



CyberArts™

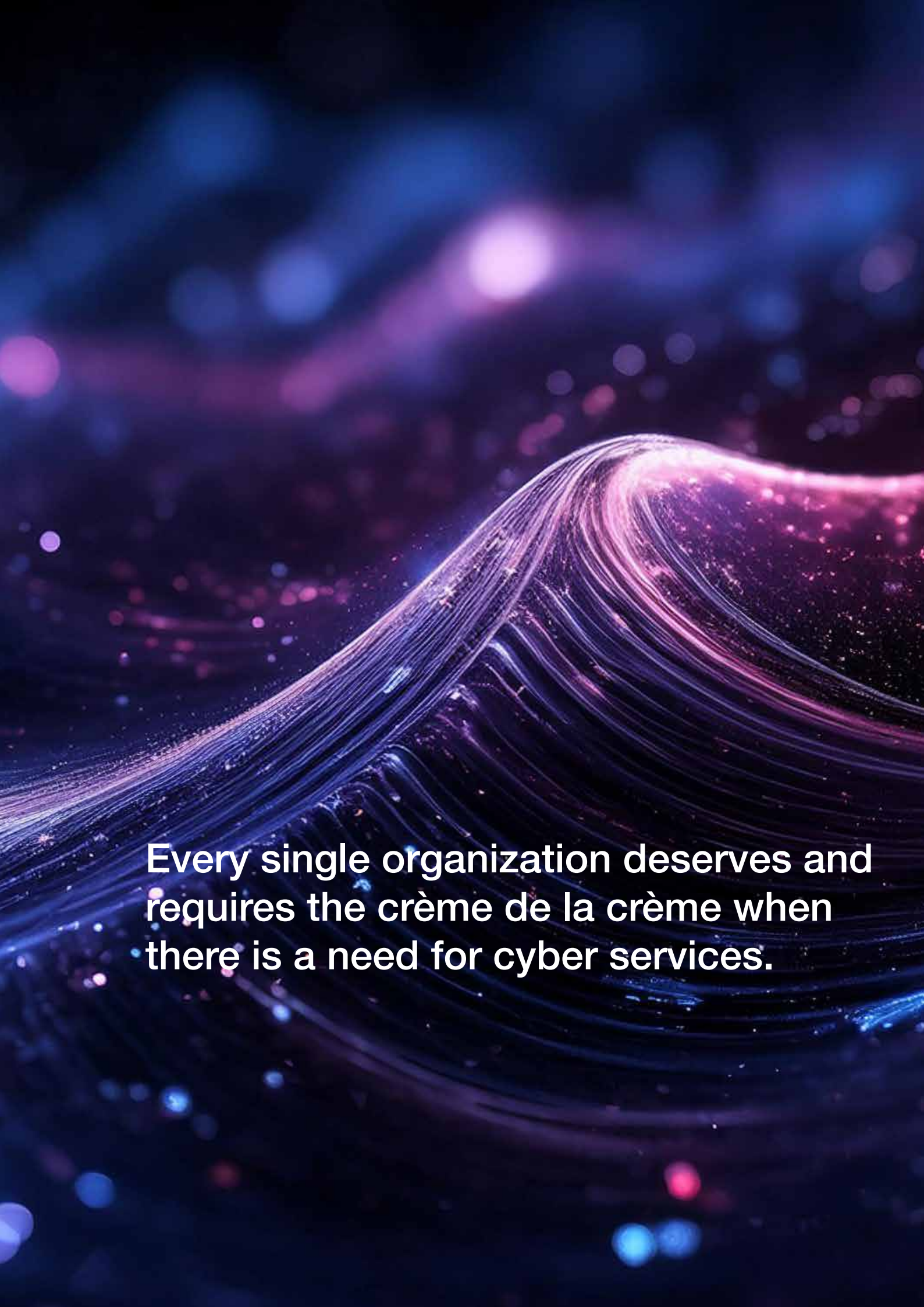
*Whatever we provide, we make sure
the “art” is always within!*



