CYBERSECURITY FOR THE SPACE ECONOMY

1 Profiled Cybersecurity: only what is needed effectively

Cybercrime attacks have reached unsustainable levels in Cyberspace, considered as the fifth dimension for human relationships and interactions, both collaborative and conflictual

Cyberspace security issues are becoming (are) serious

Nesecon with excellent skills in IPsec - SSL VPN, Cybersecurity, Virtualization, Cloudization, Backup-Storage, in Alliance with Gordionet involved for years in Services and Integration of Satellite Systems, has structured modular packages of profiled Services and Solutions for Companies in the Space Sector

Compared to what the market offers, Nesecon is an Optimizator - Orchestrator, going into the microscopic detail of what is effectively needed

Cybersecurity is no longer considered a technological cost but a business investment, due to serious incidents with economic - financial - competitive - operational - reputational losses

The damages suffered reached a worldwide cost of 8 TUSD, the Cybersec market has surpassed 200 BUSD

Continuously expanding attack surface across Networks, Cloud, Edge, Data Centers, Public/Private Offices, Fixed and Mobile Endpoints, IoT

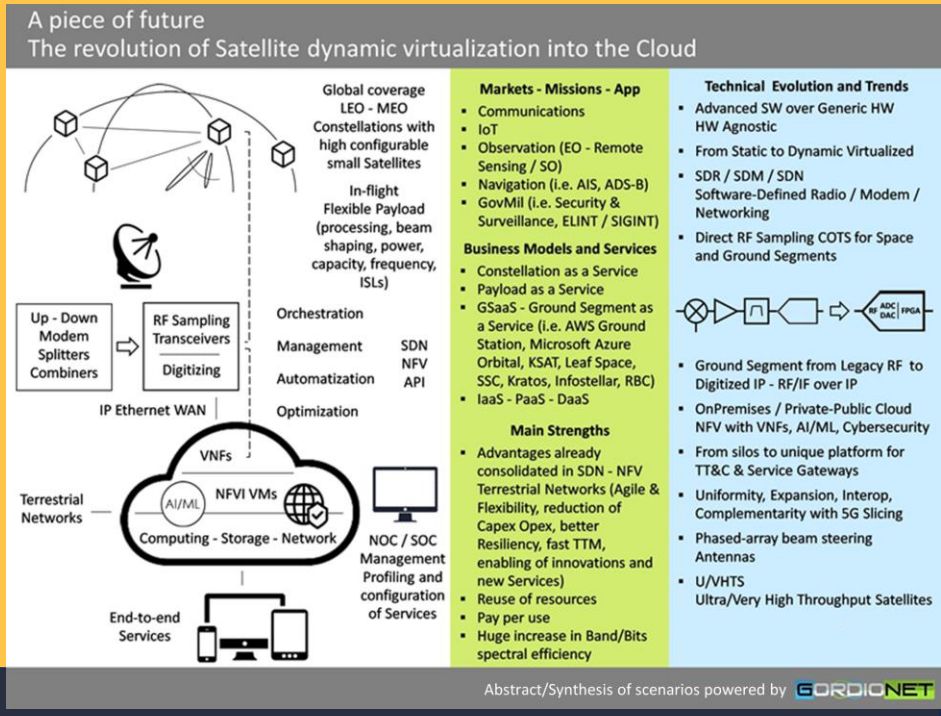
Need for Dynamic Multilayer Cybersecurity for Network - Cloud - Endpoint, with Prediction - Prevention - Detection - Response instead of Mitigation

