AROBS Engineering

# Cybersecurity study&solutions for space projects

# Current overview

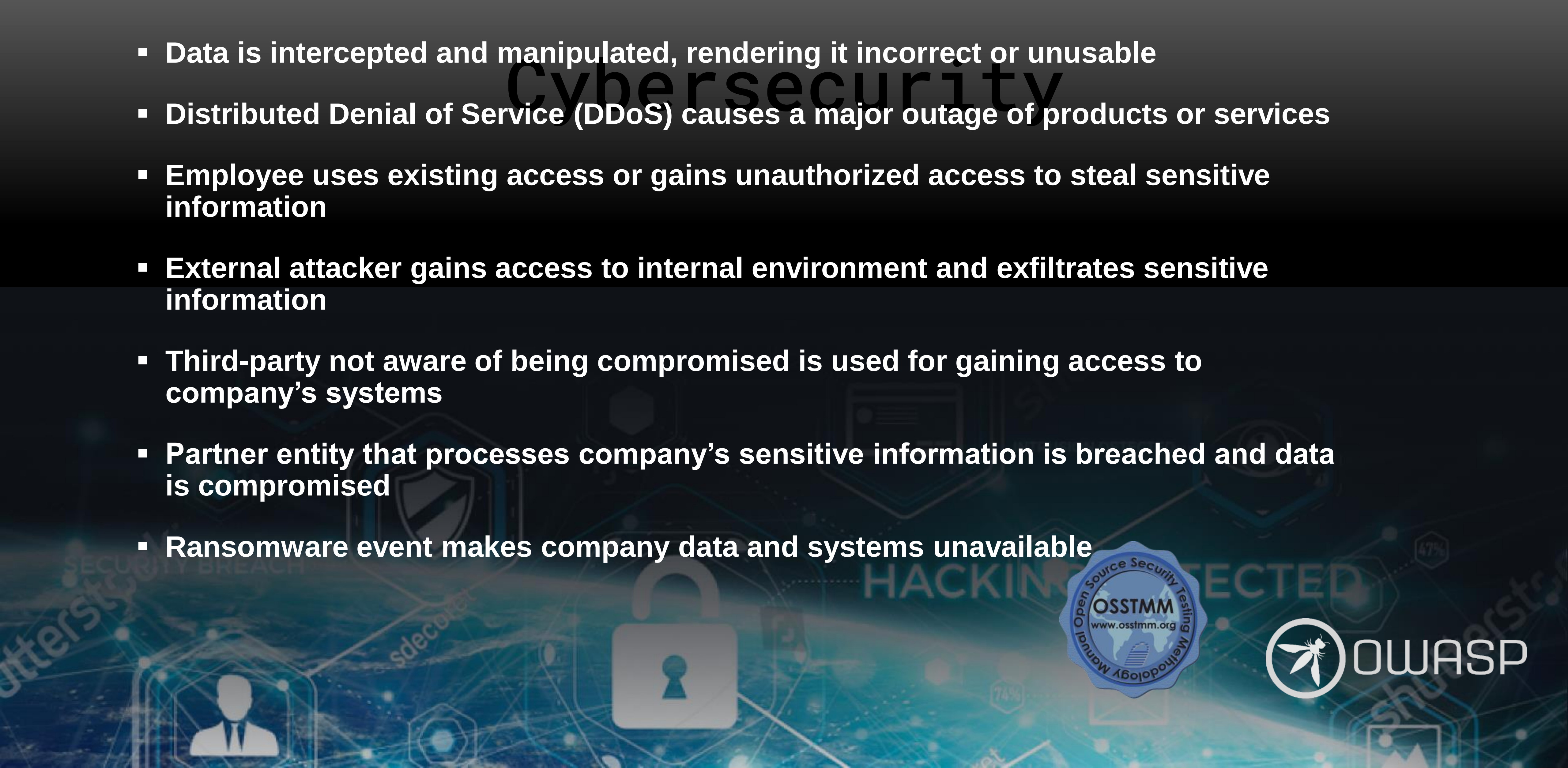
The cybersecurity threat landscape is constantly evolving as malicious actors develop new techniques and exploit vulnerabilities to compromise digital systems and data. Processing geospatial and spatial data presents its own unique set of cybersecurity challenges and threats

- It is essential that organizations have the capability to monitor data flows, access to systems, changes in configurations, correlate events, and are able to quickly triage alerts and respond to incidents.
- The maturity and level of readiness can vary  across entities – and also each has unique ways to use/store data and to setup its IT infrastructure.
- A common  way to help prevent and react to Cyber threats would be needed, as purely custom solution are very expensive.