cyberartspro

CyberArts Philosophy

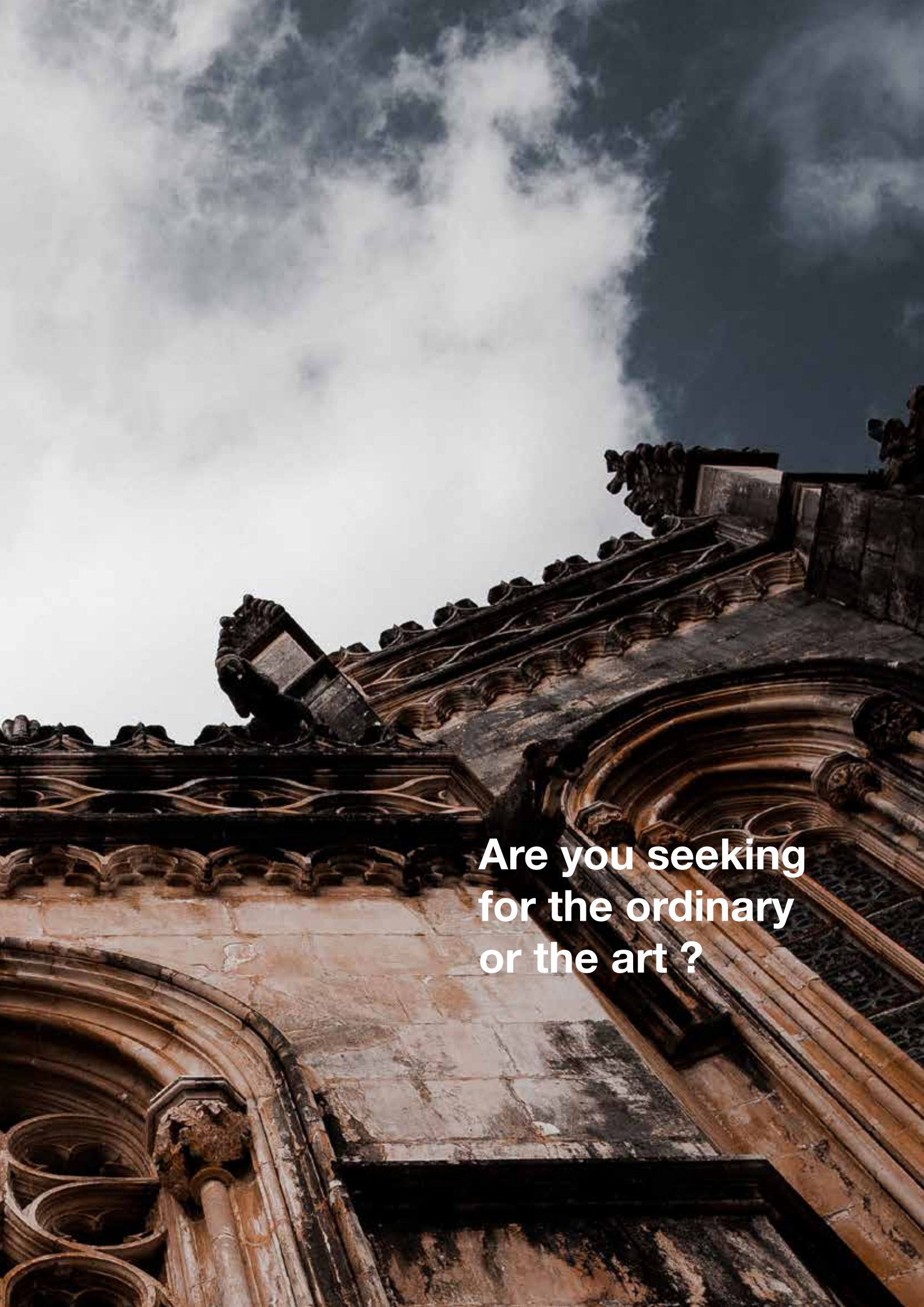




Every single organization deserves and requires the crème de la crème when there is a need for cyber services.

We are providing art for organizations who demand art not the ordinary, through utilizing other organizations and people, who work with artistic elegance and attention.

