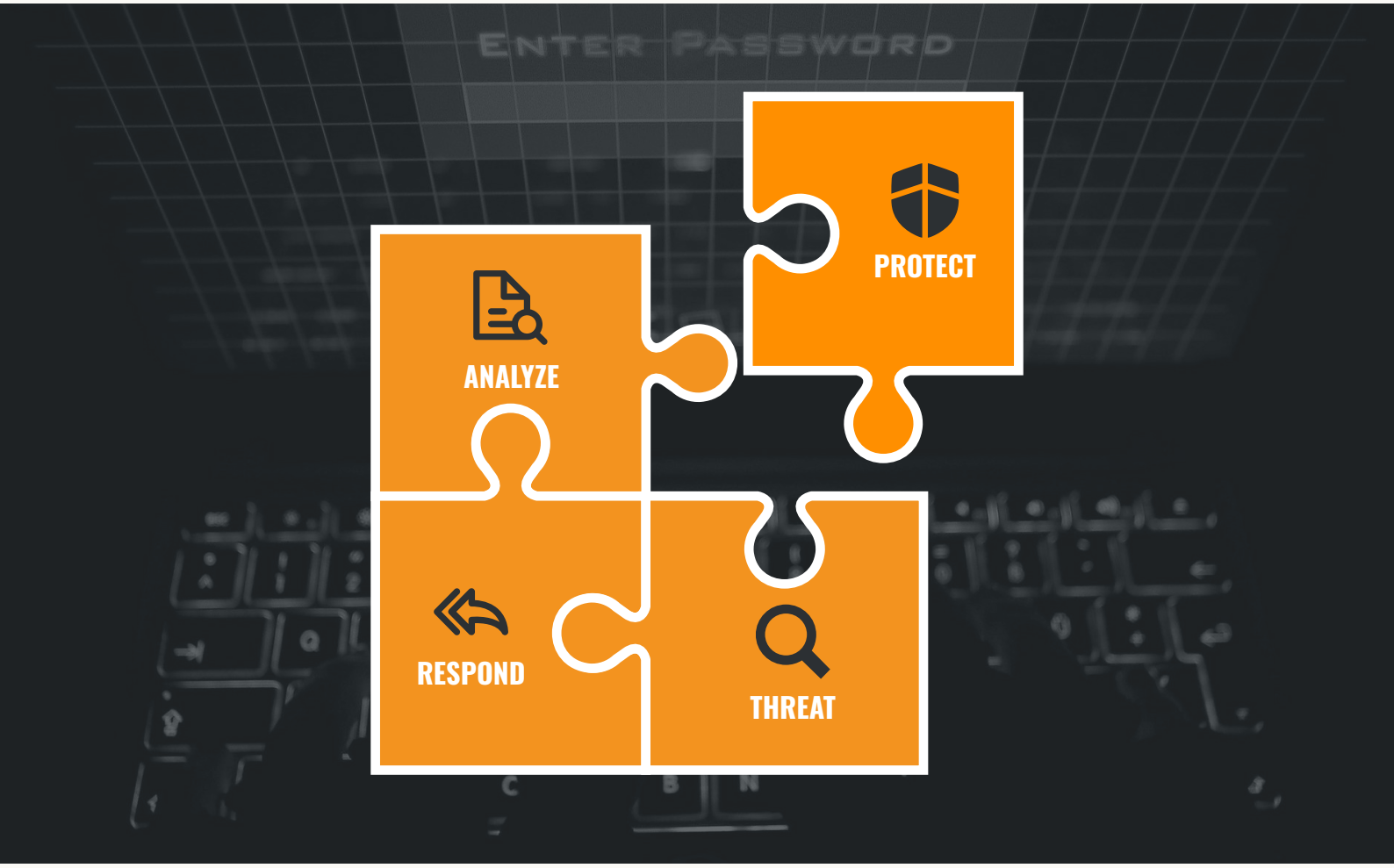
MH SERVICE
WORLD OF FORENSICS

MH SECURITY FRAMEWORK



Mission Statement – IT-Security & CSIRT Services

Our mission is to provide companies with long-term protection against cyber threats through our IT security and CSIRT services and to respond quickly and effectively in the event of an emergency. We strengthen our customers› digital resilience through a combination of preventive security measures, proactive threat detection, and professional incident response.

We identify and close security gaps, detect and analyze advanced threats such as APTs, attacks on web services and OT systems, and ensure that attacks do not go unnoticed. In the event of a cyber incident, our CSIRT (Computer Security Incident Response Team) is ready to take swift and targeted action with specialized experts, state-of-the-art forensic technology, and proven processes.

Our goal is to minimize damage, restore IT infrastructure, and ensure sustainable security improvements. Through continuous optimization, knowledge transfer, and partnership-based collaboration, we ensure that our customers are always one step ahead—secure, resilient, and well prepared for the challenges of the digital threat landscape.

