cipher
a Prosegur company

Assess, Strengthen, and Prepare: Cipher Always-On Offense

By simulating real-world cyberattacks, Cipher's expert Always-On Offense (AOO) team identifies vulnerabilities **across your operations, systems, networks, and applications.** Our methodical approach uncovers weaknesses and identifies areas of improvement, delivering actionable insights and hands-on training to strengthen your defenders' capabilities and improve their response to real threats.

Are You Ready for an Attack?

Many organizations still approach pentesting and red teaming as periodic exercises, conducted once or twice a year to find vulnerabilities or meet compliance standards like PCI. But in today's threat landscape, the question isn't *if* you'll face an attack — it's *when*. We believe there's a better way to stay ready.

At Cipher, we recommend simulating real-world attacks from real-world adversaries using tactics that mirror those of sophisticated attackers. This approach not only challenges technical defenses but also rigorously tests your organization's ability to **detect, respond to, and recover** from active attacks, ensuring you're resilient and ready for what's coming.

Our Always-On Offense (AOO) strategy continuously assesses your security posture against today's threats. AOO engagements focus on identifying and exploiting vulnerabilities across **systems, networks, applications, physical security, and operational processes.** With a continuous AOO approach, your organization gains a clear, ongoing view of technical risks, helping you stay prepared and ready to respond.

Types of Services:

- **Automated Pentest:** A software-driven approach that simulates cyberattacks against a computer system to identify vulnerabilities with minimal human intervention.
- **Pentesting as a Service (Automated but continuous):** This service provides ongoing automated penetration testing, delivering regular reports and updates on vulnerabilities and weaknesses through a subscription-based model.
- **Manual Pentest:** Is a deliberate, scoped, simulated attack against a computer system, network, application, or user base, carried out by a professional tester, to identify security weaknesses.
- **Red Team Service:** An objective-based simulation testing defenses using tactics, techniques, and procedures (TTPs) similar to those of sophisticated threat actors. The objective tests how resilient an organization is in the face of an attack.
- **Purple Team Service:** This exercise involves both offense and defense working collaboratively to enhance the security effectiveness by continuously testing and refining the organization's defenses.
- **Continuous, Always-On Offense:** An approach where offensive security measures are continuously and automatically applied to simulate persistent attacks and probe for vulnerabilities.

How Does Cipher AOO Services Work?

- First, the customer defines the systems, networks, applications, physical security, and operational processes to test.
- Then, we define the methodology or how much prior information our testers will have. Is it Black Box (no information), Grey Box (some information), or White Box (all of the information).
- Next, we work with our customer to define the approach. Is an automated test enough? Perhaps a single Pentest with a human tester working for 2 weeks is sufficient. Or maybe, a team of testers imitating nation-state actors, taking as much as six months to engage in a campaign is what's necessary.
- From there, the AOO service is engaged with a person, people, or tool analyzing the organizations environment and technology assets. The analysis will then identify potential vulnerabilities.
- Finally, once completed, the Cipher AOO team provides its report to the appropriate stakeholders.

Deliverables

- **Executive Summary:** A high-level overview for non-technical stakeholders, covering the scope, objectives, and key findings of the test.
- **Technical Findings:** A breakdown of identified vulnerabilities, including severity ratings, descriptions of each vulnerability, how they were discovered, and the potential risks they pose. Additional supporting information, such as tool output logs, screenshots, and detailed methodology used during the test
- **Exploitation Details:** An explanation of any successful exploits performed, including screenshots or logs showing how access was gained, as well as the data that could potentially be compromised.
- **Recommendations:** Remediation steps for each vulnerability, prioritized by risk level, along with guidance for mitigating future vulnerabilities.

About Cipher

At Cipher, a Prosegur company, we are a leading Managed Security Services (MSS) provider, renowned for our world-class Managed Detection and Response (xMDR) service. We meet you where you are with flexible and open support for your technology needs, providing localized expertise and global reach.

Certifications & Accreditations

ISO 20000 · ISO 22301 · ISO 27001 · ISO 9001 · CEH · CEH MASTER · WAHS · enisa · ens · Cybersecurity Career Mentor EC-Council · FIRST · PCI Qualified Security Assessor · PCI Qualified PIN Assessor (QPA) Program · Authorized to use CERT · Rede Nacional CSIRT · CSIRT.es · EC-Council Ethical Hacker Certified

Gain peace of mind knowing your organization is resilient in the face of cyberattacks.
Contact us today to learn more about how we can help you safeguard your organization.

Get Started