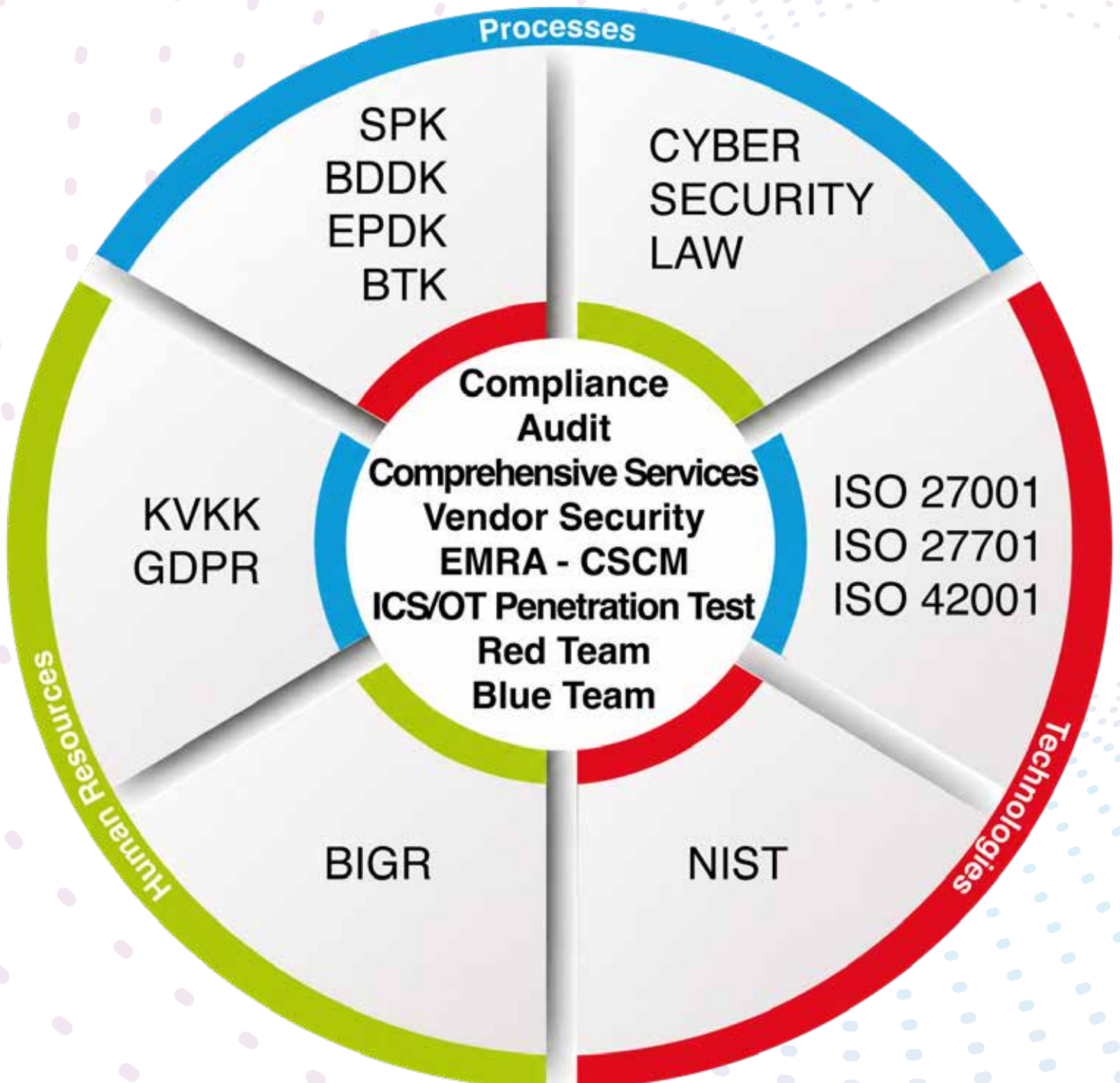




**Are you seeking
for the ordinary
or the art ?**

GRC ARTS

Bringing together the disciplines of Law,
Cyber Security and Governance for Sustainability.



CYBERSECURITY PRESIDENCY AND THE CYBERSECURITY LAW

The Cybersecurity Presidency, established on January 8, 2025, under the Presidency of the Republic of Türkiye, has been strengthened by the Cybersecurity Law No. 7545, which entered into force on March 19, 2025.

Criminal Sanctions;

In case of non-compliance with obligations, imprisonment up to 15 years and monetary fines up to 5% of annual gross sales revenue are possible.



