Cybersecurity for Satellite Control Centres

Prepared by:	GMV Team
Presenter:	Thomas Morel

Contents

Purpose

Satellite control centers multiply **network interfaces,** manage **higher volume of data,** and are increasingly **exposed to cyber security threats:**

- Alteration of **operating system** components
- **Processes** manipulation: application code, malware execution, library replacement
- **External devices**: connection of infected USB or bluetooth devices, keyboards, or hard drive
- **Data**: theft of user data, modification of configuration files

This presentation details a **set of cyber-security solutions to be deployed and integrated as well as good practices** which, **combined**, provide the maximum level of protection against cyber-security threats:

- Key capabilities including **network isolation and protection**,
- **Secure** and encrypted **remote access**
- Operating system hardening
- Software system hardening

Combining solutions

Network isolation and protection
Require several layers of firewalls, a demilitarized zone (DMZ), deep packet inspection and the deployment of virtual private networks for inter-site communication.

Centralized authentication and remote access
Based on encrypted communication and authentication

Advanced monitoring
State-of-the-art SIEM solution to anticipate and detect any unexpected activities

Operating system hardening
Prevents the system to be used by unauthorized users, limiting and controlling the number of services available and forcing rules and policies to be applied at OS level.

Software system hardening
Based on a **process and library whitelist software** which blocks any unlisted process to run.

Network

Secure network

WAN, VPN through Internet

First tier firewalls connect to WAN or inter-site networks and internet. Implements VPNs if required

2 firewall layers

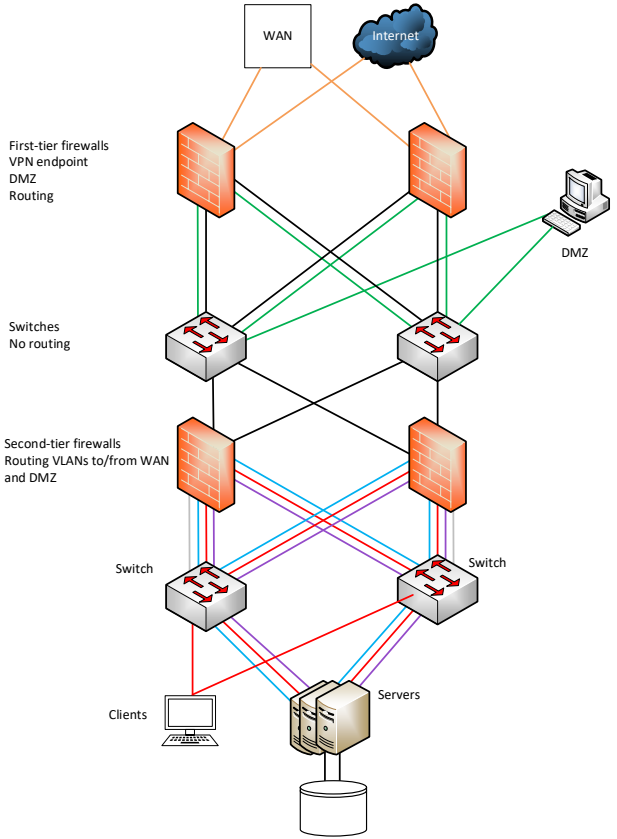
Redundancy and separate manufacturers for increased security. Second tier firewalls rule the internal network and traffic from/to the first tier and the DMZ.

DMZ and remote access

Behind the first firewall layer, the DMZ provides a controlled and limited environment to share data and access remotely to the SCC. Any access from a VPN to the SCC requires at least 3 different rules on 2 layers of firewalls in addition to the authentication steps.

VLANs

Separate VLANs logically and physically to achieve the maximum security and following good practices.



OS ACCESS AND AUTHENTICATION

OS users

One user per person

- Same user for OS and SW with authentication through a centralized authentication server (eg LDAP).
- Cons: difficult and unfriendly user switch at application level.
- Alternatives: do not rely on OS user, isolating and limiting the OS user workspace to the minimum access to operational software, allow friendly application level switch. Implement smart desktop and OS workspace restore after user switch.

SCC workstations

- Web browser: direct access to web apps
- **Application** desktop
- Advanced screenlock with monitoring mode, display visible and active but no keyboard nor mouse until unlock. Possible application user switch.

