SpaceOps-2023, ID # 621

Space mission security monitoring at the ESA Cyber Safety and Security Operational Centre (C-SOC)

M.Niezette[a]*, C.Laroque[a] and J.Irving[b]

[a] *Telespazio Germany GmbH*
[b] *ESA Security Office, European Space Agency*
* Corresponding Author

Abstract

The space infrastructure is becoming increasingly critical to the economy and society, with more activities relying on the communications, navigation or Earth observation services it provides. In order to increase the resilience of assets, ESA, under the lead of the ESA Security Office, in coordination with ESA Member States, has initiated significant extensions of their space cyber security infrastructure with the development of the Security Cyber Centre of Excellence (SCCoE) and the ESA Cyber Security Operational Center (C-SOC). While the SCCoE focuses on providing an environment for cyber security engineering, R&D and policy development, the C-SOC will provide cybersecurity services to ESA and potentially external stakeholders.

The C-SOC facilities will be geographically distributed across a number of the ESA sites. In this organisation, ESA Space Operations have an important role as the experts in mission operations to support the C-SOC space mission monitoring.

The C-SOC is currently being developed and deployed by a team led by Leonardo, where Telespazio has a specific role in supporting the service management and space mission monitoring aspects.

An essential aspect of the ESA C-SOC is that it will cover not only the Information Technology infrastructure of the Agency, but will address the Operational Technology (OT) infrastructure as well. As such it aims to be Europe's first non-military space security operational centre.

This paper will give an overview of the services provided by the C-SOC that are specific to space mission monitoring with a focus on space mission threats.

Keywords: security space threat C-SOC ESA

Acronyms/Abbreviations

C-SOC	Cyber Safety and Security Operational Centre
DS	Data Systems
ELM	Event and Log Management
EOP	Earth Observation Programs
ESEC	European Space and Education Centre. ESA main location in Belgium
ESA	European Space Agency
ESA IT	ESA Information Technology Directorate
ESACERT	ESA Computer Emergency Response Team
ESOC	ESA Space Operations Centre. ESA main space operations location in Germany
ESRIN	European Space Research Institute. ESA main location in Italy
ESTEC	ESA Technical Centre. ESA main location in the Netherlands
GndF	Ground Station Facilities
NOC	Network Operations Centre
MOI	Mission Operations Infrastructure
OT	Operational Technology
RFI	Radio Frequency Interference
SCCoE	Security Cyber Centre of Excellence
SANM	Space security And related Node Monitoring
SOC	Security Operations Centre
SIEM	Security Information and Event Management
SIHM	Security Incidents Handling and Management
SOAR	Security Orchestration, Automation and Response
SSA	Space Situational Awareness
TIA	Telecommunications and Integrated Applications

1. Introduction

Having a functional and modern Cyber Safety and Security Operational Centre is of paramount importance for an organisation like ESA that has to build, operate and protect critical assets in space infrastructure and systems. Cyber security is an essential element of nowadays systems and infrastructure. IT Security Operations Centres are a standard measure medium to large enterprises use, are mature and operate routinely. ESA space and ground infrastructures are essential assets for Europe that need adequate protection to ensure confidentiality, integrity and availability of information. A number of tools and processes are already in place today at various levels of the organisation to ensure the security of the current space missions. However, an overarching approach to cyber security in line with the state-of-the-art Security Operations Centres still needs to be implemented.

With this in mind, the future Cyber Security Operations Centre of ESA:

- harmonise the cyber expertise and security monitoring in a common facility
- provide a safe environment to develop critical space missions
- integrate the state-of-the-art of both Information Technology and Operations Technology based SOC in a solution that addresses the specificities of space mission security.
- enable industry to develop the capability needed to apply cyber security approaches to space missions operations and ground segment
- be a step forward towards standardization of security monitoring for space missions
- enable the Space Agency to open its operation to space missions performed by other European stakeholders.

A key to the C-SOC functional scope is its specific space mission orientation. The system will address space mission threats and provide ESA and external users with comprehensive SOC services.

A core team comprising the prime contractor Leonardo, Telepazio and Rhea provide the C-SOC project to ESA.

In the following sections, we introduce the ESA C-SOC context and its services and present the basis of its functionality dedicated to space mission monitoring.