Holistic Cybersecurity Packages

“All the essential services you need
for 12 months, all in one”



From Paper Compliance to Real Security:

Integrated Information Security and Cybersecurity Maturity Management

Our solution combines strategic goals and compliance requirements such as ISO 27001 or KVKK (GDPR) with concrete evidence from technical operations like Penetration Testing (Pentest). This provides you with a risk-oriented, measurable, and sustainable roadmap.

Why Integrated Approach?

In traditional methods, IT, Legal, and Internal Audit units usually operate in disconnected silos.

This situation leads to three main problems:

- Fragmented Perspective
- Static Reports
- Incorrect Prioritization

Scalable Solutions Tailored to Needs

Regardless of your organization's size and current maturity level, we have defined a suitable and actionable roadmap for you.

- Core Compliance and Awareness (Beginner Level)
- Corporate Transformation (Intermediate Level)
- Corporate Maturity (Advanced Level)
- Incorrect Prioritization

How Do We Work? Integrated Management Cycle

Our service is not a one-time project, but a continuously improving cycle; We design a GRC control tree aligned with your corporate objectives, measure your current status through risk analyses and penetration testing, and provide a prioritized roadmap to close gaps by mapping findings to business processes and risks.

The Result: A Living Security Program

Cybersecurity is a journey, not a destination.

With our "Integrated GRC and Cybersecurity Maturity Management" service, we create a tailor-made Dynamic Risk and Maturity Register for your organization, transforming security from a reactive obligation into a proactive business advantage.

EMRA SGYM AND ICS PENETRATION TESTING IN THE ENERGY SECTOR

The Energy Market Regulatory Authority (EMRA / EPDK) has implemented two fundamental and mandatory regulations to protect critical infrastructures;

1. Regulation on Cybersecurity Competency Model (SGYM) in the Energy Sector
2. Procedures and Principles for Security Analysis and Testing of ICS Used in the Energy Sector

These regulations are no longer a recommendation for energy companies, but a necessity for operational continuity and national security.

OUR EMRA COMPLIANT SERVICES

1. SGYM Consultancy and Sectoral Audit Services
2. EMRA Compliant ICS/OT Penetration Testing and Security Analysis
3. Risk Assessment and Action Plan Reporting

OUR EMRA COMPLIANT ICS PENETRATION TESTING METHODOLOGY

1. Network and Architecture Review: Mapping the Attack Surface
2. Social Engineering: Testing the Human Factor
3. Vulnerability Scanning: Silent Detection of Vulnerable Points
4. Malware Analysis: Anomaly Hunting
5. Wireless Network Testing: Invisible Attack Channels
6. Exploitation Testing: Seeing the Real Impact of the Vulnerability



COMPLIANCE CONSULTANCY



Improvement and Certification

- Improving and Updating Controls
- Certification Readiness Checks

Application

- Implementation of Controls
- Policies and Procedures

Organization

- Identifying teams that initiate adaptation processes
- Determination of Roles and Responsibilities

Control and Audit

- Internal Audits
- Supplier Audits
- Review

Planning

- Asset Groups
- Current Situation & Targeted Situation
- Gap Analysis
- Application Roadmap

AUDIT

Planning

- Determination of the Audit Team
- Understanding the Organization
- Examination of the Processes
- Determining the Scope of audit
- Establishing the Audit Program

Application

- Application of Audit Methods
- Gathering Audit Evidence
- Evaluating the Effectiveness of Implementation Process
- Evaluation of the Effectiveness of Measures
- Detection, Evaluation and Monitoring of Findings

Reporting

- Preparation of the Assessment Report
- Reporting Findings
- Determining People, Process and Technology Requirements
- Assessments regarding Maturity Level
- Solution Offers
- Integrated System Inputs

SUSTAINABILITY CONSULTANCY

Monthly Activities

- Follow-up Management of Corrective Actions
- Bulletins
- Support for Implementing Controls
- Tracking and Management of Incident Violations

Six Monthly Activities

- Updating Asset Inventory
- Risk Analysis and Gap Analysis Review
- Reviewing Information Security Measures and taking a

