



LoopTech

شركة لوب تيك للأمن السيبراني

“ أول شركة سعودية متخصصة في مجال توزيع حلول وخدمات الأمن السيبراني على المستوى المحلي والشرق الأوسط ”

Value Added Distributor⁺



VAD
Value-Added
Distributor⁺



Specialized
Techniques



Professional
Assistance



Local
Implementation



Best
Consultant
Services

NEXT GENERATION OF CYBERSECURITY

Who we are



Loopstech Co. is a trusted name in the field of cybersecurity, which has developed unique and unmatched cybersecurity solutions for satisfying its clients needs all over GCC Countries and Middle East.

The primary aim of **Loopstech** Co. is to raise the level of cybersecurity among government agencies as well as private sector companies with a clear vision that is inclined towards minimizing cybersecurity threats and maximizing confidentiality, integrity and availability within an organization.

The core value of **Loopstech** Co. is distributing knowledge and expertise instead of merely focusing on cyber security services and solutions, which enable our clients to individually improve their actions, policies, and procedure, in order to reduce cyber security vulnerabilities and threats at SMB as well as enterprise level.

The vision of **Loopstech** Co. is to safeguard the global environment from continuously increasing cyber security threats, which have increased the costs of your Information security budget. For this reason, end to end cyber security services and solutions are part of the complete roadmap offered by **Loopstech** Co. to achieve your organizational objectives and business goals.

Our Services

include but not limited to:

- ✔ IT Security Services and Consultancy.
- ✔ E-mail Security Gateway Solutions.
- ✔ E-mail Archiver Solution.
- ✔ Web Application Firewall Solutions (WAF).
- ✔ Identity Access Management Solution (IAM).
- ✔ Privileged Access Management Solution (PAM).
- ✔ Network Access Control solutions (NAC).
- ✔ Public Key Infrastructure Solutions (PKI).
- ✔ Mobile Device Management (MDM).
- ✔ Next Generations Remote Access.
- ✔ Packet Capturing and Recording Solutions.
- ✔ Instant Messaging and Management Solutions.
- ✔ Infrastructures Monitoring & Detection.
- ✔ Vulnerabilities & Penetration Testing.
- ✔ Network traffic monitoring and security.
- ✔ Anti Fraud Detection and Threat Intelligence solution.
- ✔ Infrastructure Full Monitoring Solution (FMS).
- ✔ Security Information and Event Management Solution (SIEM).
- ✔ Cloud Security Solutions.
- ✔ Microgateway and Anomaly Shield.
- ✔ Data Classification.
- ✔ Secure Mobile Container.
- ✔ Unified Endpoint Management (UEM).
- ✔ Email Phishing Simulation.
- ✔ SOC Consultancy.
- ✔ Secure Web Gateway.
- ✔ Secure Video Conference.
- ✔ DMARC Protection.
- ✔ Secure File Share.
- ✔ Media Crusher Machine.