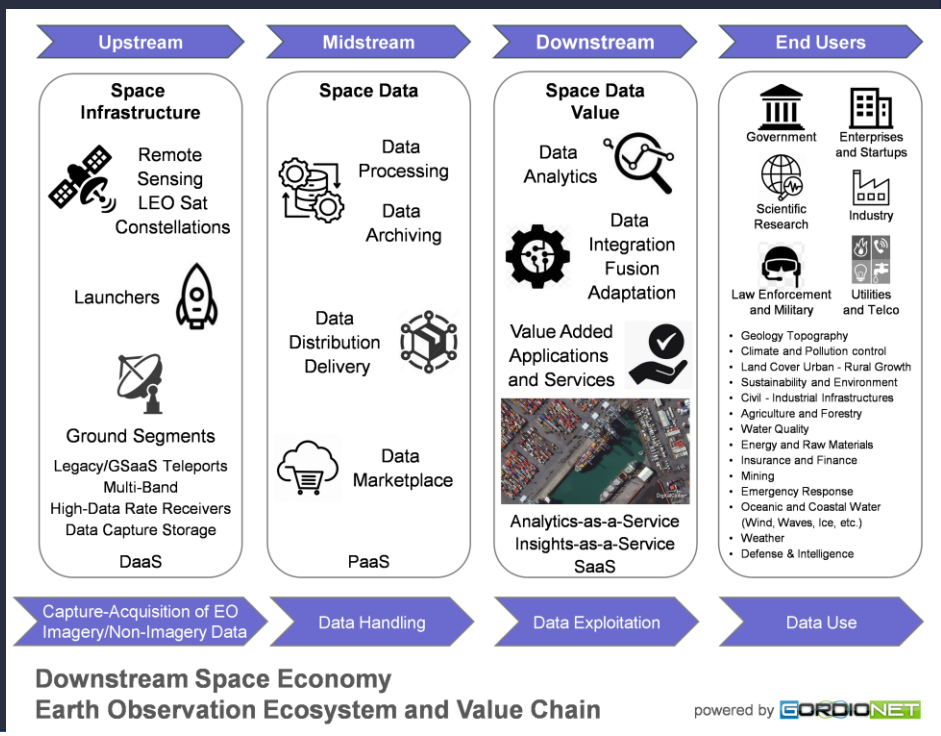
GORDIONET NESECON SAFE DIVE INTO THE NET

2 Space Sector in continuous evolution

The Space Sector in complementarity-alternative with the Terrestrial one, is in great Civ/Mil expansion thanks to the constant increase in reliability, capacity, performance, compactness of systems, global coverage of LEO MEO constellations, reduction in the cost of technologies and services

SatCom (GEO-LEO), SatEO (LEO), SatNav (MEO), have benefited from the experience gained on the Terrestrial Networks for Software-Defined, Virtualization, Cloudization, Hyperscaling, AI/ML, Digital Twin, As-a-Service, 5G Slicing, with global trends currently focusing on Multi-Orbit, Multi-Band, In-Flight Flexible Payloads, RF/IF over IP, RF MW to Laser for ISL, 5G NTN





GORDIONET NESECON SAFE DIVE INTO THE NET

3 Next-generation Cybersecurity

The expansion of networks, Third-Party integration, mobility outside the corporate protection perimeter (roaming users - smart working), have greatly extended the area of exposure for data breach, privacy and Malware threats such as Viruses, Worms, Trojans, Bots, Ransomware, Backdoors, Spyware, Adware

Traditional defense measures (Firewalls, IDPS-RASP Systems, Antivirus, AppSec, etc.), are in a situation of passive vulnerability and are no longer sufficient to counter new types of attacks with an increasingly high degree of coordination and intelligence

Dynamic Multilayer defense strategies-tactics have now become essential, allowing automatic updates and reconfigurations on flexible Zero-Trust models for Zero-Day vulnerabilities

Current state of Cyberblocks

Network Security

Network Firewall - NGFW Next Generation Firewall
IDS, IPS, DDoS Protection, Threat Emulation, Threat Extraction, Antivirus, Anti-Bot, App Control, URL Filtering, Identity Awareness, Content Awareness, Mobile Access, IPsec-SSL VPN, VDI, Advanced Networking & Clustering, SSL/TLS Visibility and Orchestration, SIEM Security Information and Event Management, Machine-Deep Learning UEBA User & Entity Behavior Analytics

Gi/SGi Firewall for Mobile-5G-IoT
GiLAN, CGNAT, DDoS protection, Application Visibility

Cloud/Web Security

WAF Web Application Firewall
Private-Public-Hybrid Cloud Visibility-Management-Protection, DDoS Protection, Vulnerability Management, CASB Cloud Access Security Broker, Data discovery-classification, Data Protection, DLP

Endpoint Security

EPP Endpoint Protection Platforms, EDR Endpoint Detection and Response, XDR Extended Detection and Response
Device Control, Wiping and Control, Advanced Endpoint Protection, Machine Learning, Threat Intelligence, Server Security, DLP, Mobile and Virtual Environment, Security Management, IoT Security, Endpoint Detection and Response, System Performance and User Productivity

GORDIONET NESECON SAFE DIVE INTO THE NET

4 Understand and evaluate with Prediction - Prevention

First of all, to understand what vulnerability situation the company is in

Prediction - Prevention with a rapid Auditing - Assessment on the Network, on the Data Protection Processes - Privacy and through OSINT-based Tools Services