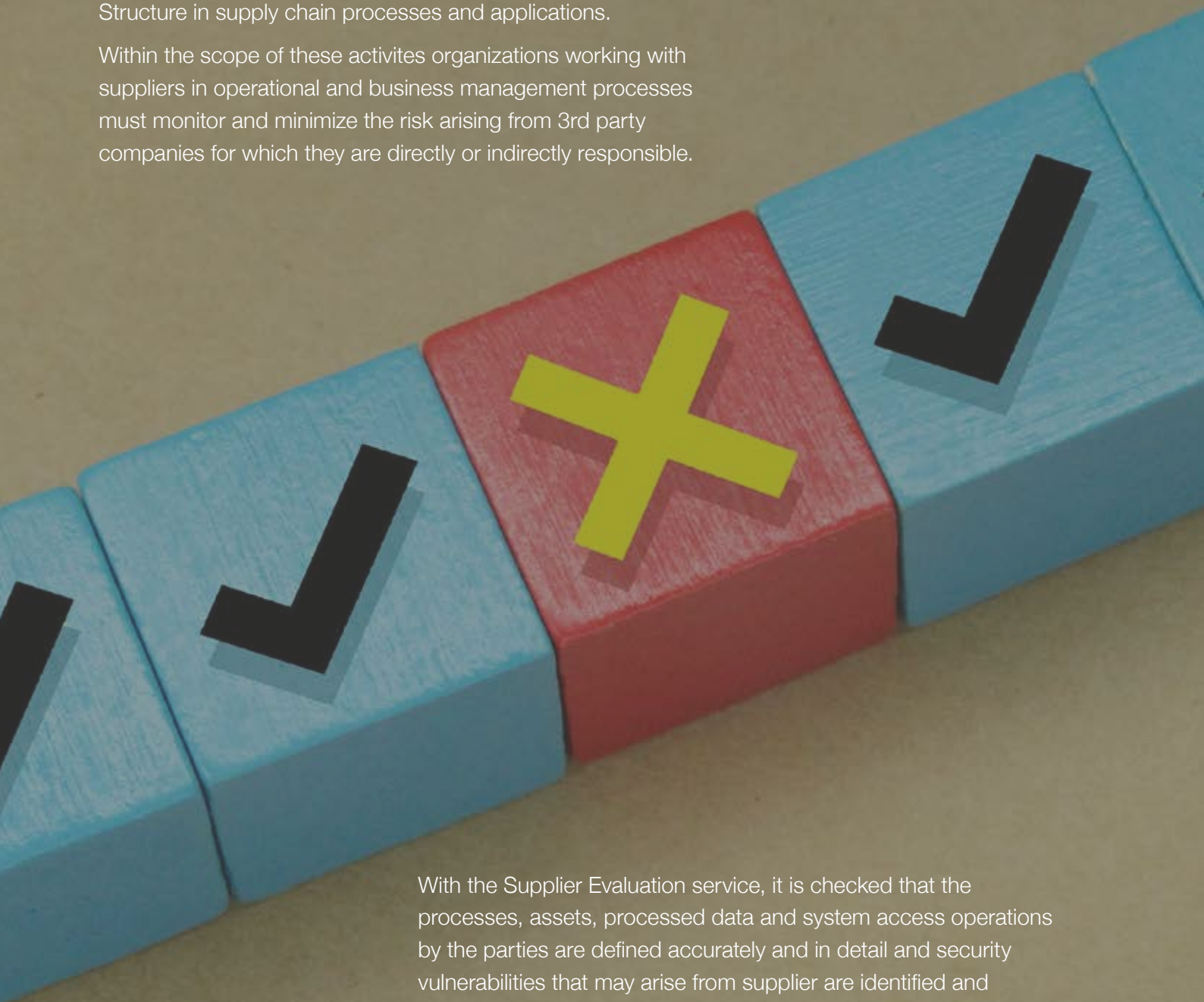
Annual Activities

- Audit and Certification Preparation
- Awareness Training
- Updating Policies & Procedures
- Internal Audit & Supplier Audit
- Participation in Senior Management Meetings

SUPPLIER EVALUATION

Supplier Evaluation (Audit and Assessment) in IS activities aim to take Information Security Measures and create a Secure Structure in supply chain processes and applications.

Within the scope of these activities organizations working with suppliers in operational and business management processes must monitor and minimize the risk arising from 3rd party companies for which they are directly or indirectly responsible.



With the Supplier Evaluation service, it is checked that the processes, assets, processed data and system access operations by the parties are defined accurately and in detail and security vulnerabilities that may arise from supplier are identified and solutions for these vulnerabilities are proposed.

