COM|CODE

Cyber Defense & Threat Intelligence Services

Defense In Depth

Cyber threats have become faster, more complex, and more business-critical than ever before. Traditional defense models are no longer sufficient to protect highly connected enterprises, critical infrastructures, and global supply chains. Attackers exploit cloud platforms, IoT devices, and AI-driven tools with unprecedented speed and precision. To stay resilient, organizations must move beyond fragmented security measures and raise Cyber Defense to a *NextGen* level — intelligence-driven, cloud-ready, and fully integrated into business continuity and crisis leadership.

COMCODE is a trusted strategic advisor for organizations seeking to build, transform, and strengthen modern cyber defense capabilities. With over 15 years of international experience in high-stakes security incidents, COMCODE guides CISOs, CIOs, and executive leadership in shaping resilient defense strategies tailored to real-world threats and business realities.

COMCODE Expertise

- **Cyber Defense Strategy & Target Operating Models:** Designing and implementing SOC/CDC blueprints (greenfield, hybrid, transformation) aligned with organizational maturity, governance, and regulatory requirements.

- **Architecture & Technology Advisory:** Vendor-neutral guidance on SIEM, XDR, SOAR, cloud-native security, and toolchain integration to ensure sustainable and future-ready defense architectures.

- **OSINT & Threat Intelligence:** Development of modular frameworks for Open Source Intelligence and Cyber Threat Intelligence, including ATT&CK mappings, MISP integration, darknet monitoring, and exposure analysis.

- **Simulation & Incident Preparedness:** Realistic crisis exercises, tabletop simulations, and strategic planning for effective incident response and business continuity.

- **Cloud-Native Defense:** Advisory on detection and response in Azure, M365, AWS, and hybrid environments with focus on visibility, control, and resilience.

- **Cyber Crisis Leadership:** Hands-on leadership in high-pressure cyber incidents – from crisis center moderation to integration of defense, communication, and business recovery.

- **Business Continuity Management (BCM):** Development of integrated continuity strategies linking cyber incident response with enterprise resilience. This includes analysis of critical dependencies, fallback levels, and alignment with ISMS and crisis management frameworks.

Cyber Defense & Threat Intelligence Services

COM|CODE

Our Customers

Our Cyber Defense & Threat Intelligence services address organizations with complex threat environments and high dependency on digital infrastructures, including:

- Industrial enterprises (manufacturing, automotive, chemicals, engineering)
- Energy and infrastructure providers
- Logistics and supply chain operators
- Financial institutions and insurers
- Critical infrastructure (KRITIS) organizations
- Global technology companies

Our Services

Our services combine strategic foresight with hands-on experience, enabling organizations to establish resilient, intelligence-driven cyber defense capabilities.

Defense Blueprint
Tailored SOC/CDC design, governance frameworks, and regulatory alignment.

Intelligence Edge
OSINT and Threat Intelligence frameworks for proactive detection and awareness.

Crisis Readiness
Simulations, playbooks, and leadership coaching to strengthen response capability, combined with Business Continuity Management to ensure resilience across the entire organization.

Cloud Shield
Scalable defense strategies for Azure, AWS, M365, and hybrid environments.

Cyber Crisis Leadership
Executive-level support in acute cyber incidents: leadership of crisis teams, decision facilitation, and integration of defense, communication, and recovery efforts