Our Vendors

AIRLOCK[®]
SECURE ACCESS HUB

LIBRAESVA

FUDO
SECURITY

essendi **it**

APPTec360[®]
Unified Endpoint Management

NACVIEW

syc **ope**

PANDORA **FMS**
ENTERPRISE

nomios

MATERNA
Virtual Solution

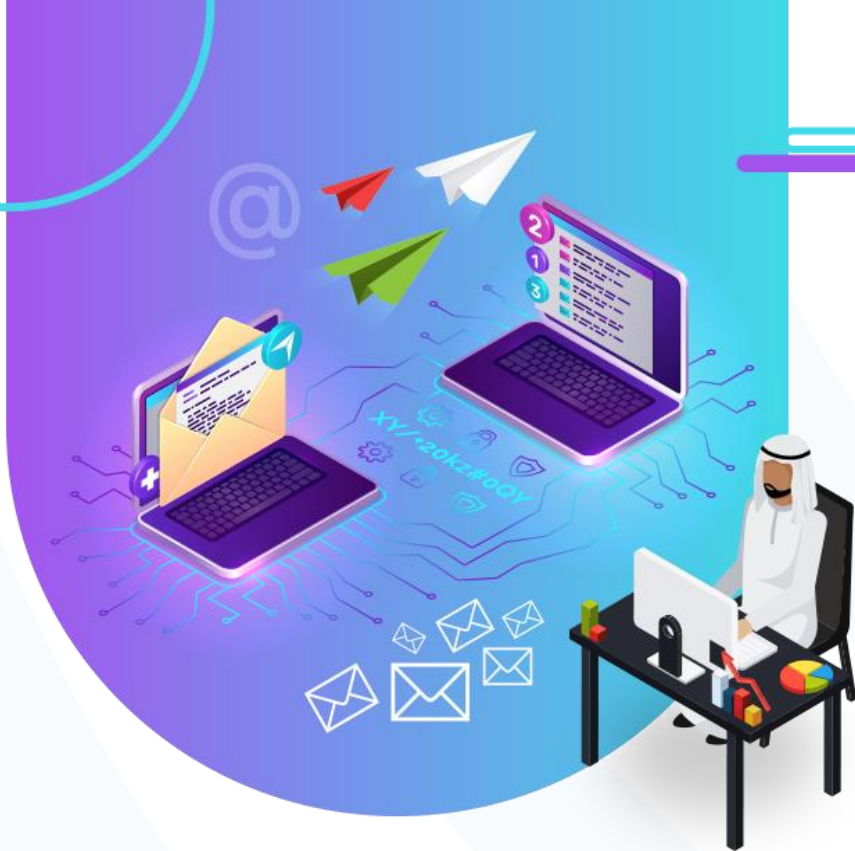
Councilbox

ecos

.Cleafy

LABYRINTH

Privacy-i



/LIBRAESVA

EmailSecurity 



WATCH VIDEO



Made in Italy

Email Security Gateway

- ❖ Multi Tenant Solution
- ❖ Real Time Protection
- ❖ File Sandboxing
- ❖ Inbound Email Protection
- ❖ Outbound Email Protection
- ❖ Multiple Engine Anti-Virus
- ❖ Anti Evasion Techniques (AET)
- ❖ URL Sandbox for Malicious URL
- ❖ ANTI (MALWARE,PHISHING,SPAM,VIRUS)
- ❖ Machine Learning Technology (ML)
- ❖ Artificial Intelligence Technology (AI)
- ❖ Multi-layer Analysis Engines
- ❖ Document Sanitization
- ❖ Risk Email Relation Assessment
- ❖ High Availability
- ❖ Support SPF, DKIM, DMARC
- ❖ Public RBL Checks
- ❖ Support IOS, Android App For End-user.
- ❖ End Users Portal
- ❖ Business Email Compromise Protection
- ❖ Email Encryption
- ❖ Recall Emails
- ❖ Outlook Add-in
- ❖ Threat Analysis Portal



/LIBRAESVA
EmailArchiver 



WATCH VIDEO



Made in Italy

Email Archiver

- ❖ Next Generation Email Archiving
- ❖ Up and Running In Minutes
- ❖ Email Import From SMTP Servers
- ❖ Multiple Storage Support: local, lan, cloud
- ❖ Folder Replication for Each Mailbox
- ❖ Enhance Mail Server Efficiency
- ❖ Native Outlook Plug-in
- ❖ Web Responsive Interface
- ❖ Quick Complex and Fast Searches
- ❖ Data Privacy
- ❖ Certified Time-stamping (RFC3161)
- ❖ Email Encryption (AES256)
- ❖ Full Management and Monitoring Interface
- ❖ Advanced Permissions for User Roles
- ❖ Approval To Access Sensitive Data
- ❖ Auditing and Anti-tampering
- ❖ Data is Stored in Standard Formats
- ❖ OTP Included
- ❖ Native Office 365 Integration
- ❖ Real Defense Against Data Loss
- ❖ On-premise
- ❖ Multi Tenant
- ❖ Full API Integration
- ❖ Security Add-in
- ❖ Advanced Retention Rules
- ❖ Arabic language Supported



/LIBRAESVA

PhishBrain 



WATCH VIDEO



Made in Italy

PhishBrain

- ❖ Real-time reporting on phishing campaign statistics and high-risk employees
- ❖ Send phishing emails all at once or distributed over a period of time
- ❖ Set a repeating schedule so employees can be tested on a regular basis
- ❖ Seamless integration with Microsoft 365®, Google Workspace and other LDAP servers
- ❖ Submit emails and websites to be converted into templates for use
- ❖ Flexible licensing (by number of mailboxes or number of email sends)
- ❖ Set up and manage campaigns from specific industries
- ❖ Multi tenant contact

USER FRIENDLY:

> using a simple and intuitive interface, anyone can configure realistic phishing simulation campaigns.

QUICKLY UP & RUNNING:

> phishing campaigns are ready to go in less than 10 minutes by easily choosing from several templates and landing pages.

BRING YOUR BRAND:

> personalize the experience with a brandable interface and fully customizable templates.

BETTER INSIGHTS:

> real-world templates and landing pages with in-depth reporting provide better insights into the most vulnerable employees.



/LIBRAESVA

LetsDMARC 



WATCH VIDEO



Made in Italy

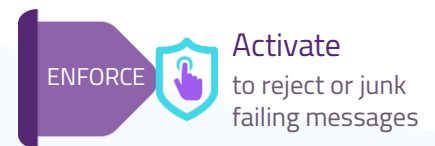
Let's DMARC

GET VISIBILITY:

- > Make sense of detailed XML RUA data sent by ISPs, with easy to comprehend dashboard visualizations.
- > Understand all the sources sending emails on behalf of your domain and identify the origin of email traffic failing authentication.
- > At a glance view of message flow over time, with email volume, pass, quarantine and reject rates.
- > Drill down explanation of authentication failure reasons.

TAKE CONTROL:

- > Manage DMARC, DKIM and SPF from an intuitive portal without needing to access your DNS.
- > Pinpoint alignment and configuration errors.
- > Intelligent "what happened" analysis provides easy to understand explanations and guidance on next steps.
- > See every change to DMARC, DKIM and SPF – as well as third-party domains included in the SPF - with before and after values tracked and highlighted in the DNS timeline.