OSINT-based Tools perform information collection from open public sources on the Web/Dark-Deep Web without copyright-privacy violation and not indexed by common search engines, monitoring, data analysis, traffic types, strategic risk analysis

citing of names, email addresses, passwords, photos, articles, social media posts, bank accounts, copyright violations, presence of sensitive data in cracked DBs, IP addresses involved in attacks, etc..

firewall security, open ports, network vulnerabilities and flaws, unprotected SW and files, hidden or insecure connections, rDNS lookups, error-based SQL injection, sensitive files such as robot.txt

OSINT-based monitoring tools used by Nesecon, can identify violation scenarios and possible attacks in advance, allowing to integrate or strengthen a certain level of Cybersecurity consistently with the level of exposure to risk

Can be used additional Tools that simulate attack attempts or other activities to test the reaction capacity of the company systems perimeter

OSINT

GORDIONET NESECON SAFE DIVE INTO THE NET

5 Acting with Detection - Response

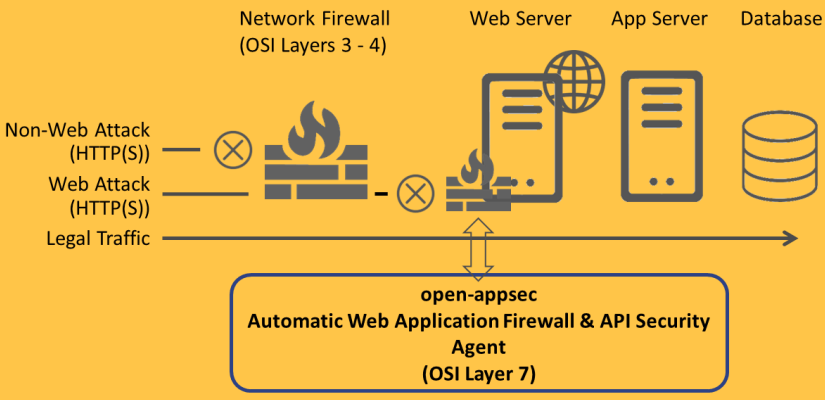
From the results of Network Auditing Assessment - Data Protection Processes - Risk Analysis Tools, implement-replace-upgrade the Cybersecurity **Detection - Response** of Network-Cloud/Web-Endpoint, avoiding expensive Systems-Services I HW-SW I OnPrem-Cloud, which are useless if not evolved and not profiled on the exposure of the own vulnerabilities

New generation of Cybersecurity based on AI/ML - NLP, with automatic dynamic self-learning techniques on behavioral analysis, traffic, databases, without reference to signatures, IP addresses, DNS, etc.

First Rule: Next-Generation Firewall for Network and Web/Cloud Security

WebApp/Services and APIs are replacing traditional applications with an urgent need to integrate advanced WAF Web Application Firewalls to strengthen security strategies

Nesecon, in addition to directing Customers on Network-Cloud/Web-Endpoint Security choices and configurations, is Ambassador for Italy, Competence Center, 1st Level Help Desk of open-appsec (Check Point), innovative Automatic WAF & API Protection through Contextual ML Machine Learning, with the best Balanced Accuracy on the market