2. C-SOC Operational Context

The C-SOC Operational Context is presented in Figure 1. It depicts the key entities that interface with C-SOC.

The main actors who can play a role in the context of the C-SOC environment are:

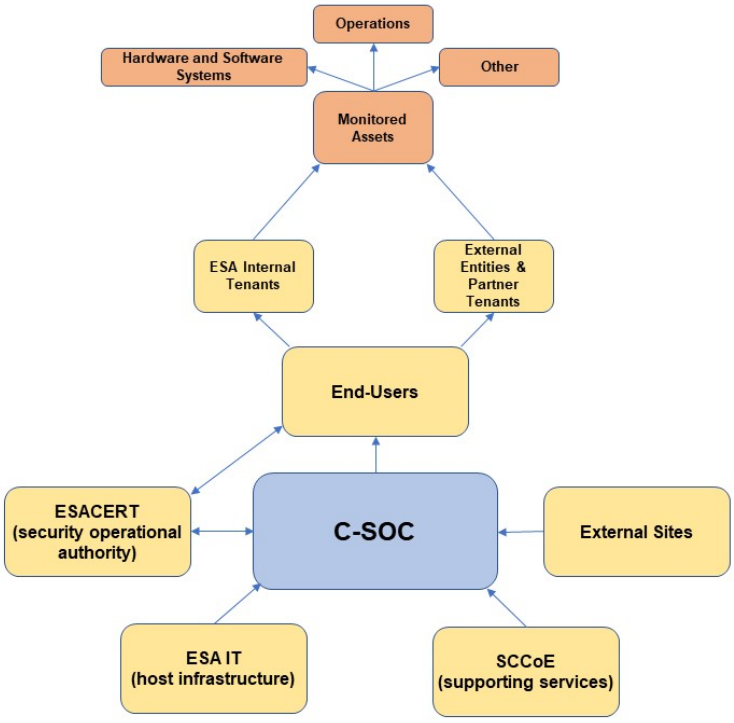

Figure 1 C-SOC Operational Context

- C-SOC Operations Users: Personnel directly interacting with the C-SOC system for the purpose of delivering its service functions;
- End-Users: Organisations engaging the C-SOC system to take advantage of its service functions;
- Additional Stakeholders: Organisations or personnel identified to cooperate with the C-SOC to deliver cybersecurity services to ESA.

The C-SOC End-Users, identified as Tenants, subscribe to one or more C-SOC service. Subscribers can be either ESA Internal Tenants or External Entities & Partner Tenants. For the initial release of the C-SOC the focus is made on the ESA Internal Tenants distributed over a number of the Agencies sites.

External Entities & Partner Tenants generally select C-SOC services will depend largely on their existing capability and the perceived benefits that may come from engaging one or more C-SOC services. The design of the C-SOC considers the varying risk appetites and information sensitivity of ESA missions and partner Tenants.

3. ESA C-SOC System and Services Context

The C-SOC provides a comprehensive suite of services to support users having a wide variety of systems and services to monitor (as illustrated in Figure 2). There are three main aspects of the C-SOC:

- *C-SOC Core System*. The heart of the C-SOC and its services. The Core system hosts the server applications to deliver the Services (as shown in Figure 3). Geographically distributed cloud server clusters host the C-SOC core system. The C-SOC Operations team use the Core system and maintain and deliver the services for ESA and Tenants.
- *C-SOC Peripheral Element* (PE). Normally there is an instance of the PE hosted in the Tenant infrastructure. This sub-system ensures that data received or retrieved from the Tenant infrastructure is not lost, even when there is an extended loss of connectivity to the C-SOC core system and ensures a secure exchange from the Tenant site to the C-SOC core system.
- *C-SOC Portable Operations Platform* (C-POP). The C-POP is an innovation of the ESA C-SOC, which recognises that Tenants often wish to have more than a simple e-mail/ticketing interface for interacting with SOC services. This platform facilitates the Tenant's remote access to the C-SOC services, ensuring segregation between the different monitored systems.
  The C-SOC allows the tailoring of the services accessed via the C-POP for each Tenant. This tailoring ranges from the C-SOC Core System Operations team providing the entire 'SOC as a Service' all the way to the Tenant having the autonomy to perform their own offense analysis and incident response.