- ✂ Guided configuration so no DNS expertise required
- ✂ Manage DMARC, DKIM, SPF from a single console
- ✂ What happened explanations to fix configurations
- ✂ Timeline provides at a glance view of DNS changes
- ✂ Smart alignment analysis to identify errors
- ✂ Automatic RUA report parsing and aggregation
- ✂ Dashboard insights with visibility of email flow
- ✂ SPF flattening to overcome 10 record limit
- ✂ Bring your brand personalize the UI
- ✂ DNS monitoring tracks every DMARC, DKIM, SPF change

WHAT THREATS DOES DMARC PROTECT AGAINST?

Without DMARC, spoofer can steal personally identifiable information (PII) by sending emails that appear to originate from your domain. They do this by falsifying the header "from" address – that's the one visible in the From: field.



Domain Security



EMAIL DELIVERABILITY



BRAND REPUTATION PROTECTION



GUIDED CONFIGURATION



UNLIMITED SPF

AIRLOCK[®]
SECURE ACCESS HUB



WATCH VIDEO



Made in Switzerland

WAAP "Web Application & API Protection"

- ❖ Advanced Web Application Firewall
- ❖ Load Balancer
- ❖ Reverse Proxy
- ❖ Webroot Integrated
- ❖ Integrated IAM & 2FA
- ❖ API Gateway Protection
- ❖ Top 10 OSWAP
- ❖ Filtering (Attack blocking)
- ❖ Fraud Detection
- ❖ Threat Intelligence
- ❖ Rapid Deployment – DevSecOps
- ❖ Reporting & Monitoring
- ❖ SIEM Integration
- ❖ Virtual Patching
- ❖ Learning Mode for Easier Administration
- ❖ MS Applications



Micro gateway



DevOps



API Protecting



Zero Trust



AIRLOCK®
SECURE ACCESS HUB



WATCH VIDEO



Made in Switzerland

2FA "Two Factor Authentication"

✦ Authentication and Transaction Approval

✦ Appropriate Authentication Means for Every use case:

- > Zero-Touch
- > One-Touch
- > Offline QR-Code
- > Passcode
- > Hardware Token Option

✦ Optimized User Experience:

- > Self-migration by The User
- > Self-management by The User

✦ Minimum Time to Market:

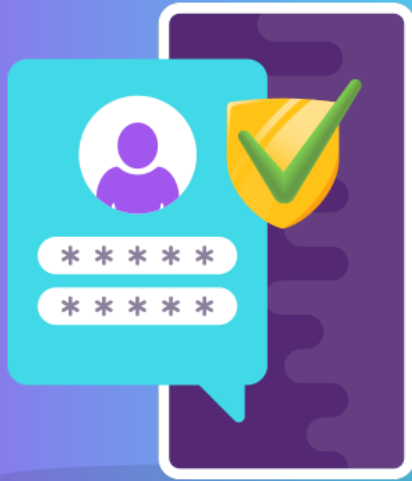
- > Ready-to-use Mobile App for IOS and Android
- > No Integration Effort

✦ Simple adaption to business requirements:

- > White Labeling of Mobile Apps und login portals
- > SDK for Deep Integration
- > REST APIs for Authentication and Management

✦ Operation:

- > Helpdesk and Admin-tool
- > REST API
- > Reporting and User-trail Logs



AIRLOCK[®]
SECURE ACCESS HUB



Made in Switzerland

IAM "Identity Access Management"

❖ User authentication :

- > Password authentication.
- > Wide spectrum of authentication methods for strong authentication.
- > X.509 client certificate.
- > RADIUS server.
- > Adaptive and risk-based.
- > <Remember Me>.
- > Workflow-based.

❖ Request authentication :

- > Authentication of REST calls.
- > JWT, Basic Auth, Client certificate.

❖ User self-services :

- > Password-reset.
- > Registration of second factor.
- > Administration of second factor.
- > Kiosk- and portal function for user's own user data.

❖ User directories :

- > Databases, LDAP, MSAD

❖ Single sign-on (SSO) :

- > Large range of supported protocols

❖ Login RSET API

❖ Admin RSET API

❖ SAML 2.0 IdP and SP

❖ OAuth 2.0 and OpenID Connect 1.0

❖ Multitenancy

❖ Highly scalable

❖ Security at bank level

❖ Individually extendable

❖ User-, token- and role administration incl. helpdesk-tool



AIRLOCK[®]
SECURE ACCESS HUB

 Made in Switzerland

Microgateway & Anomaly Shield

Benefit

- ❖ Cloud-native = Modern, lightweight and automation-ready
- ❖ Agile security = more autonomy for application teams
- ❖ Shift Left = Security from the start
- ❖ Zero Trust = No bypass



Kubernetes native



API + Application Firewall



Based on Envoy Proxy

Highlights

- ▶ **Multi-level security filters** for award-winning protection against known attacks (e.g. OWASP Top 10) and zero-day exploits like Log4Shell.
- ▶ **Kubernetes-native:** Istio service mesh support, operator and CRDs, automatic sidecar injection, hot reload.
- ▶ **Modular configuration** with and without templates (with customize, helm, etc.)
- ▶ **Telemetry interfaces** such as Prometheus metrics and structured logs in ECS format (Elastic Common Schema) facilitate monitoring and analysis.
- ▶ **Plugins for modern IDEs** for automatic validation, code completion, and tooltips when editing the configuration.