MH SECURITY FRAMEWORK
ANALYZE

Mission Statement – Analyze Module (Hunt for new attack vectors & assess existing security postures)

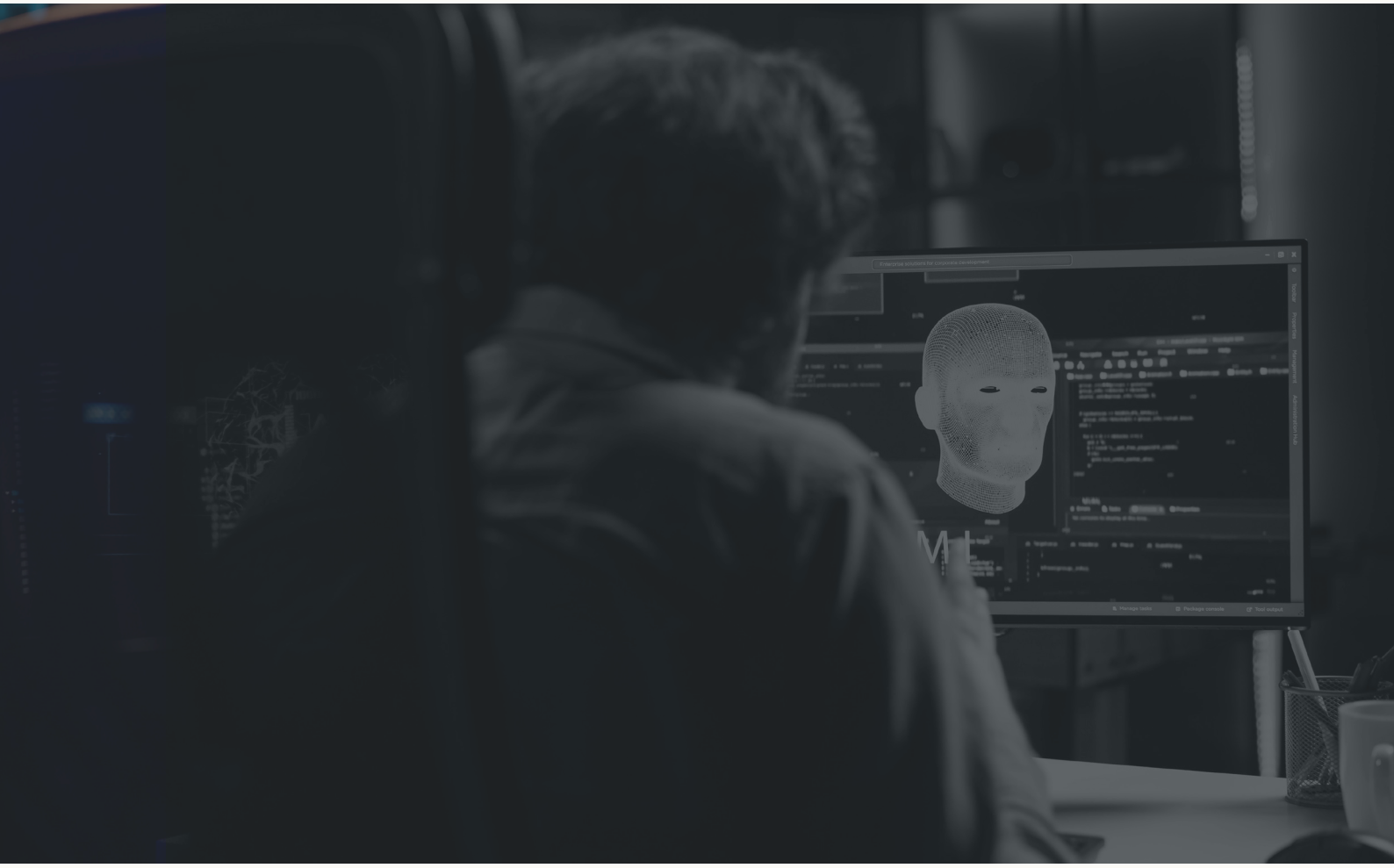
Our mission in the Analyze division is to proactively identify both new attack methods and existing security vulnerabilities. Through in-depth analyses of customer infrastructure—from Active Directory to firewalls and endpoint security to cloud security—we uncover weaknesses and assess potential attack surfaces. With a forensic look at current threat landscapes and innovative research methods, we ensure that security risks are identified early and addressed in a targeted manner. Our goal is to make organizations more resilient to future cyber threats and to derive effective protective measures.

MH SECURITY FRAMEWORK
PROTECT

Mission Statement – Protect Module (Implement countermeasures for well-known attacks or malware)

Our mission in the Protect division is to further develop and adapt existing and proven security measures in order to provide organizations with the best possible protection against known threats. By implementing robust protection mechanisms in the areas of Active Directory, firewalls, endpoint security, and the cloud, we minimize attack surfaces and strengthen our customers› resilience to cyberattacks. We rely on automated defense strategies, continuous optimization, and best practices to proactively counter threats. Our goal is to create a resilient security architecture that can withstand constantly changing threats and provide companies with lasting protection.

MH SECURITY FRAMEWORK
THREAT



Mission Statement – Threat Module (Find threats, generate incidents)

Our mission in the Threat division is to detect cyber threats in real time and accurately identify security incidents – from classic attacks to sophisticated advanced persistent threats (APT). Using state-of-the-art threat intelligence, anomaly detection, and proactive security analytics, we monitor the entire corporate infrastructure, including Active Directory, firewalls, endpoint security, cloud environments, web services, and OT systems. Our goal is to reliably detect attempted attacks, minimize false positives, and classify critical security incidents with maximum accuracy to enable a fast and effective response. In this way, we ensure a transparent, resilient, and robust security posture that protects companies from complex threats.

MH SECURITY FRAMEWORK
RESPOND

Mission Statement – Respond Module (Remediate Incident)

Our mission in the Respond division is to provide companies with fast, effective, and targeted support in the event of a security incident. Thanks to our mobile response teams, specialized hardware, in-depth expertise, and established processes, we are able to be on site quickly and respond professionally to cyberattacks of all kinds—from ransomware and APTs to attacks on web services and OT systems.

Our focus is on rapid containment, forensic analysis, and sustainable remediation of the incident to minimize business disruption and prevent future attacks. Working closely with the customer, we develop customized recovery strategies, optimize security measures, and ensure that the organization emerges from the incident stronger than before. Our goal is to restore critical business processes as quickly as possible and make companies more resilient to future threats.