Virtual environment with thin clients: an additional access control layer

Authentication through LDAP

Access to remote desktop solution client only

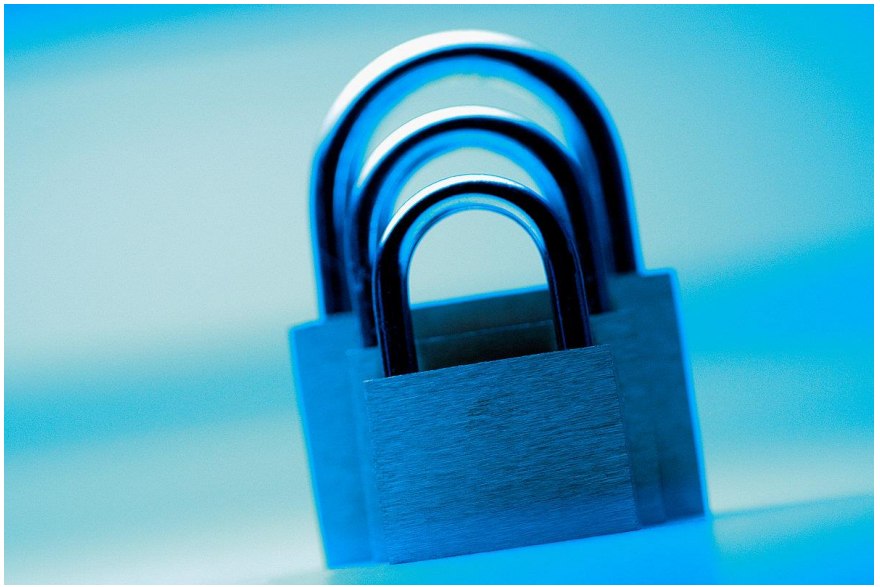
SW ACCESS AND AUTHENTICATION

Apps users

One user per person
For user and SW admin accounts, authentication through centralized authentication server (eg LDAP)

SW admin users
Allow admin users to **access through physically separated areas, both at network and workstation level.**

SW applications profiles and privileges
Set of roles or profiles for each SW subsystem. Users are allowed to login with a specific role or profile.



Remote connection – a real example

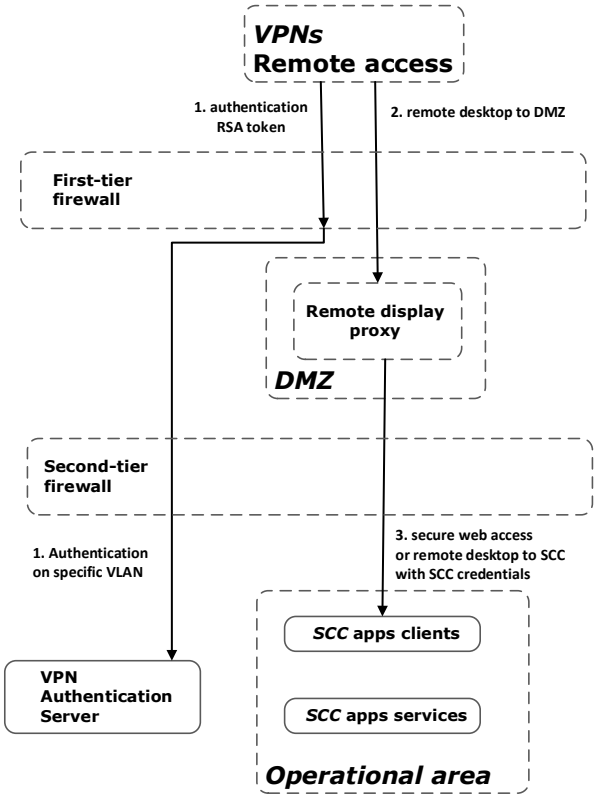
Remote display through VPN

Access through **2 firewall layers** and **2 authentication layers** with up to 4 credentials and tokens

1. Access VPN with user, password and multi-factor authentication token. Depending on the provider, tokens can be accessed through a mobile app, a PC or a specific hardware.

2. Authenticate and access DMZ workspace through a remote desktop solution (e.g. nomachine):
- Local permission to enable remote desktop access
- Support several virtual workspaces on the DMZ workstation.