Set up
10 min



Collect Data
1 week



Configure
10 min



Protect
Continuous monitoring



 Made in Switzerland

PKI & Certificate Management

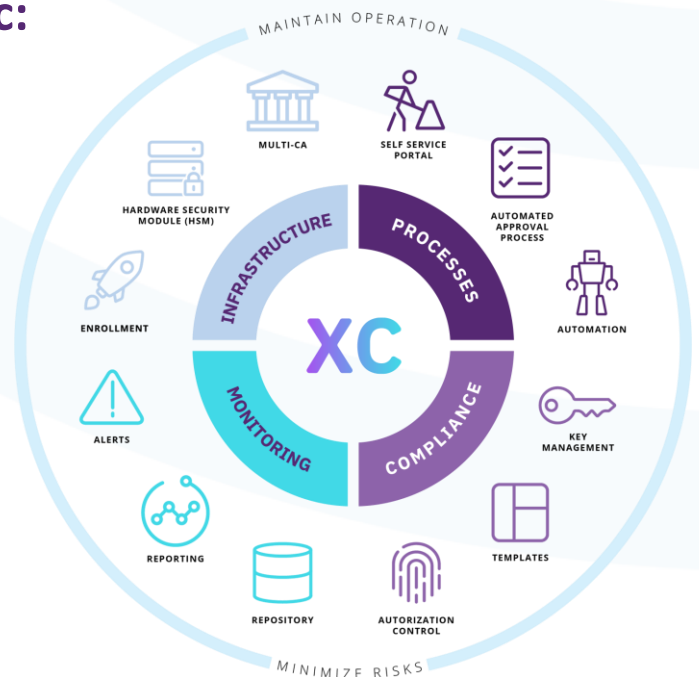
Key Management with essendi xc:

- ❖ Key generation.
- ❖ Key management: monitoring of service life and status, incl. alert function.
- ❖ Certificate and key storage: in HSM and key vault.
- ❖ Controlled recovery of keys in case of destruction or loss.
- ❖ Certificate and key handling.
- ❖ Forward-looking risk management.

1 360 certificate cockpit

2 Individual configuration

3 Process Engine



essendi xc makes all the difference
Certificate management
smart and secure.



user



WATCH VIDEO



Made in Poland

PAM "Privileged Access Management"

- ❖ All in One Solution
- ❖ Password Changer
- ❖ Full Session Control
- ❖ Agentless
- ❖ AI-powered Prevention
- ❖ Virtual & Hardware Appliance
- ❖ User Behavior Analytics
- ❖ One Day Deployment
- ❖ Efficiency Analyzer for User
- ❖ User Portal
- ❖ Strong Encryption
- ❖ Session Recording (RDP , SSH , HTTP , Telnet , etc.)
- ❖ Acting as a Security Network Device L3 , L4
- ❖ Integration with Ticketing System
- ❖ Integration with Active Directory
- ❖ SSO Authentication
- ❖ Highly Customized Dashboard
- ❖ OTP for Admin Users
- ❖ Support External Storage
- ❖ Session Sharing
- ❖ Copy & Paste Control
- ❖ Full API Access
- ❖ High Load Ready
- ❖ Easy High Availability: (Master-Passive) or (Master-Master)



WATCH VIDEO



Made in Germany

Secure Boot Stick



❖ SBS (Secure Boot Stick)

- > ECOS Secure OS
- > Bootable Stick
- > 100% Working Isolated
- > Integrated Firewall
- > All Required Software Were Included

❖ ECOS central VPN Gateway & Authentication

- > Active Directory (AD) Integrated
- > Web Service For VWC Download
- > Two Factor Authentication 2FA
- > Full Central management
- > Users VPN Profiles
- > VPN Time Control
- > Central Update
- > High Availability
- > PKI Integrated
- > NATO & BSI



WATCH VIDEO



Made in Poland

NAC "Network Access Control"

Your Network - Your Rules

Various authentication methods

Working on groups

Response action

Access control

Advanced configuration options for access policies thanks to the built-in RADIUS server and 802.1X authentication and authorization.

Network visibility

Detection of all elements connected to the network and insight into parameters crucial for safety.

Integration

Automatic elimination of threats thanks to information from integrated systems (SIEM, FW, Antivirus, etc.).

Monitoring

Real-time preview of network devices, visualization of network traffic on ports and ongoing reporting.

DDI

DNS, DHCP, IP Address Management - automatic management of addressing, networks and IP addresses from one place.

Guest access

Fast and secure guest access to the network using Captive Portal or time accounts.

