



SCUT
SECURITATE CIBERNETICĂ UNIFICATĂ

Your Partner in Unified Cybersecurity

www.SCUT.com



Who We Are and What We Do

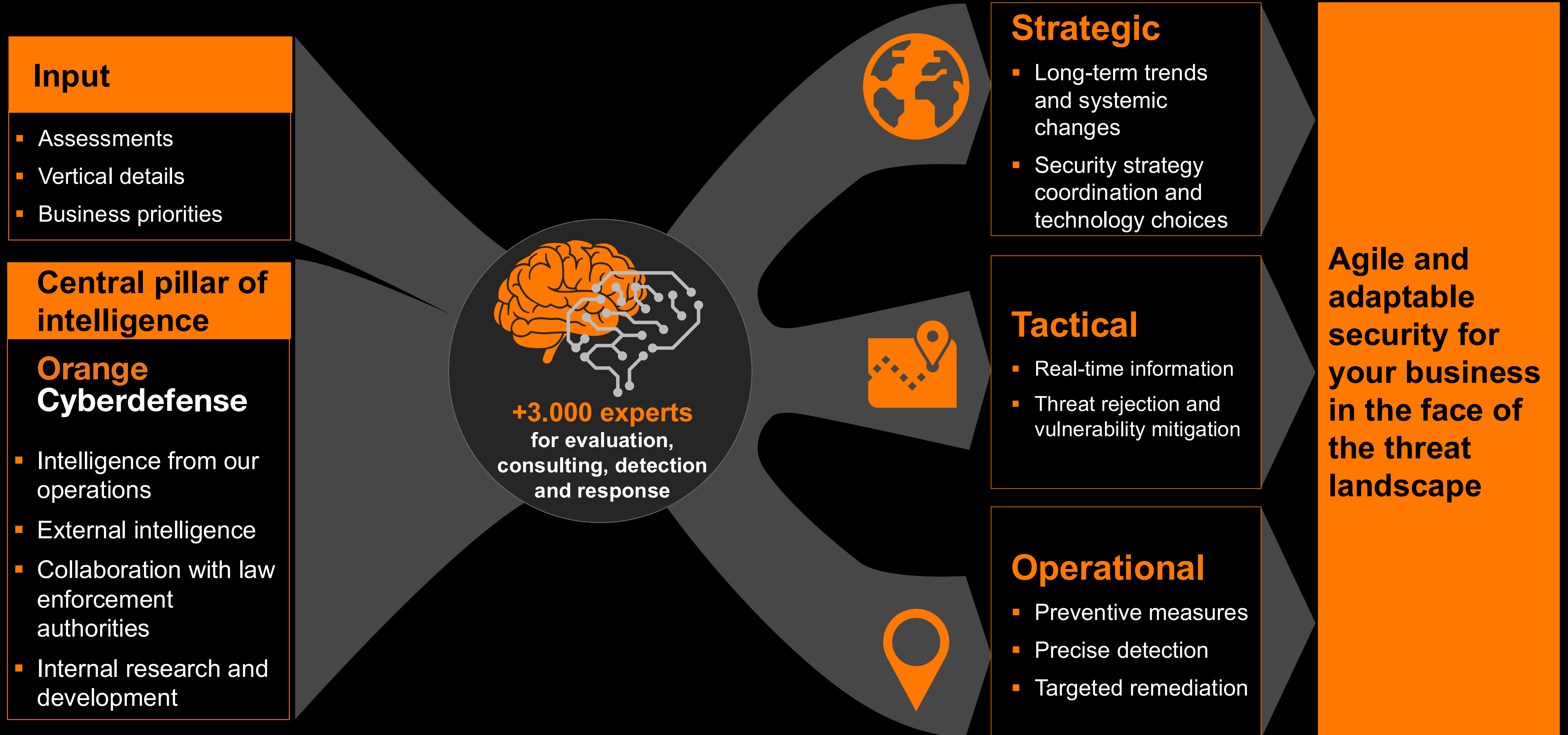


- ◆ we are a team with over 20 years of experience in cybersecurity, strengthened through the strategic partnership with Orange Romania and Orange Cyberdefense, the European leader in cybersecurity
- ◆ we ensure operational continuity and digital security for your business
- ◆ we identify and neutralize threats before they cause impact
- ◆ we offer integrated and unified cybersecurity solutions, tailored to your organization's needs



Orange Cyberdefense

Recognized market leader



Orange Business in Romania

Fiber & mobile
network **#1**

for businesses built with
passion

~ 200k Companies
~ 2m Fix & Mobile Devices

95% potential

IoT & Smart Cities

>30 projects
smart city

□ 1.3m connected devices
(industrial & medical sensors,
PoS, vending machines, smart
meters, etc.)