Supplier Evaluation services enable the prevention of data, service, operations, workforce, time, reputation and financial losses and legal sanctions originating from the supply chain.

Cyber Security Arts

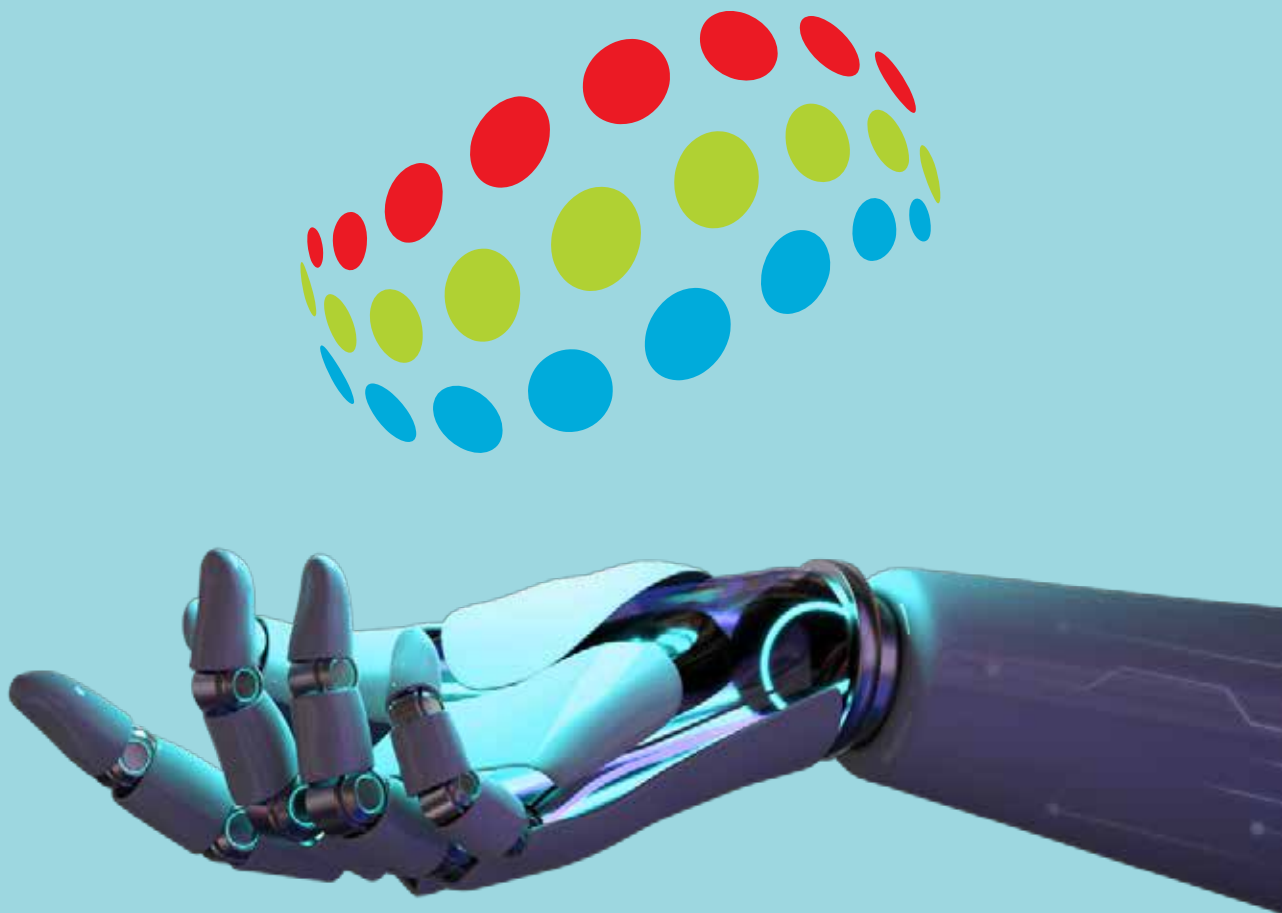
Get your guard with CyberArts.