Application

Better device control, more efficient network configuration, and stronger authentication with NACVIEW apps.



syclope

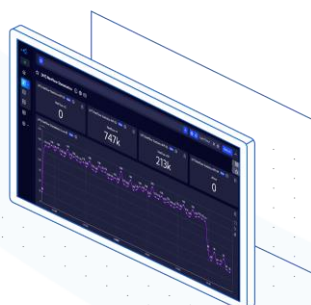


WATCH VIDEO



Made in Poland

Network Traffic Security



Visibility

Network Visibility

- ❖ Network Operating Center
- ❖ Advanced analytics
- ❖ Network Data Mining
- ❖ Out of the box anomaly detection
- ❖ Multi-protocols support
- ❖ Full analytics in L3 & L4
- ❖ Contextual search bar
- ❖ Custom dashboards

Performance

Network Performance (NPM)

- ❖ Single solution for long-term full traffic analysis
- ❖ Utilise real application detection
- ❖ Measure real-life app performance
- ❖ Combine network & application metrics
- ❖ Additional data sources
- ❖ DPI for L7 real application detection
- ❖ Dedicated L4L7 analysis for performance
- ❖ Dedicated performance dashboards

Security

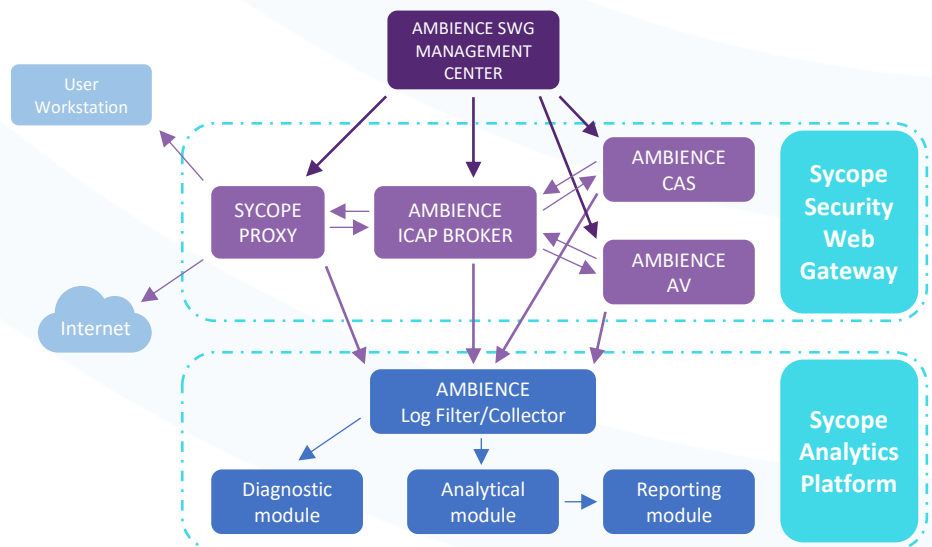
Network Threat Hunting

- ❖ Threat detection, analysis & mitigation
- ❖ Advanced attacks analytics
- ❖ MITRE ATT&CK tactics & techniques
- ❖ Syclope CTI (Cyber Threat Intelligence)
- ❖ Custom Security Operations Center views
- ❖ Constant security ruleset enhancements
- ❖ Active mitigation using NAC system
- ❖ Detection rules customization



Secure Web Gateway

The Syclope Secure Web Gateway system is a state-of-the-art, multi-module solution designed to provide control over Internet access. Leveraging advanced machine learning algorithms, it offers unparalleled accuracy in content classification across multiple languages, not just English. This system expertly evaluates traffic for potential threats and manages access to inappropriate or unrelated content.



Components of the Syclope SWG System:

- ❖ SYCOPE PROXY.
- ❖ AMBIENCE WEBSITE CONTENT CLASSIFIER (CAS).
- ❖ AMBIENCE AV.
- ❖ AMBIENCE ICAP BROKER.
- ❖ AMBIENCE SWG MANAGEMENT CONSOLE.

Syclope Analytics Platform:

- ❖ DATA COLLECTOR MODULE.
- ❖ ANALYTICAL-REPORTING MODULE.
- ❖ DIAGNOSTIC MODULE.



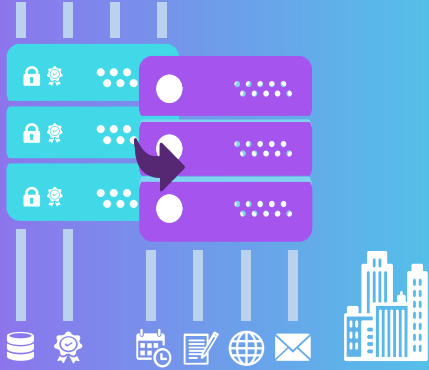
WATCH VIDEO



Made in Spain

FMS "Full Monitoring System"

- ❖ Network and communications monitoring
- ❖ Servers and infrastructure
- ❖ User experience
- ❖ Application performance
- ❖ Log collection
- ❖ Service level
- ❖ Inventory and CMDB
- ❖ Remote control
- ❖ Network Configuration Management
- ❖ Active Directory Monitoring
- ❖ ITSM and Service desk
- ❖ Network Flow
- ❖ Dashboards & reporting
- ❖ IT Automation
- ❖ SAP monitoring
- ❖ Business process monitoring
- ❖ High scalability and centralization
- ❖ IoT projects



APPTec360[®]
Unified Endpoint Management



WATCH VIDEO



Made in Switzerland

UEM "Unified Endpoint Management"

Scope of services and benefits:

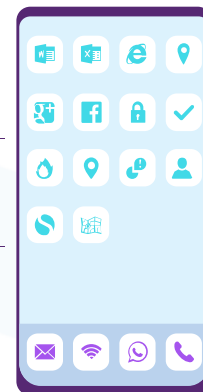
- ✦ Mobile Device Management.
- ✦ PC & Mac Management.
- ✦ Mobile Email Management.
- ✦ Mobile App Management.
- ✦ Mobile Content Management.
- ✦ Inventory & Asset Management.
- ✦ Web-based Management Console.