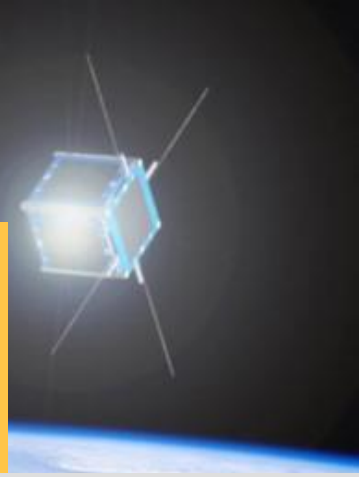


WAF BYPASS HACKERS TECHNIQUES

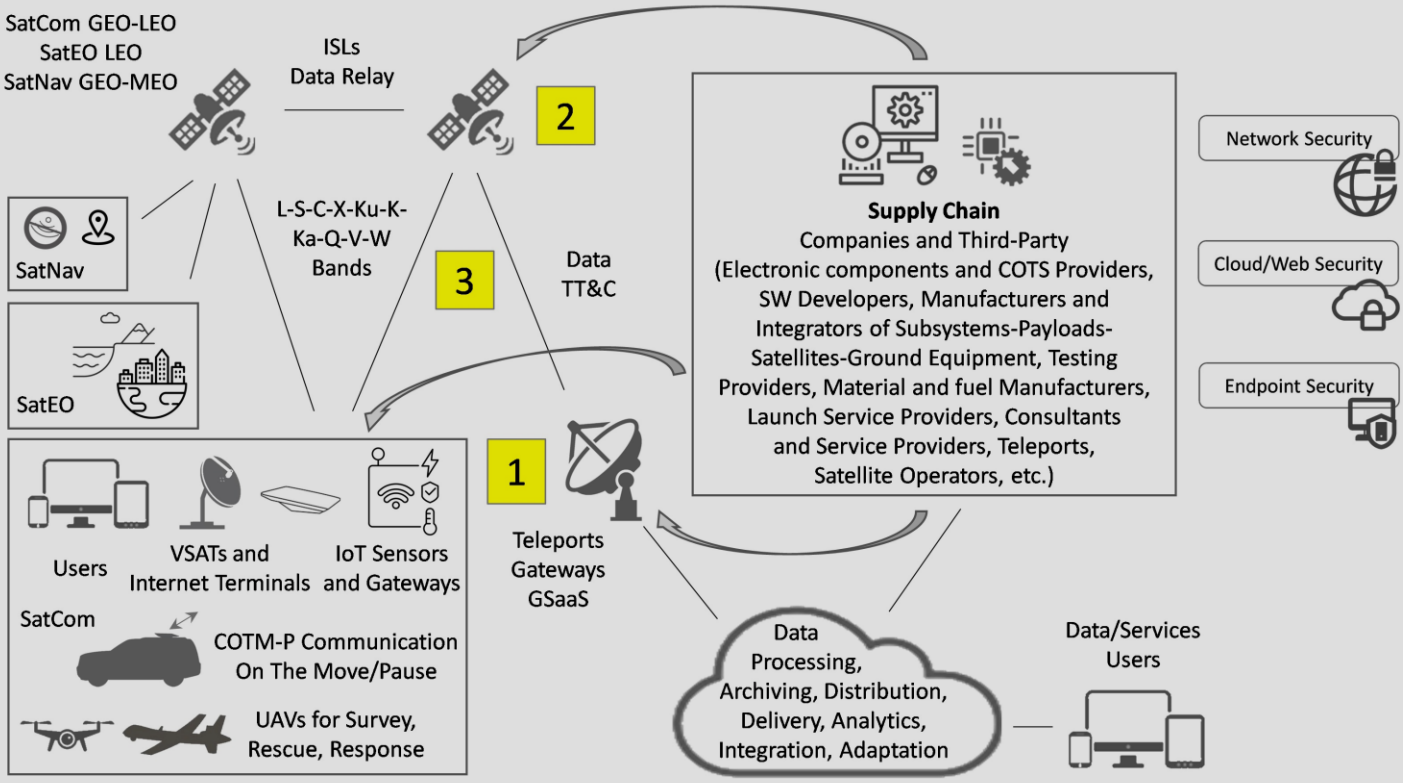
Content size limit exceeded, JSON-based SQL Injection, Regex Bypass, Charset Encoding-Obfuscation, Unicode Compatibility, Case Toggling, URL Encoding, HTML Representation, Comments, Double Encoding, Wildcard Obfuscation, Dynamic Payload Generation, Junk Characters, Line Breaks, Uninitialized Variables, Tabs and Line Feeds, Request Header Spoofing, Null Bytes, HTTP Parameter Pollution....

GORDIONET NESECON
SAFE DIVE INTO THE NET

6 Space Sector Critical Infrastructure



Attack surface composed of three potentially vulnerable segmentations: Ground Segment, Space Segment, User Segment (the last one as the weakest link in the chain). Attack propagation via OnPrem-Cloud, Satellite Data Channels, TT&C, ISL



Generic example of Space Economy scenarios, Perimeter, Vulnerabilities, Threats, Attack Propagation

Powered by GORDIONET

EXAMPLES OF RISKS-THREATS WITH CYBERSECURITY NEEDS

1 CNE Computer Network Exploitation - DoS by Network/Cloud Infrastructure failure - Data Corruption/Modification - Supply Chain Attack - Malware Injection - Social Engineering - HW Backdoor

2 DoS (SDR Software-Defined Radio and DSP SW corruption with possible buffer overflow risks) - HW Backdoor - Malware Injection - Privilege Escalation - Hijacking - Sensors Manipulation