LoRaWAN
LTE-M
NB-IoT

Data Centers & Cloud

7 Data Centers

- 2x Bucharest
- 2x Cluj-Napoca
- 2x Braşov
- 1x Timișoara

Expertise

>75
IT&C Experts

with a total of
490 certifications from
27 technology partners

IoT Security

Cloud Security

Revenue +25% per year
cybersecurity

Network Security

The added value of SCUT for Your Business's Unified Cybersecurity



Highest level protection and complete visibility
over the company's digital infrastructure



Prevention, detection and real-time response to cyber attacks



Legal compliance with legal standards such as NIS2 and GDPR



Local support in Romanian and specialized consulting



Innovation and AI technology for proactive and efficient security



Flexibility and customization for any size and industry
(co-creation)



Why Do We Need Unified Cybersecurity?

Fragmented Security

The overlap of over 6 security tools (antivirus, firewall, VPN, MDM, email security, application protection) creates operational burden and slows threat detection or response.



Exceeded Perimeter

In the last 10 years, with migration to cloud and remote work from anywhere in the world, the attack surface has expanded, exceeding the old perimeter formed by Intranet, DMZ and Internet.



Vulnerable APIs

They become entry or exfiltration channels if not protected and monitored.



Vulnerable Supply Chain

Third-party collaborations create value but increase vulnerabilities. Protection requires risk assessments, shared policies, and regular audits across the supply chain.



Legislative Compliance

NIS2, DORA
require strong governance and rapid response.



Vulnerable Identities

The number of non-human identities (services/automation/bots) exceeds that of users, increasing the risk of unauthorized access.



Slow Detection

Without 24/7 real-time detection and rapid response, incidents can cause significant damage.



Hybrid Data

Unified data governance is required.



AI-powered analysis
Rapid response

We activate the **cyber shield** for companies in **Romania.**

Infrastructure Security

Powered by  **Business**

- BIS Business Internet Security
- DDOS
- WAF Web Application Firewall
- SOC

Managed Detection and Response

Secured by  **Cyberdefense**

- Continuously updated threat intelligence
- Best EDR + XDR technologies
- Monitoring 24/7
- AI-powered analysis
- Rapid response

Assessment

- Vulnerability Assessment,
- Cyber Risk Assessment,
- Threat Hunting

Active Protection

- MDR
- Security Platforms Management

Attack Response

- SCUT Cyber Attack Assistance
- MDR
- Cyber Risk Assessment

Compliance

- NIS2 Consulting
- Virtual BISO
- Vulnerability Management



Energy

Financial
Sector



Transport

Public Sector



IT, Telecom

Healthcare



Retail

Manufacturing



Managed Detection & Response (MDR)

Complete Visibility. Rapid Action. Controlled Response.

Secured by



Continuous Monitoring and Rapid Response

- top EDR technologies (CrowdStrike, SentinelOne) and the Sekoia XDR platform are used for automatic correlation of alerts across the entire IT infrastructure.

Globally Recognized EDR

- award-winning and certified solution in Gartner rankings, for next-generation detection and response.

Advanced XDR Platform

- provides extended visibility and multi-cloud integration, for complete and coherent protection.

Updated Threat Intelligence

- daily data from regional and international sources, for proactive detection of real threats.

Certified Local Analysts

- dedicated team with practical experience, ready to respond quickly to any incident.





NIS2 Consulting

Simplified Compliance, with Expert Support



Technical and Organizational Controls

implementation of policies, processes and minimum measures necessary for managing cyber risks.



Incident Reporting

transmission of notifications for significant incidents: 24h initial notification, 72h update, 1 month final report.



Supplier Requirements

continuous evaluation and monitoring of critical suppliers to reduce supply chain risks.



Continuity and Audit

ensuring incident response plans, periodic testing and maintaining updated documentation for audit.



Virtual BISO

Your digital
cybersecurity
consultant

Internal Security Assessment

We analyze the current maturity of systems and processes to identify vulnerable points.

Regulatory Alignment

We provide end-to-end support for compliance with NIS2, GDPR, and ISO/IEC 27001.

Vendor & Supply Chain Assessment

We verify partners and supply chain for cybersecurity risks.

Policy & Procedure Updates

We review and adapt security documentation based on current requirements and risks.

Phishing Training & Simulations

We develop training programs and practical exercises to increase awareness levels.