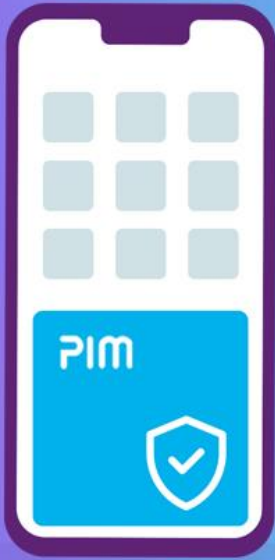
Unified Design

Secure Settings App

Protection from Unwanted Resets

Protection from Unwanted App Installations





MATERNA Virtual Solution

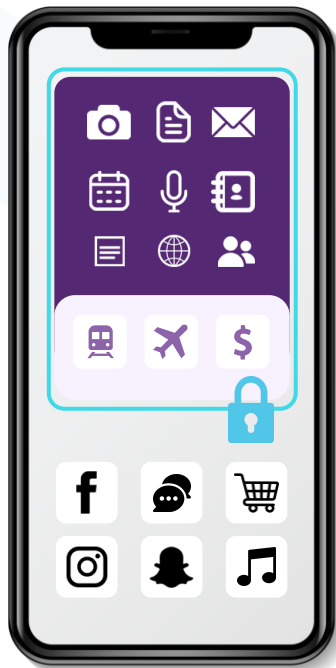


WATCH VIDEO



Made in Germany

Secure Mobile Container



Personal

- ✓ No Device-Management
- ✓ User has full control
- ✓ No access by IT-Dept
- ✓ Unlimited private usage

Flexibility & Freedom

Official

- ✓ Secure Container is part of Authority-Network.
- ✓ All important features for mobile communication.
- ✓ IT-Dept. fully in control.

Everything encrypted



Official - Personal

Work like on Desktop



Secure Mobile Communication Messenger (IM)





LoopCom Messenger

A secure communication solution with **end-to-end encryption**.
LoopCom keeps your conversations confidential, whether you're sending text messages, making voice, and video calls, or sharing files.



**Encrypted
Calls**



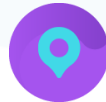
**Chat &
Conference Rooms**



**Encrypted
Video Calls**

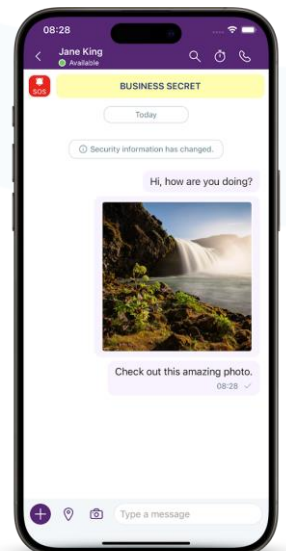
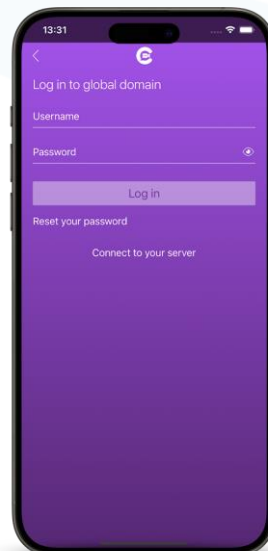


**Encrypted
Group Chat**



**Location
Share**

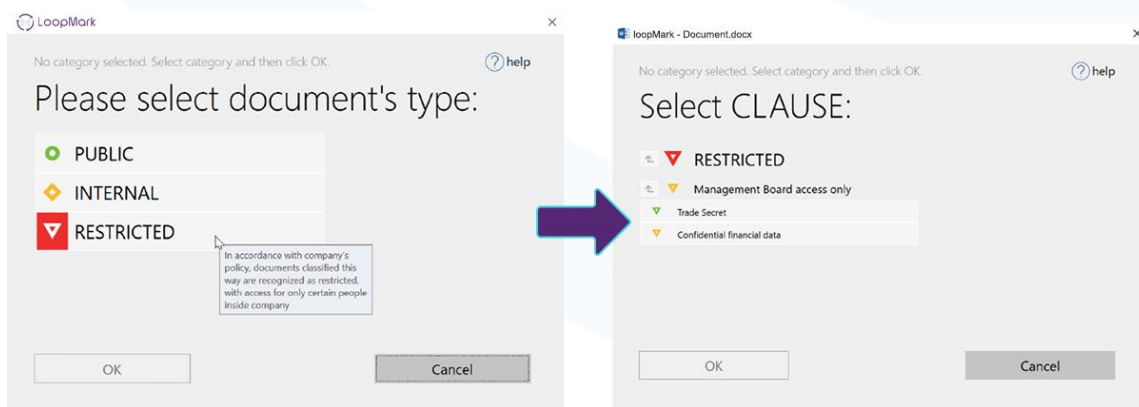
- Encrypted Messages
- Self-destructing Messages
- Encrypted Voice Mail
- Encrypted Conference Calls
- LoopCom Evidence
- Advanced Comms
- LoopCom BOT
- Location History
- Location Tracking
- On-Premise Maps










File and Email Classification System

LoopMark makes it possible to supplement automatic file and e-mail classification mechanisms with invaluable knowledge of the user regarding the level of confidentiality of the content created by them.