MSSP Services

- Penetration Testing and Vulnerability Analysis
- Cyber Drill
- Cyber Crisis Management
- Cyber Threat Intelligence
- Incident Response and Forensic Analysis
- Compromise Assessment
- Phishing Simulation
- Information Security Audit
- Cyber Security Trainings
- Selection, Installation and Support of Technologies
- Integration with existing solutions
- Monthly Evaluation Meetings and Reporting



**We implement the next generation
smart technologies that provide
solutions for today's complex threats,
and we are providing an end-to-end
complementary portfolio.**





INFRASTRUCTURE AND NETWORK SECURITY

- NDR
- NAC
- SD-WAN
- Firewall
- ZTNA
- Active Directory
- HSM
- Crypto Systems
- Secure Gateway Systems
- ECS Security

END-POINT PROTECTION

Server

Tablet

Laptop

Mobile Phone

AV

EDR

MDR

EPP

XDR

Virus

Malware

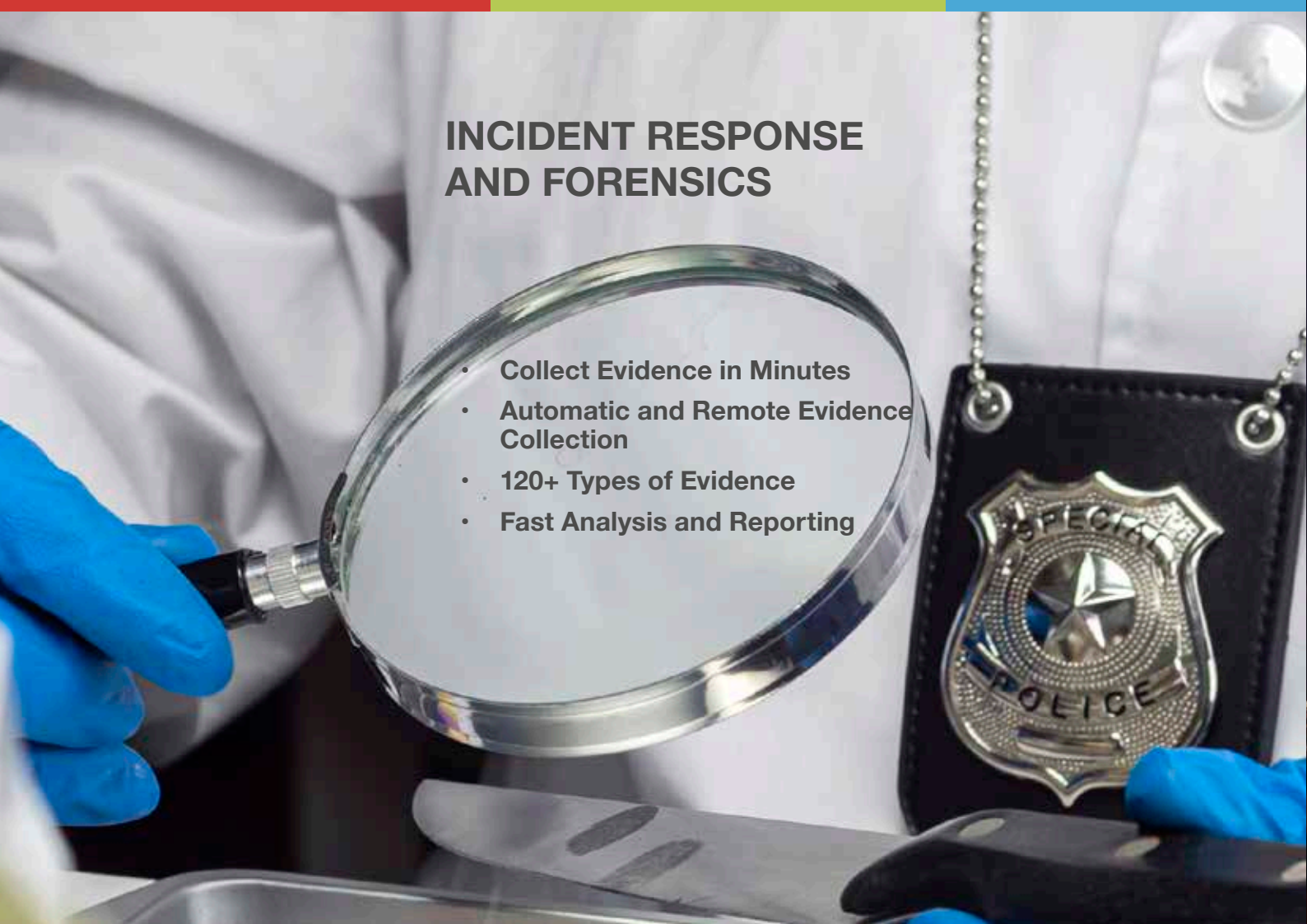
Spyware

Ransomware



DATA SECURITY

- Data Encryption
- Database Security
- Data Leak Prevention (DLP)