RF Signal/Optical/Comm

3 Jamming (SatCom, SatEO, SatNav) by Signal/Command Injection - Eavesdropping - Satellite Hijacking - Spoofing (SatNav GNSS) - Metadata Analysis - Replay Attacks

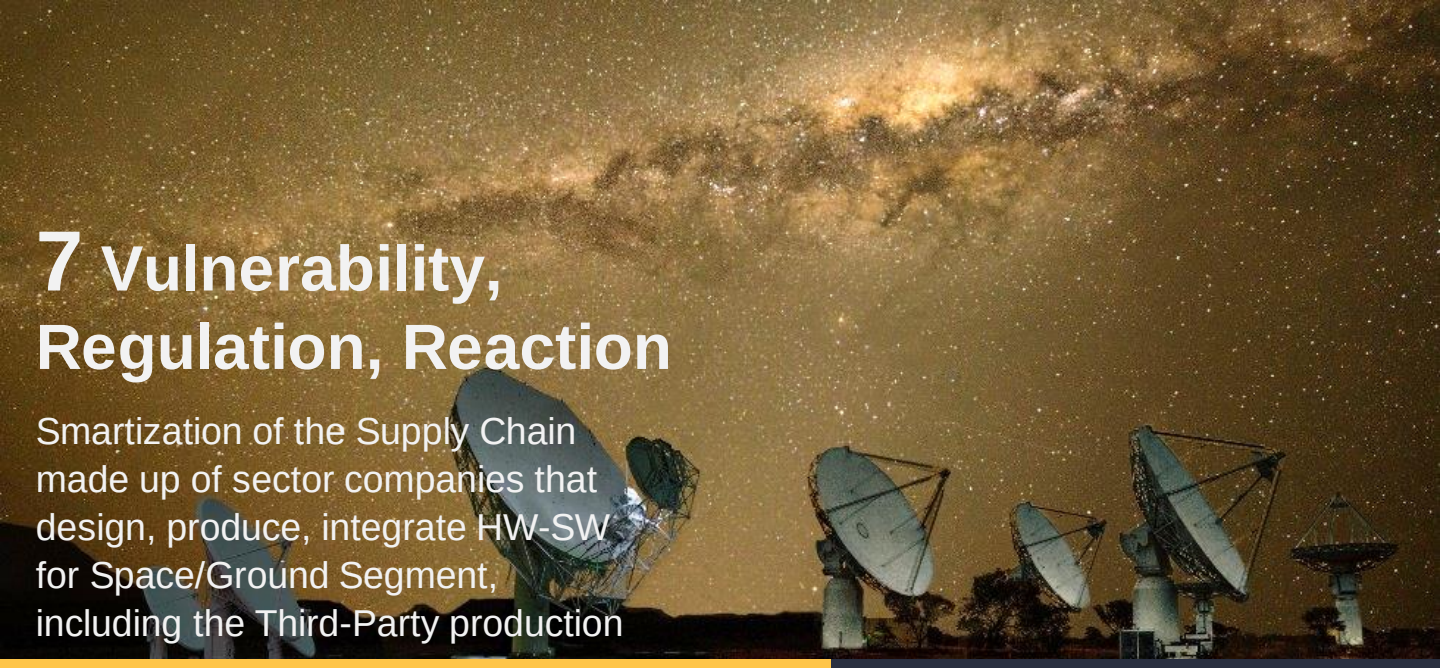
Physical Vulnerabilities

Physical Attack of Ground/Space Segments, Orbital Impact and Debris in the Space Segment (Large Constellations i.e. SpaceX Starlink)

Increasingly complex Topological-Orbital Dynamics will imply an evolution in the security of UpDownLink and ISL Protocols (worked at OSI level on MAC and Routing according to parameters that depend on the Mission), generally lighter than traditional ones in terms of power and memory consumption with an increase in transmission speed

i.e. Multi-Orbit, In-Flight Flexible Payload, Space-Time dynamic routing, Collaborative-Autonomous formation flying (Rendezvous & Docking, Constellation, Swarms, Formation Flying come Trailing, Cluster, Leader-follower,..)