- Flexible configuration 
- Integration with security systems 
- Flexible distribution methods 
- Central management and reporting 

MAIN FEATURES

-  Classifying previously created documents
-  Forcing the classification of documents on their creators
-  Protection against downgrading classification level



DLP "Data Loss Prevention"



Endpoint DLP

Discover, Monitor, Prevent Sensitive Data Leakage on Your Endpoints



Network DLP

Blocker at the network gateway

Product Overview



DISCOVER Sensitive Data

Scan and Locate sensitive Data Encrypt or Destroy Data



PREVENT Data Breach

Prevent data breach via removable storage, printer, network services (e.g. Gmail, Google Drive)



REPORT

Real-time Alerts of incidents Event logs and forensic evidence

DLP provides

- Compatibility with the latest software and protocol
- Control and deploy with effortless precision
- Approval Process
- Customize Consulting Service



Cleafy



WATCH VIDEO



Made in Italy

Anti Fraud Detection

- ❖ Zero Impact on end-users / Endpoints
- ❖ Transparent Application Traffic Monitoring
- ❖ Zero Touch to Backend Infrastructure
- ❖ Comprehensive Real-time Threat Detection
- ❖ Patented Dynamic Application Protection
- ❖ Easy Integration and Orchestration
- ❖ Open Architecture & Full API support
- ❖ Lightweight and Highly Scalable Infrastructure
- ❖ Multichannel Support: Web, Mobile & API channels
- ❖ Real-time End-to-End Visibility (Events / Session)
- ❖ Patented real-time Application Integrity verification
- ❖ On-Premise, Cloud, SaaS Deployment Options
- ❖ Different Installation Option (Physical, Virtual, Docker Containers)
- ❖ Detection of Advanced Attack Scenarios, such as (ATO), (ATS), Phishing, etc.
- ❖ Real-time Threat Evidence (TTPs, generic vs targeted attacks, Malicious Injected Code, Etc.)
- ❖ Detection of Advanced Attack Techniques, such as MITM, MITB, Mobile Overlay, SIM SWAP, Etc.
- ❖ Behavior Analysis
- ❖ Cross channel visibility
- ❖ Real-time Risk Scoring
- ❖ Client-less / Agent-less
- ❖ Multi-Entity Correlation
- ❖ Adaptive Threat Response
- ❖ Compliance support (PSD2)
- ❖ Device Integrity verification
- ❖ Customizable Rules/Actions
- ❖ Integrated Threat Intelligence
- ❖ Deterministic Malware Detection
- ❖ Transactional Risk Analysis (PSD2)



nomios



WATCH VIDEO



Made in Poland

SOC Consultancy & Professional Services

Benefits of the SOC24 service:

- ❖ Cooperation with experienced and competent staff of SOC24 engineers.
- ❖ Lower price compared to the costs of constructing the first line with your own resources.
- ❖ Fast service launch.
- ❖ Reduced infrastructure maintenance cost.
- ❖ SLA compliance.
- ❖ Increased safety of data and systems.
- ❖ Possibility to build a SOC functioning in a continuous mode without using own resources.
- ❖ Reduction of the number of tasks of house teams – the ability to relocate competences.
- ❖ Guaranteed continuity and high quality of service provided.

Available solution packages:

