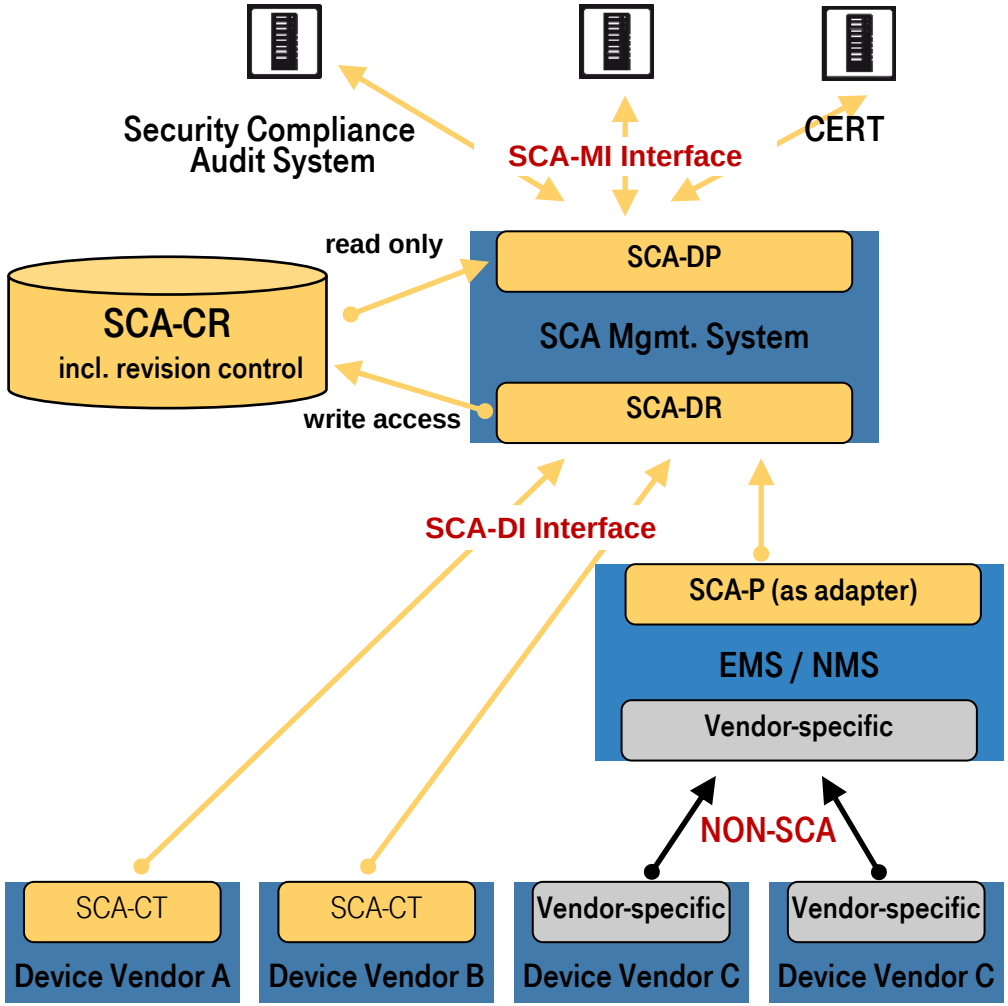
- Stores collected data
- Filter on critical or restricted information

SCA-CT (Collect & Transmit)

- 1st collects local SCA data. 2nd transmits collected SCA data

SCA-DI Interface :