GORDIONET NESECON SAFE DIVE INTO THE NET



7 Vulnerability, Regulation, Reaction

Smartization of the Supply Chain made up of sector companies that design, produce, integrate HW-SW for Space/Ground Segment, including the Third-Party production

Satellites are equipped with security measures against attacks, and gaining control of the Onboard-Payload systems, exploiting SW vulnerabilities, modifying their orbit, violating TT&C channels, requires considerable skills, knowledge, tools-systems.
Therefore the major vulnerabilities are concentrated in the Ground-Terrestrial Segment, Supply Chain of Ground/Space Segment, User Segment

Rapidly evolving scenarios with national, European and international regulations, among which dominate the NIS2 and NISTIR 8276 Directives monitored by ENISA, which imply the compliance by large-medium critical-strategic companies in the Space Sector, the non-compliance of which entails heavy administrative or criminal sanctions

Management and Awareness, Reporting to Authorities (Reporting & Collaboration), Risk and Incident Management (Company and Supply Chain Security), Business Continuity (NIS2 Articles 49 and 89, etc.)

EXAMPLES OF SUPPLY CHAIN ATTACKS
Browser-based - Software - Open-source - JavaScript - Magecart Formjacking - Watering hole - Cryptojacking

MAIN REACTIONS

- Vulnerability Scanning
- Encryption, Authentication, Access Control, Revocation
- Secure Protocols
- Network Segmentation
- Browser Isolation
- Routing and Distributed Control
- Redundancy and Backup Systems
- Timely Security Updates
- DoS Prevention-Prediction-Mitigation
- Anomaly Detection and Intrusion Prevention
- Zero-Trust per Zero-Day
- Malware Detection and Blocking
- Detect Shadow IT or CASB Cloud Access Security Broker with Shadow IT detection
- Secure Supply Chain Management and Third-Party Vendor Assessment (can include CSP Content Security Policies or SRI Subresource Integrity to check suspicious content on JavaScript)
- Regular Audits and Testing
- Incident Reporting and Response
- User Education
- Regular Security Training

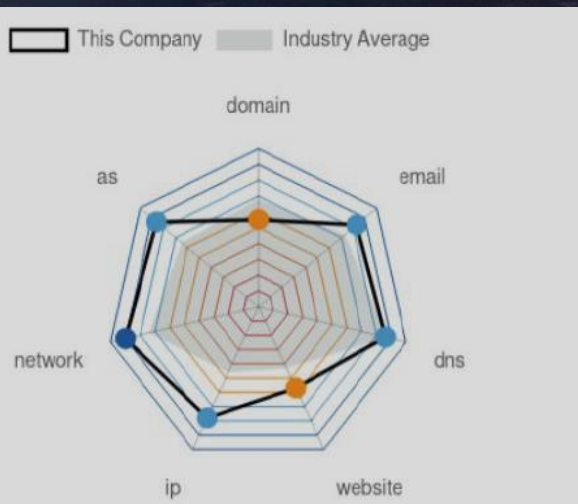
GORDIONET NESECON SAFE DIVE INTO THE NET

8 Nesecon's modular proposals

GROUND-TERRESTRIAL SEGMENT
SUPPLY CHAIN GROUND/SPACE
USER SEGMENT

PREDICTION - PREVENTION

- Auditing - Assessment of the Network, Data Protection Processes, HW-SW Production-Integration Chain
- Risk and Vulnerability Analysis Tools Services with Rating Report
- Third-Party Auditing - Assessment
- Training on Data Protection Processes



DETECTION - RESPONSE

- Analysis and supply or Support for the purchase and configuration of tested Solutions of OnPrem/Cloud Network-Cloud/Web-Endpoint Security, Business Continuity, Data Recovery, Backup-Storage
- Training On-the-job of the Solutions

Partnerships & Alliances

Microsoft · vmware by Broadcom · cisco · cisco SECURE · TALOS · CHECK POINT · open-appsec · PROXMOX · veeam · Synology · N-ABLE · dataprobe · Cove Data Protection · stratodesk · NComputing · GORDIONET

Constant Touch
info@gordionet.com
info@nesecon.com
nesecon.com
ServiceOnFarm

NESECON SKILLS - COMPETENCES

- DPO, CIO, CISO Certifications-Functions
- Multi-Hypervisor / Multi-Containers Engine Virtualization
- Security Protocols-Rules-Privileges IPsec VPN and SSL VPN on both Terrestrial and Satellite Networks
- Firewalling - Switching - Routing Integration
- IaaS CSP Cloud Service Provider and NOC Services, Business Continuity, Disaster Recovery, Backup-Storage, CyberProtection, with GDPR e ISO 27001 compliance
- VAS Value Added Service
- MSSP Managed Security Service Provider
- Cisco Partner-Networker certification with international Case Studies
- Projects - Contracts for Enterprise, PMI, Finance, Insurance, Utilities-ESCO, Healthcare, Manufacturing, Verticals segmentations