BRONZE PROTECTION PACKAGE

- 1st line of SOC
- 8/5
- Service Delivery Manager

SILVER PROTECTION PACKAGE

- 2nd line of SOC
- 24/7
- Service Delivery Manager

GOLD PROTECTION PACKAGE

- 1st line of SOC 24/7
- 2nd line of SOC 8/5
- Service Delivery Manager

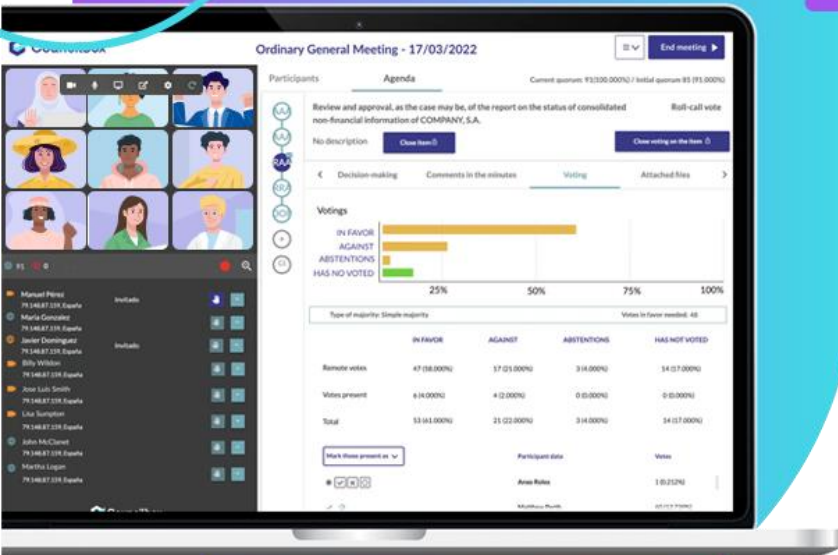
PLATINUM PROTECTION PACKAGE

- 1st line of SOC 24/7
- 2nd line of SOC 24/7
- Service Delivery Manager

Systems provided in the service model

Below are some examples of systems that we can implement to enrich the SOC24 service by skillfully selecting them to the business area, size and real needs of Your organization.

- SIEM class solutions
- EDR/XDR class solutions
- SOAR class solutions
- Vulnerability management class solutions



WATCH VIDEO



Made in Spain

Secure Video conference with Legal Validity



Attendees
(over any device & location)



Assistant
(over any device & location)

- ❖ We certify and provide legal security to the entire workflow, not just parts of it.
- ❖ We are not a videoconference provider; we are provider of legal security for complete remote procedures providing a new channel of presence.



Schedule Appointment

Client and advisor schedule a meeting.
Possibility to integrate with the entities scheduling tool.



Share Documentation

Before the appointment the client and advisor can exchange documentation linked to the procedure.



Bidirectional Communication

Before the appointment they can exchange information by certified email.



Identity Verification

Customer identity is securely verified.
Possibility of integration with identification standards.



Remote Participation

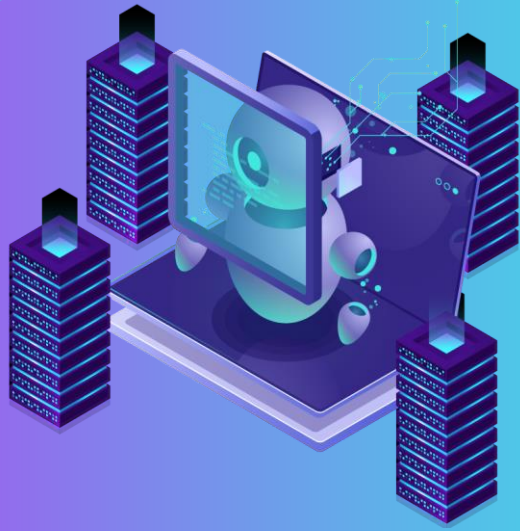
Advisor and client have a video meeting where the necessary decisions are submitted to consent.



Sign Documents and Minutes

Minutes and documents digitally signed, guarded for 5 years.
Exportable (through integration to the entities tools)

Blockchain evidence with legal validity



LABYRINTH



WATCH VIDEO



Made in Poland

A Deceivingly Simple Solution to Complex Threats

Deception Platform - This is how it works

01

Workstation

Seeder agent directs An attacker to the point.

02

Worker Node

Point interacts with An attacker & sends alert To MC.

03

Admin Node

Management Console

MC notifies security team and sends metadata about an incident to IR.

04

Incident Response

IR checks metadata with external databases and stops an attack.

01

Zero Performance Impact

02

Stop Advanced Threats

05

Automated Incident Response

04

Cut Operational Costs

05

Minimum Manual Configuration

BUSINESS VALUES

LABYRINTH Deception Technology



Targeted Attacks Uncovering



Post-Infection Detection



Lateral Movement Recognition



Dwell Time Reduction



Early In-Network Threat Detection



Accurate Alerts



Looptech Cybersecurity Consultancy Services

Main Scope

Milestones

Procedure Risk and Compliances	Security Policies & Procedures Drafting and Review
	BCP / DRP Strategies and Plans
	Feasibility Studies
	Security Investment analysis & roadmaps Infrastructure Evolution Scenarios
Gap Assessment and Auditing Services	Detailed Gap Assessment and remediation plans (ISO 27001, ISO 22301, PCI DSS, ...)
	Risk Assessment (ISO 27005, MEHARI, EBIOS, etc.)
	Process Maturity Assessments
	Privacy Impact Assessment / NCA Compliance
Configuration Review and Architecting	Security Solutions Benchmarks
	Compliance Audits & Action Plans (Standards and Regulations)
	Identity & Access Management support Studies
SOC Consultancy Services	Building use cases based on your assets
	Building Playbooks
	Building Dashboards and KPIs
Training and Mentoring	Training & Awareness support
	Training on Privacy & Personal Data Management
	Project Scoping
	RFP Support: Detailed Technical & Functional specifications Drafting
Governance, Risk, & Compliance (GRC)	Risk Management
	NCA Compliance Assessment & Review including (Policies and Controls and standards)
	systems & applications security analysis

NEXT GENERATION
OF CYBERSECURITY



Loopstech



+966 11 225 7879
+966 53 5792174



www.loopstech.com.sa



sales@loopstech.com.sa



@l8ptech