INCIDENT RESPONSE AND FORENSICS

- Collect Evidence in Minutes
- Automatic and Remote Evidence Collection
- 120+ Types of Evidence
- Fast Analysis and Reporting

SECURITY INFORMATION EVENT MANAGEMENT (SIEM)

- Big Data Analysis
- Proactive Cyber Security
- Behavior Analysis with Artificial Intelligence

SECURITY ORCHESTRATION AUTOMATION & RESPONSE (SOAR)

- Harmony & Control over Security Infrastructure
- Comprehensive & Simultaneous Incident Response



WEB SECURITY

- WEB Application Firewall (WAF)
- Intrusion Prevention System (IPS)
- Intrusion Detection System (IDS)
- Distributed Denial of Service (DDoS)
- DNS Security

CYBER THREAT INTELLIGENCE (CTI)

- Fraud Abuse & Phishing Tracking
- Brand Protection
- Deep Web/Dark Web/Social Media Monitoring

THREAT SIMULATION

- Detecting Security Vulnerabilities
- Continuous Threat Analysis
- Attack Surface Management (ASM)
- Breach Attack Simulation (BAS)

APPLICATION SECURITY

- Zero Trust Architecture
- Secure Access Service Edge (SASE)
- API Security
- Sandbox



MOBILE SECURITY

- Bring Your Own Device (BYOD) Risk Management
 - Mobile Phone Loss Scenarios
 - App Shielding
 - Mobile Device Management (MDM)
 - Mobile Application Management (MAM)



SECURE COMMUNICATION

- Webinar
- Video Call DESK TELEPHONE

DESK TELEPHONE

VOIP

IP

BACKDOOR

THREAT

MANAGEMENT INFORMATION SYSTEMS

- Governance and Audit
- Risk Analysis
- Compliance Management

PHYSICAL IDENTITY & ACCESS MANAGEMENT

- Smart Access Card
- Biometric Verification
- Body Language Analysis



DIGITAL IDENTITY AND ACCESS MANAGEMENT

- Passwordless Architecture
- BIOS Encryption
- Artificial Vision
- AM - Privileged Access Management
- IAM - Identity and Access Management
- MFA - Multi-Factor Authentication



REMOTE IDENTITY AUTHENTICATION & ACCESS PACKAGE

Remote Biometric Authentication

- Biometric Verification Success Rate : 99.614%
- Using Vector Information (HASH)
- Encrypted Security in Blockchain Architecture
- Mobile, Web, Cloud Framework
- NFC, OCR, MRZ compatible
- Adaptive API/SDK
- Metadata Detection and Reporting (48 types of metadata)

Passwordless MFA

- Enterprise MFA
- Single Sign-on
- Password Management
- Sharing Center
- Endpoint Access Management

Mobile App Security

- SSL Pinning
- Anti-Keylogger
- Device List
- Overlay Detection
- Anti-Malware
- Device Fingerprinting
- Central Management Console
- Root/Jailbreak Detection



A blurred photograph of an orchestra performing. In the upper left corner, a conductor's baton is visible, pointing upwards. The background is dark, and the musicians are out of focus, with their hands and instruments (like flutes and violins) visible. The text is centered in the lower half of the image.

*Whatever we provide, we make sure
the “art” is always within!*



CyberArts™

Corporate Certifications



Team Certifications



Information and Communication Security Auditor D1



Information and Communication Security Auditor D2



CompTIA Security+



CRTP



CRTO



EC-Council Certified Ethical Hacker



eWPTX Certification
INE Security
INE Internetwork Expert



EMRA Energy Sector
Cybersecurity Competency Model Regulation



EMRA ICS Security
Analysis & Testing



ISO/IEC 27001
Lead Auditor



ISO/IEC 27701
Lead Auditor



ISO 42001



MCTS



OSCP



OSCP+



PMP



Certified
Penetration Tester



MCP