# Threats and risks

AROBS Engineering

- Data is intercepted and manipulated, rendering it incorrect or unusable
- Distributed Denial of Service (DDoS) causes a major outage of products or services
- Employee uses existing access or gains unauthorized access to steal sensitive information
- External attacker gains access to internal environment and exfiltrates sensitive information
- Third-party not aware of being compromised is used for gaining access to company’s systems
- Partner entity that processes company’s sensitive information is breached and data is compromised
- Ransomware event makes company data and systems unavailable



OSSTMM
Open Source Security Testing Methodology Manual
www.osstmm.org

OWASP

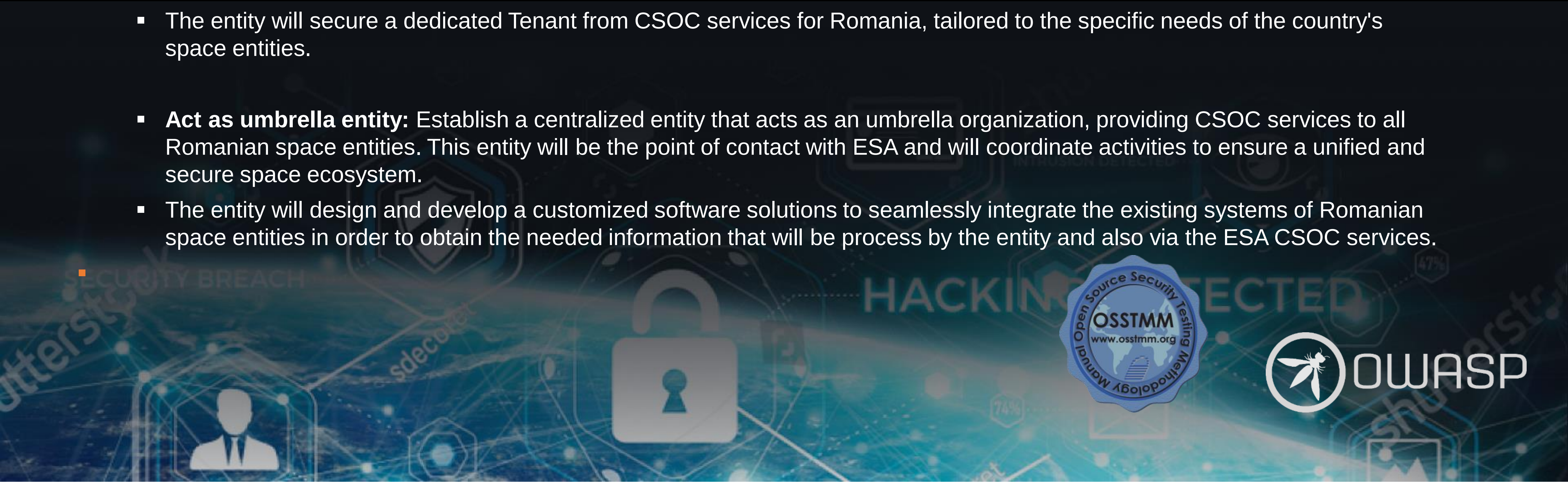
# Cybersecurity models

- **Isolated**
  - In this model – we can invest in each entity in to deploy an independent CSOC type group that will perform all the needed activities; and only share CTI level information with the other entities inside/outside Romania.
  - This would be the most “powerful” solution and could address most/all identified risks – but it would also be the most expensive and time-consuming to implement.
- **Partnership**
  - This is a model where the local entities have limited internal security capabilities and rely on an external partner (CSOC) for most activities, (such as VA/ PT, Incident Management, anti-APT) to augment its current internal capability.
  - This model offers some important advantages, as it is faster to implement and retain the current local security solution/services and offers a balanced cost.
- **Outsourced**
  - In this model, the local entities rely completely on external (CSOC) partners that use their core systems and their dedicated personnel to support the entities for all levels of security operations.

# Proposed solution

- The study concluded with the proposal to create a central/independent CSOC entity in Romania (which can be supplied by a private entity or via public-private partnerships) that will have the following objectives:
  - **Provide CSOC Services:** The main option foreseen is for this entity to collaborate with the European Space Agency (ESA) to obtain CSOC services, leveraging the established infrastructure developed by Leonardo. This will serve as the foundation for a robust cybersecurity framework and will ensure that the timeframe needed to have these services operation towards the local entities in Romania is short/efficient.
  - The entity will secure a dedicated Tenant from CSOC services for Romania, tailored to the specific needs of the country's space entities.

  - **Act as umbrella entity:** Establish a centralized entity that acts as an umbrella organization, providing CSOC services to all Romanian space entities. This entity will be the point of contact with ESA and will coordinate activities to ensure a unified and secure space ecosystem.
  - The entity will design and develop a customized software solutions to seamlessly integrate the existing systems of Romanian space entities in order to obtain the needed information that will be process by the entity and also via the ESA CSOC services.



# Proposed solution

| Service Type | Provided directly by central RO entity | Provided by central RO entity from ESA CSOC |
|---|---|---|
| Vulnerablity Assesment | X | |
| Peneration Tests | X | |
| Anti-APT (Advanced Persistent Threats) | X | |
| Security Event Monitoring | | X |
| Incident Management and Threat Response Support | | X |
| Cyber Threat Intelligence (CTI) | | X |

AROBS Engineering

🌐 arobs.engineering

f arobs/engineering

arobs_engineering

in arobs_engineering