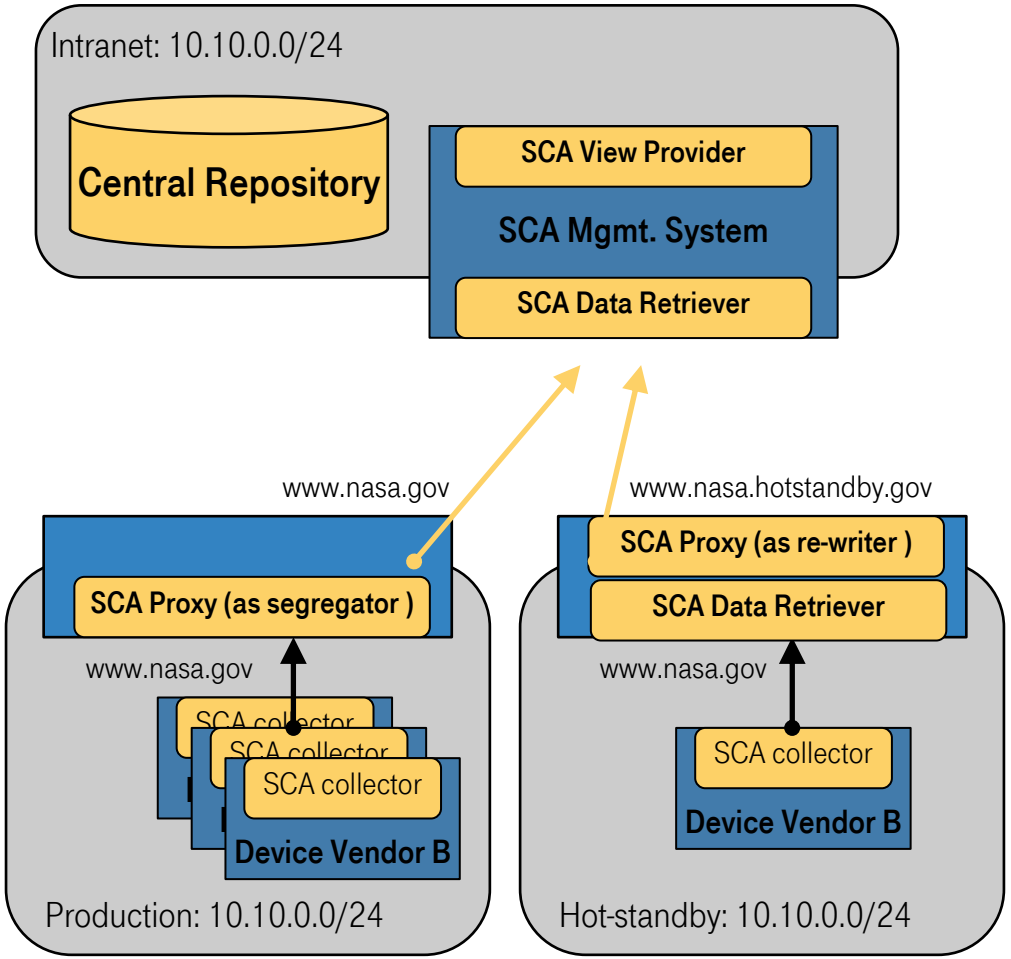
- Transmits Log Data, Config Data, Network & System telemetry data (System status Data), Auto discovery of SCA-DR



Three SCA proxy functions are distinguished: adapter, re-writing and segregation.

Proxy Functions

- Segregation:
  - Segregates networks
    (e.g. minimize IP address conflicts)
    Application
    firewall, 2-Tier
- Re-writing:
  - Adds additional “location” information
    (e.g. re-writes FQDN)
- Adapter
  - Connects non-SCA systems to the SCA Management System
  - Transforms proprietary non-SCA messages to SCA conform messages



Incorporating TMF standard into our devices reduces cost and improves the quality of information collection and much more.

Operations

- Burden of data collection is shifted to vendor (build-in by default)
- Full vendor support of data collection
- Vendor delivers all relevant information in a standardized way
- All relevant information comes with a highly standardized documentation
- Collected information can be reused for many non-security use cases: Support ("SUN Explorer"), License Management, reconcile Identity information, Performance management, ACMDB, even Recovery...

Sourcing

- Reduced individual DTAG requirements
- Reduced supplier selection (RfP/RfI) efforts
- Integrate standard in Procurement Framework (General Frame Agreement)
  - Currently TMF615 in Security Framework for System Suppliers

Current status of SCA and roadmap.

Status

- Scope, requirements and use cases are defined in TMF528 Business Agreement of SCA
- TMF528 Business Agreement is nearly finished and entered final TMF ESEC team review process

- Detailed specification of SCA will be defined in the Information Agreement (TMF619) in 2012
- Final SCA Information Agreement (TMF619) will be expected around Q1 2013
- In addition to the Information Agreement (TMF619) a compliance test kit or sample implementation of the SCA Interface will be described in the Interface Implementation Specification (SCA IIS TMF900)

- DTAG already build up a system with more than 4000 servers that implemented the suggested SCA principles.

- Please join us and support SCA to

Thanks for your attention.

Contact:

Christian Kagerhuber
Deutsche Telekom AG
Group IT Security

Phone: +49 6151 680542

Mobile: +49 171 9754104

Email: kagerhuberc@telekom.de