As every system is different, for each new end-user/Tenant, an onboarding activity is performed to define the services, performance levels, equipment, and applications to be monitored. Depending on the client's

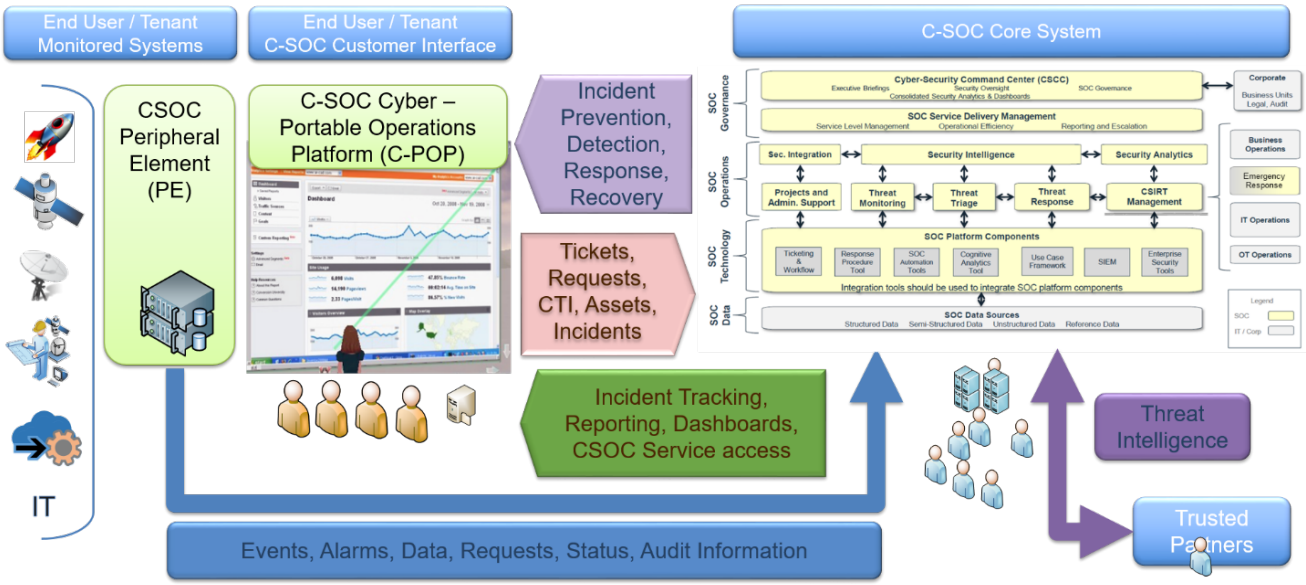

Figure 2 C-SOC System and Services Context

infrastructure and systems complexity, this can take a few weeks to months. The design of the C-SOC enables gradual service additions and subscriptions without affecting other end-users or their services.

4. ESA C-SOC Services

C-SOC offers a comprehensive suite of services to the End-Users (as summarised in Figure 3). These services cover classic SOC functions, but extend with the latest generation features and include the support for the Space Mission Monitoring:

- Security Event Monitoring;
- Incident Management and Threat Response;
- Tailored Services;
- Cyber Threat Intelligence (CTI);
- Space Missions Monitoring.

Figure 3 C-SOC Service Functions

Security Event Monitoring is the primary function of C-SOC and consists of the operation of the full set of security event detection and handling systems and a reporting service. The security event detection systems deployed at the Tenants are configured to detect security-relevant events based on analysis of signatures and anomalies. When a security event is detected with sufficient confidence, perhaps correlated with other intelligence information and analytics, C-SOC staff will support the end-users/Tenants to escalate the event to an incident, which the C-SOC normally manages in close coordination with ESACERT.

Incident Management and Threat Response is the service C-SOC provides once an incident is declared. C-SOC staff delivering the Incident Management service play a pivotal role given the aggregated information they have and can obtain on ESA systems as well as their access to threat and vulnerability information.

The Threat Response service also encompasses the monitoring of external sources of threat intelligence and vulnerability information to increase the incident management activities through derived context awareness.

Tailored Services are a group of advanced analytics and support services.