3. From DMZ remote desktop workspace:
- Access **web interfaces** through a web client. Add both client and server certificate-based authentications
- Access to a ***remote desktop*** with a specific encryption scheme enabled and client certificate based authentication

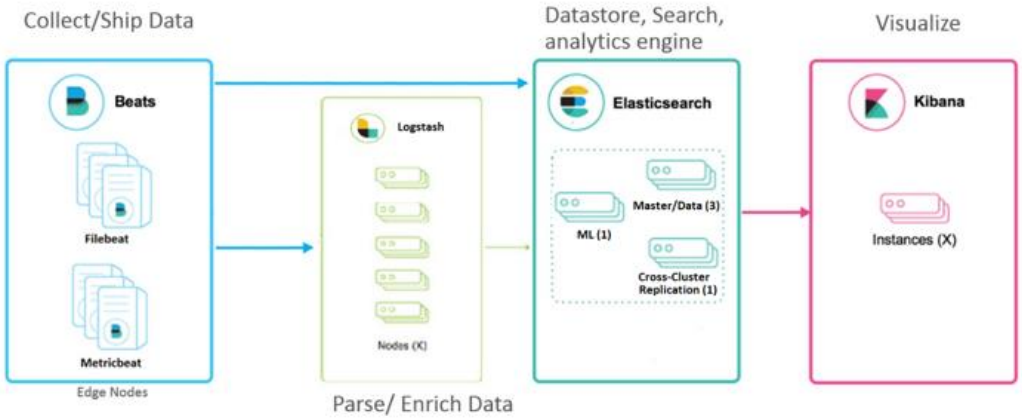


SIEM

Deployed solution

Security events and incidents

- **Elastic Search**: search and analytics engine
- **Beats**: send security events and other data from agents to Elastic Search
- **Logstash**: server-side data processing pipeline that ingests and transform data from Log sources
- **Kibana**: visualize data with graphics and charts.
- **Elastic SIEM**: event correlation
- **ElastAlert**: security alerts



SIEM

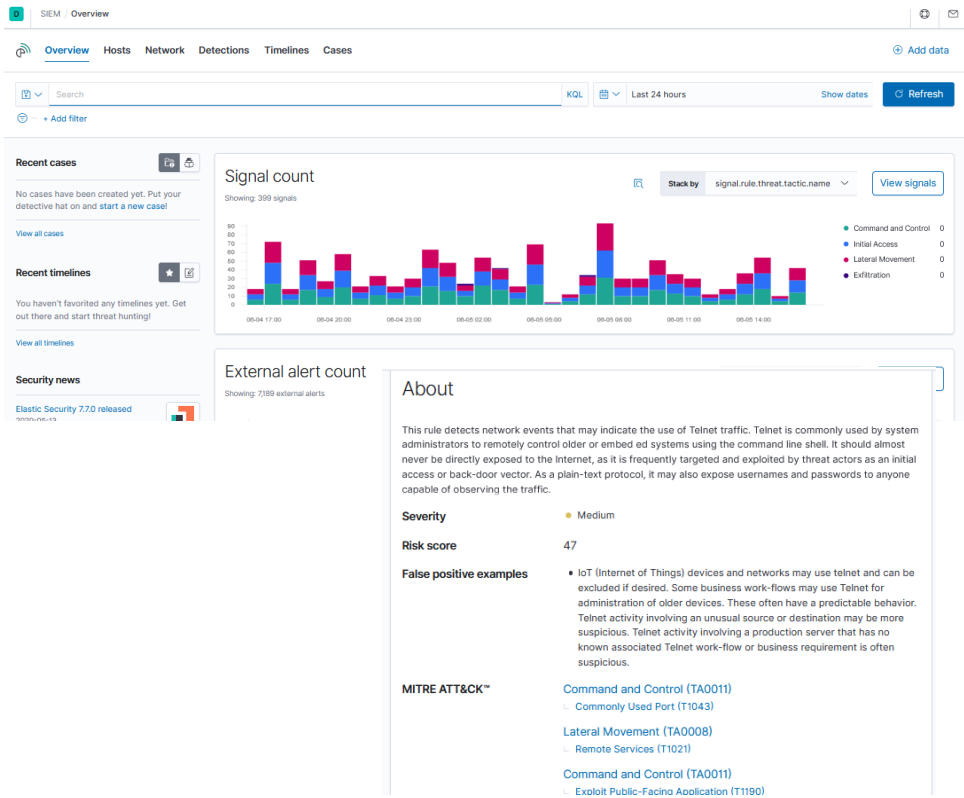
Security rules

Event collection and **correlation** for the whole environment

- 1st and 2nd tier firewalls
- Alerts from system hardening software
- OS syslogs
- App level logs
- Database logs