Incident Response Support

We coordinate incident response, communications, and the necessary corrective actions.

Cyber Risk Assessment

Cyber Risk Assessment for Critical Projects

- ◆ **Complete Risk Register** – you have an updated record of all identified risks, organized by categories and severity.
- ◆ **Phased Action Plan** – we establish concrete measures, deadlines and clear priorities for reducing identified critical risks.
- ◆ **Pragmatic Recommendations** – we offer technical and organizational solutions immediately applicable, adapted to your company's context.
- ◆ **Clear Executive Reports** – structured documentation for board and audit, with management summary and relevant technical details.
- ◆ **Standards Alignment** – results compliant with NIS2, ISO 27001 and GDPR regulations requirements.





SCUT

Post-Cyber Attack Support

Rapid Intervention, Complete Analysis and Safe Recovery

- ◆ **Rapid Recovery** - restore normal system functioning and significantly reduce downtime.
- ◆ **Avoided Losses** - prevent costs associated with attacks. From financial damages to reputation losses.
- ◆ **Legal Compliance** - comply with legal requirements regarding incident reporting and prompt response according to NIS2/GDPR.
- ◆ **Consolidated Trust** - demonstrate to partners and clients that your organization professionally manages cyber incidents.
- ◆ **Certified Expertise** - access accredited specialists and standardized procedures for analysis, response and remediation.

+30%

Ransomware attacks are increasing year over year, and full compromise can occur within hours.

70%

of attacks are detected by third parties, not by the affected company;

Threat Hunting

Search for Hidden Threats Undetected by Security Systems



1

Local Expertise, European Context:

indicators are based on real attacks observed both in Romania and Central Europe.

2

Dedicated Team:

Certified analysts with practical experience in real investigations and complex compromise scenarios.

3

Recognized Methodology:

We follow established international standards: NIST, MITRE ATT&CK and SANS.

4

Total Complementarity:

Works perfectly alongside MDR and SCUT Cyber Attack Assistance, closing visibility gaps.

5

Clear Reports:

Results are presented in a way everyone understands, from IT teams to management.

6

Cost Efficient:

Enterprise-level services, also adapted for SMEs, with excellent cost-benefit ratio.

Vulnerability Assessment

Evaluate, prioritize and resolve vulnerabilities before they become incidents.

Proactive Identification

Discover real risks early and see where problems can arise before they affect systems..



Operational Continuity

Avoid unexpected interruptions and blockages, maintaining IT infrastructure performance and stability.

Reduced Cyber Risk

Reduce exposure by up to 90%, quickly remediating critical vulnerabilities identified in infrastructure.



Regulatory Compliance

Results are aligned with NIS2, ISO 27001 and GDPR requirements, simplifying audit processes.

Optimized Costs

Prevention is significantly more affordable than recovery after a major cyber incident.



Consolidated Trust

Demonstrate to clients and partners that security is a strategic priority for your company.

Vulnerability Management

AI-based prioritization which enables faster remediation and keeps operations stable.

Accelerated Remediation

Reduce response time by up to 80%, thanks to automatic vulnerability prioritization.

Total Visibility

You gain full 24/7 visibility and control over your infrastructure and all critical IT assets.

Reduced Costs

You reduce post-incident financial impact by up to 60%, according to BIS 2025 data.

Ensured Compliance

You maintain continuous alignment with NIS2, GDPR, and ISO/IEC 27001 requirements—without additional effort.

Informed Decisions

You access clear, up-to-date dashboards that enable fast, data-driven management decisions.



85%

of attacks exploit vulnerabilities known for over 6 months.

**23.000+
new vulnerabilities
emerge every year
(NIST 2024).**

**70%
of organizations have
over 1,000
uncorrected
vulnerabilities**

Security Platforms Management

Unified Protection, Validated Technology, Continuous Operation



Globally Validated Solutions

Internationally recognized technologies, used by organizations in critical and regulated sectors.

Modular and Scalable Delivery

Each component can be implemented separately or gradually expanded, depending on company needs.

Professional Implementation and Integration

We ensure correct configuration and native integration with existing infrastructure, without operational interruptions.

Compliance Support

We facilitate alignment with standards such as NIS2, ISO 27001 and GDPR, with simplified audit and reporting.

Unified Security

A defense-in-depth approach that protects all layers—from endpoint to cloud.

Centralized Administration

Complete management with continuous monitoring and optimization.



SCUT
SECURITATE CIBERNETICĂ UNIFICATĂ

We Activate the Cyber Shield for Your Business

www.SCUT.com