Cyber Threat Intelligence (CTI) provides services to allow users to manage the entire cyber threat intelligence cycle, from planning & direction up to dissemination & feedback. The CTI is based on a set of best practice models to perform the threat intelligence tasks, including collection, processing, analysis and dissemination. The collection occurs organically through a variety of means, including pulling metadata and logs from internal networks and security devices, subscribing to threat data feeds from industry organizations and cybersecurity vendors, scanning open-source news and blogs, scraping and harvesting websites and forums, infiltrating closed sources such as dark web forums and intelligence reports from cybersecurity experts and vendors.

5. Space Mission Monitoring

The C-SOC is able to collect and ingest information coming from spatial components and leverage them for alert detection and response.

On the Tenant sites, for the majority of space missions, there will be a Flight Operation Segment (FOS) deployed and responsible for the command and control of the satellite(s). The FOS typically consists of a Ground Station and Communication Network, Flight Operations Control Centre and a General-Purpose Communication Network. FOS facilities provide the capability to monitor and control the satellite during all mission phases, including the Flight Dynamics System facility responsible for orbit determination and prediction, and the generation of attitude and orbit control telecommands.

These facilities, which host monitoring and control capabilities to operate ground and space assets at different levels are mainly:

- Information Technology (IT) for service provisioning of different infrastructure components at IT and networking level;
- Data Systems (DS) for supporting flight control teams in the preparation and daily routine operations, as well as for the development and maintenance of generic and mission-specific satellite monitoring and control system and information security. Each mission is responsible for the operations of the security systems applicable to the mission, and for the overall mission-specific information security;
- Ground Station facilities (GndF) consisting of a set of distributed terrestrial radio (or optical) stations designed for ensuring enough connection time for the commanding and control of satellites and the downloading of payload data. The location and characteristic of the Ground Station depends on the frequency, bandwidth and orbital characteristic of the satellites;
- Supporting Operational Technologies (OT) such as power, cooling that are provided by the related hosting site infrastructure;
- Space Situational Awareness (SSA) providing capabilities and services to support detection of objects and natural phenomena that could harm satellites in orbit or infrastructure such as power grids on the ground.

In mission-critical systems design and operations, availability is normally the highest priority. However, Space is rapidly evolving, and the aspects of Integrity and Confidentiality need to be considered due to increased threats on space missions and the range of missions and Tenants that must be supported.

The SOC operations for IT systems typically rely on data from the network (packets, traps, alerts, network events, correlation alerts) and host (application and OS). In the case of the C-SOC, there is a need to build situational awareness to provide a holistic approach to security. This additional information represents mission-specific information that would support security teams in identifying with better precision potential threats and enabling security orchestration playbooks or procedures to prevent security incidents that could impact space or ground segment operations. Examples of additional sources of information that can be considered for ingestion include:

- Spacecraft telemetry, including spacecraft TM status of on-board and link security function (e.g., encryption, authentication)
- Telemetry provided by critical ground OT systems, in particular, applications for spacecraft and ground station monitoring and control, including RF spectrum recordings;
- Event/logs generated by the ground data systems (including ground station systems);
- Contact and Tracking Plans;
- Communications configurations and tasking plans;
- Maintenance and commanding planning and activities;
- Spacecraft Radio Frequency Interference (RFI) events;
- Other feeds of data, from users, projects and space related systems as well as classic CTI.

From the security orchestration side, there is also the need to define several recommendations and use cases in order to support the security teams in effectively carrying out incident responses and security operations. By further understanding the space-specific collected events, this allows to perform fine grain assessment, further standardise security procedures and automate workflows for threat analysis, hunting and forensics investigation.

6. Threats Specific to Space Mission

Space missions involve the deployment of significant IT infrastructure and, as such, are subject to typical IT threats. Additional threats are specific to the context of the space missions. One of the major added-value of the ESA C-SOC compared to a standard SOC service is the extension of the system monitoring to address these threats by interpreting space and ground data collected via the mission control segment.

The identification of the data to collect for C-SOC is based on an analysis of threat events for spacecraft mission operations and resulting threat scenarios. This data collection is specific to space and ground systems and excludes information technology already covered by other C-SOC services.