Security rules mapped to **MITRE ATT&CK**

Customizable dashboards



System hardening

Whitelisting processes

Permanent control and execution of resources

Security control based on policies, which includes execution control of processes and accesses to resources (files, directories, libraries and drivers).

Integrity verification of the binaries (executables) and the **resources** through electronic signature (SHA256).

Control and verification through electronic signature of all the resources used by the interpreters (Java virtual machine, bash, python, perl...).

Incoming/outgoing communications control,
Filtering origin/destination addresses as well as the sender/receiver applications.

Incidents reports
Local log and centralised on the server.

System hardening

Space equipment have very specific functionality and behavior which do not usually change significantly during the mission lifecycle. In such scenario, with a large number of processes involved, a **process whitelisting software** with **learning capability** is ideal, **reducing the possibility for operational human mistakes**.

Agents
Deployed on all the secured machines
Receive and enforce **policies**
Send events of forbidden actions performed in the system **through a secure channel**

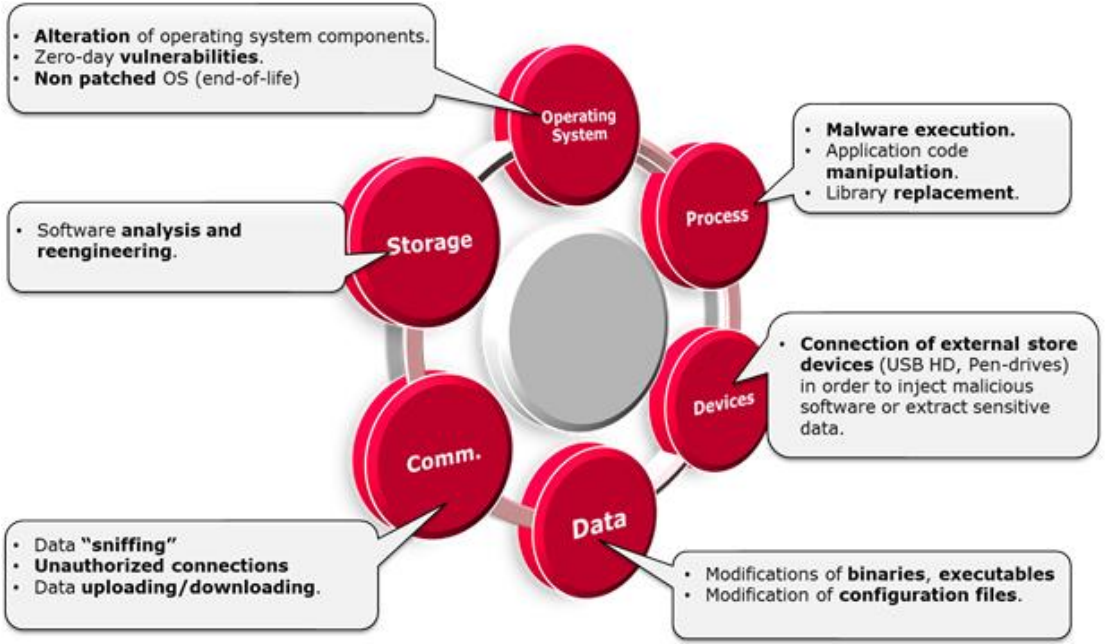
Central management console
Manages all the systems from a web interface

The overall system is transparent, compact and has a **very low footprint**. Server hardening combined with process whitelisting fit well to space systems particularities removing the drawbacks of other typical security safeguards. **Capabilities are implemented and deployed without affecting the reliability, scalability and the productivity of operations.**

At GMV, implemented with *Checker for SCC* derived from world-class ATM *Checker* solution. Integrated with all GMV SCC products including *Hifly*, *Magnet*, *Flyplan*, *Focussuite.* All *are* **server-client and three-tier architecture and fit well with this solution and a very flexible deployment strategy**

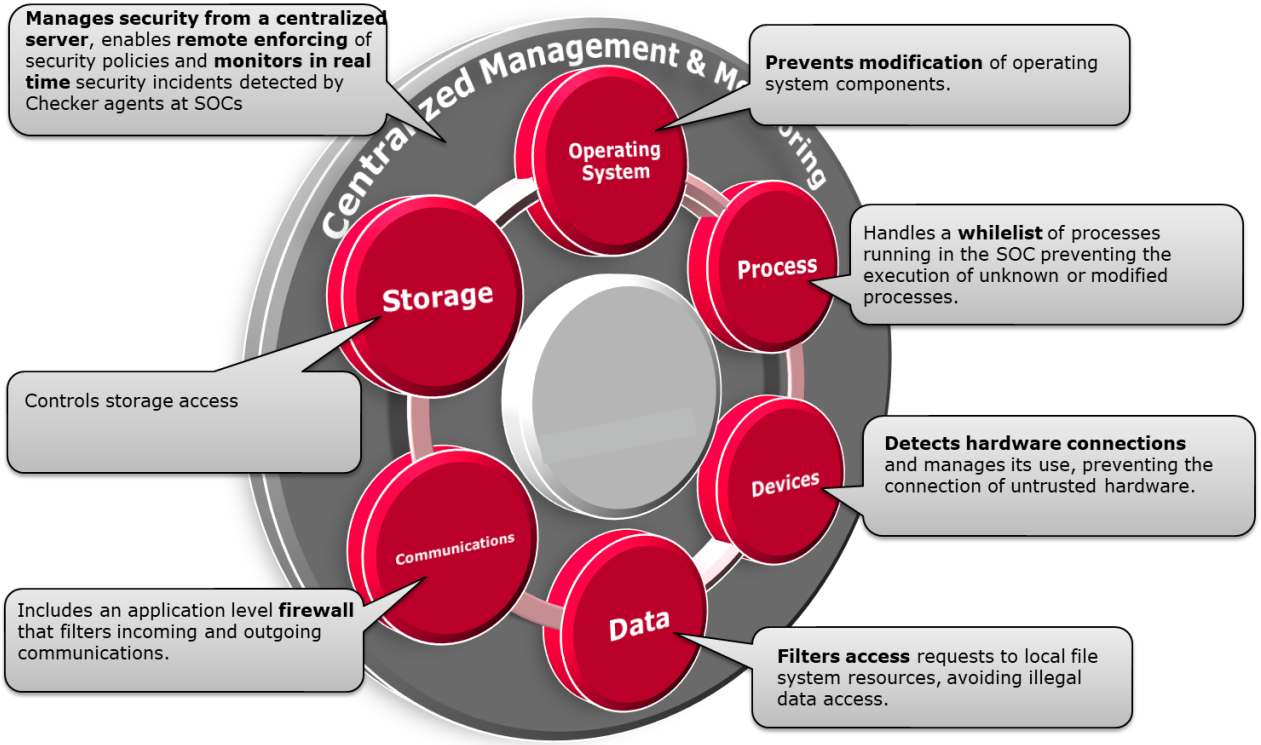
System hardening

Threats



System hardening

Protection capabilities

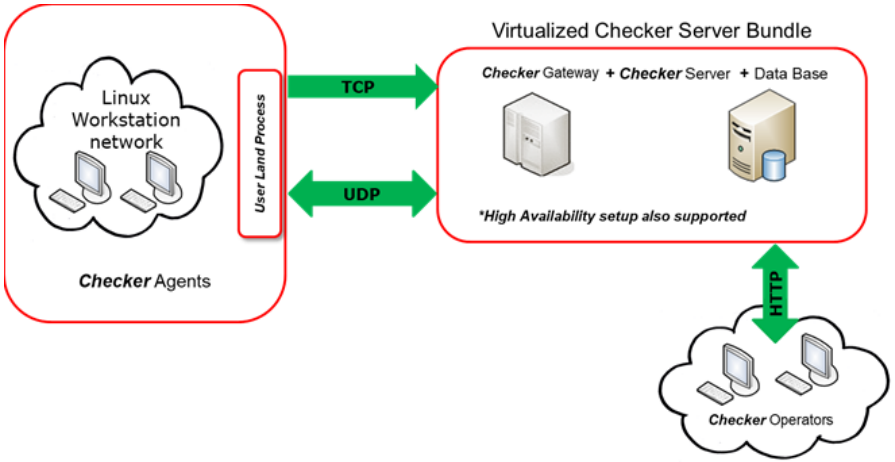


System hardening

Architecture

Components

- Gateway
- **Server**: gateway and management console
- Database
- Web client
- **Agents** deployed on all secured machines, MS Windows or Linux.
  - Loadable kernel module
  - Not unloadable, requires change in boot setup



System hardening

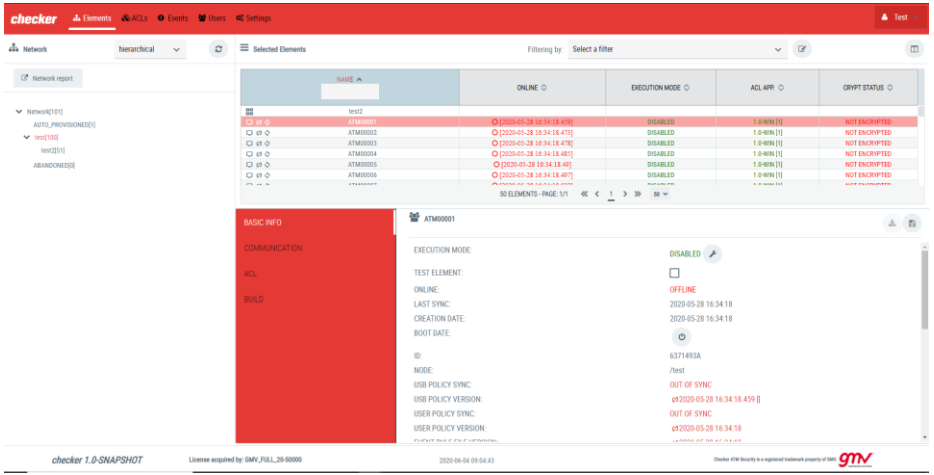
Execution modes

Active mode ("enforcing" mode)
The system blocks and prevents any activity that is not allowed in the applicable policy and generates an alert for each unexpected activity.

Learning mode
No restriction, no alerts
The system builds the policy and learns all the actions to be allowed.

Operator mode
No restriction, alerts for actions not allowed by the policy

Disabled mode
No restriction, no learning and no alert



Challenges

Complex systems: many products and steps to integrate for system-level integration

- **Very complex policies with up to thousands of entries and rules**
- **Firewall rules** and full configuration required to test the system
- System hardening software requires **complete security policies** definition to test the system.

Products in **development** until **late in the integration phase:** requires the system hardening software to be able to **update policies in an easy and intelligent manner.**

Several O.S., or different versions of the same O.S. make more difficult the hardening development and overall integration.

Uncontrolled provider specific appliances or systems requires perimeter security.

Lessons learned

User access definition
Define authentication, authorization and remote access **requirements early** in a project as they can affect all layers and subsystems development and interfaces. In particular profiles, users and privileges and **access levels** have to be clearly identified **before the final design phase**

Integration
For **iterative integration** purposes, policies can be enabled and disabled based on their types: communication, file access, integrity, etc.
Learning mode and **advanced policies edition** capabilities are essential for this purpose.
First phase of integration on a subsystem basis. Incremental integration with interfaces.

Dynamic policies
Mature and stable products early in the integration phase help to validate the system and **increase the security level of the policies.**

Use of **standard and homogeneous interfaces**, protocols and software deployment also makes **the policies easier to maintain and audit**

Future work

Make the system hardening software easier to upgrade and deploy on different versions of the O.S.

Multi-user remote operations: for critical and sensitive operations, implement a remote mission control to ensure two humans are connected from two devices and different communication and authentication channels. Requires integration of all the layers up to the app level.

Fully automatic security policies based on machine learning capabilities

Thank you

GMV Team
tmorel@gmv.com