6.1. Adversarial threat events

These events (as shown in Table 1) describe tactics, techniques and procedures attackers can utilize to cause harm to assets, operations, and organizations. They range from reconnaissance and information gathering to achieving results like obtaining information, destroying critical infrastructure, and data corruption. Some of these events may result from unintentional or accidental incident, for the purposes of brevity, the term Adversarial

threat event is used. Although built independently by the Authors, it is consistent, but simplified versus the Sparta [1][2] model focused on adversary events on the core system and the satellite There is some overlap with classical tactics and techniques such as those described in the Mitre ATT&ACK framework [3] but tailored to focus on the most relevant for the satellite domain. They range from reconnaissance and information gathering to achieving results like obtaining information, destroying critical infrastructure, and data corruption. Some of these events may result from unintentional or accidental incident. For the purposes of brevity, the term Adversarial threat event is used.

Table 1 Adversarial Space Mission Threat Events

ID	Event	Description
ATE-01	Conduct RF communications interception attacks	Adversary takes advantage of RF communications that are either unencrypted or use weak encryption (e.g., encryption containing publicly known flaws), targets those communications, and gains access to transmitted information and channels.
ATE-02	Conduct optical free space (over the air) communications interception attacks	Adversary takes advantage of optical free space communications that are either unencrypted or use weak encryption (e.g., encryption containing publicly known flaws), targets those communications, and gains access to transmitted information and channels.
ATE-03	Conduct RF communications jamming attacks	Adversary takes measures to interfere with wireless communications to impede or prevent communications from reaching intended recipients.
ATE-04	Conduct optical free space (over the air) communications jamming attacks	Adversary takes measures to interfere with optical free space communications to impede or prevent communications from reaching intended recipients.
ATE-05	Conduct optical sensor jamming attacks	Adversary takes measures to interfere with optical sensor to impede or prevent imaging for one or multiple optical wavelengths. This can potentially damage the sensor.
ATE-06	Conduct targeted Denial of Service (DoS) attacks	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
ATE-07	Conduct brute force login attempts/password guessing attacks on RF link	Adversary attempts to gain access over RF link to a satellite by random or systematic guessing of passwords, possibly supported by password cracking utilities.
ATE-08	Conduct Airborne Communications Attacks	Adversary takes measures using optical or RF to perform unauthorised communication with the spacecraft. This maybe resulting from unprotected link or exploiting features of the satellite via other attacks or modes of the satellite (for example, interference leading to a safe-mode, which disables link security enabling a bypass of the encryption or an exploit of a side-channel attack).
ATE-09	Conduct brute force login attempts/password guessing attacks on information systems	Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.
ATE-10	Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components. Such attacks may exploit weak supply chain integrity (e.g. code signing), another example could be that a hosted payload is compromised and used to interfere with the platform or gain unauthorised privileges.

ID	Event	Description
ATE-11	Orbit trajectory manipulation	Adversary changes the trajectory of a spacecraft by docking to it with its own spacecraft and performing manoeuvres while remaining docked, or manipulating the planned orbit via measures such as laser ablation.
ATE-12	Use of ballistic Anti-Satellite (ASAT) weapon	Adversary physically strikes an object in order to disrupt or destroy it. This maybe direct from ground (such as a kinetic weapon, such as a missile, or laser to blind or damage the vehicle), or from a space based platform, perhaps a hijacked satellite.
ATE-13	In orbit proximity intelligence	Adversary performs proximity operations to gather intelligence on the characteristics of satellite system in orbit.
ATE-14	Compromise the Platform/ Payload	Adversary has access to the Telecommand/Telemetry and utilises this to perform unauthorised activities and compromise the satellite. Such attacks could include unauthorised modification of logs, disabling functions, unauthorised commanding, exploit of vulnerabilities between payloads, modification of configuration, software and similar.
ATE-15	Ground Systems Manipulation	Adversary physically, or via network vulnerability gains access to the ground systems to gain access to the main system, interfere or manipulate the configuration of the systems at the ground station or the main control systems.

6.2. Non-adversarial threat events

These threat events (as shown in Table 2) are caused either accidentally or by environmental factors. They are not actively initiated with the goal to cause harm.

Table 2 Non-Adversarial Space Threat Events

ID	Event	Description
NATE-01	Geomagnetic storms	A geomagnetic storm, also known as a magnetic storm, is a temporary disturbance of the Earth's magnetosphere caused by a solar wind shock wave and/or cloud of magnetic field that interacts with the Earth's magnetic field.
NATE-02	Solar radiation storms	Solar radiation storms occur when large quantities of charged particles, protons, and electrons, are accelerated by processes at or near the Sun. When these processes occur, the near-Earth satellite environment is bathed with high energy particles.
NATE-03	Radio blackouts	Radio Blackouts are caused by bursts of X-ray and Extreme Ultraviolet radiation emitted from solar flares. Radio blackouts primarily affect High Frequency (HF) (3-30 MHz) communication, although fading and diminished reception may spill over to Very High Frequency (VHF) (30-300 MHz) and higher frequencies.
NATE-04	Satellite collisions	Satellites can collide with other active (but not intentional collision - see ATE-12, ATE-14), inactive satellite systems or space debris. The collision can cause harm to subsystems or lead to the destruction of the entire satellite and the creation of new space debris.

7. Monitoring Data Sources

The threat analysis above leads to the identification of space and ground data sources that can be collected in the control segment and provided to the C-SOC to support the mission security monitoring and are configured and tailored to minimise false alerts and information not useful to support the threat assessment.

Table 3 Space Mission Monitoring Example Data Sources

Data Source	Affected Element	Description	Usage and Relevance
Satellite Live Telecommands/ Telemetry	Space Element	Telecommands and Telemetry such as out of limits, Command verifications, housekeeping received 'live'.	Can be used to provide context information on the S/C commanding, or to show reception of un-expected/wrong commands. Relevant to the threats ATE-03, ATE-04, ATE-06, ATE-07 and ATE-10
Satellite Logs	Space Element	Telemetry cached on-board and downlinked at next available contact.	Collect events with specific severity that could inform of security incident in the space element, including on-board failures, anomalies and hardware built-in test results. Relevant to the threats ATE-03, ATE-04, ATE-05, ATE-07, ATE-10, ATE-11, NATE-01, NATE-02 and NATE-03.
Ground Mission Alerts and Logs	Ground Element	Alerts and logs from the Ground segment related to the mission. Such as protocol errors, link problems, network errors.	Support detection of intrusions, attacks on the link, interference, anomalies on-board and on-ground. Relevant to the threats ATE-03, ATE-04, ATE-07 and ATE-10

8. Extensions for additional Tenants

The C-SOC framework is designed to be multi-Tenant and provides flexible modes of operation. This enables the different needs of Tenants to access and utilise the C-SOC in line with its sensitivity and operation's needs.

For example, a current tenant may desire changes to in place or add additional services. Another Tenant may require the full support of C-SOC, perhaps including updating the EDR and automated intrusion protection.

Even in New Space, where there is a move to have larger constellations, common platforms, standards and use of IT protocols, there remains a wide range of protocols and solutions. Tailoring is common for commercial IT SOCs to adapt to a Tenant infrastructure, software and configuration, handled within the onboarding activity and initial service activation.

The C-SOC infrastructure is designed to be scalable without major re-design.

9. Conclusions

The C-SOC will provide a central focus of Operational cyber security monitoring for ESA and its partners. The first version is planned to go live within the next 18 months, providing centralised, state-of-the art security monitoring services for the core activities of ESA. The C-SOC is also designed to be flexible and support additional Tenants and services without impacting ongoing operations. The Space security And related Node Monitoring (SANM) functions of the C-SOC are designed to enable the integration of the space elements into a Security monitoring platform that can be extended and improved in line with the Tenant security posture and needs.

The C-SOC is a major contributor to improving the cyber resilience of ESA for Europe in Space in the coming years.

Acknowledgements

The authors would like to acknowledge the contribution of the Leonardo who are leading the development of the C-SOC, the European Space Agency and its Member States who have supported the C-SOC initiative to improve ESA and Europe Cyber Resilience.

References

[1] Aerospace Org, Space Attack Research and Tactic Analysis (SPARTA) matrix v1.2, Dec 08 2022, https://sparta.aerospace.org/, (accessed 29/01/2023).

[2] B. Bailey, Space Attack Research an Tactic Analysis (SPARTA) overview, Nov 22 2022, https://sparta.aerospace.org/resources/SPARTA_Overview_InDepth_Nov22.pdf, (accessed 29/01/2023).

[3] MITRE Org, MITRE ATT&CK® Matrix for Enterprise v12.1, Apr 01 2022, , https://attack.mitre.org/matrices/enterprise/, (accessed 29/01/2023).