SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY

Intelligence Led Pentesting with SAMA PARTNERS for a Proactive Security Posture

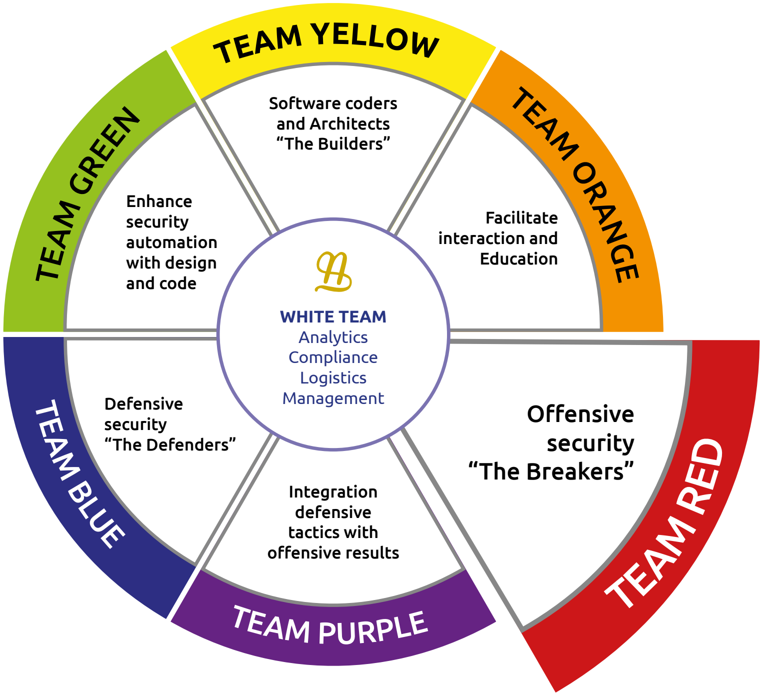
Know Your Enemy – Achieve Your Security Resilience

State of the Art

Sound and efficient Security Programs do not only rely on good planning and implementation but specially on continuous checking and improvements. Pentesting was established since years as an efficient tool to identify technical and organizational gaps on IT systems and organizations.
The pentesting approach, matured over the years and covered different aeras of application and even developed to be compliance prerequisite for maintaining successful Information Security Management System (ISMS) or compliance requirements such as PCI DSS. The classical Pentesting approach is witnessing a considerable enhancement thanks to threat intelligence.

SAMA PARTNERS Your Team for a Proactive & Effective Security Posture

SAMA PARTNERS sphere of knowledge and expertise is based on a one strong fact: proceed and act with our security operation's capabilities as a whole.


TEAM YELLOW
Software coders and Architects "The Builders"
TEAM ORANGE
Facilitate interaction and Education
TEAM RED
Offensive security "The Breakers"
TEAM PURPLE
Integration defensive tactics with offensive results
TEAM BLUE
Defensive security "The Defenders"
TEAM GREEN
Enhance security automation with design and code
WHITE TEAM
Analytics
Compliance
Logistics
Management

Only having Red and Blue Security Teams is not enough. The people building what must be defended need to be included. If Red, Blue and Yellow Teams are primary, SAMA PARTNERS have the capability to blend their skills together to create secondary teams that combine the skills and strengths of two primary teams.

SAMA PARTNERS sphere of knowledge

SAMA PARTNERS Red Teams in Security Testing: Vulnerability Assessment, Pentesting & Attack Simulation

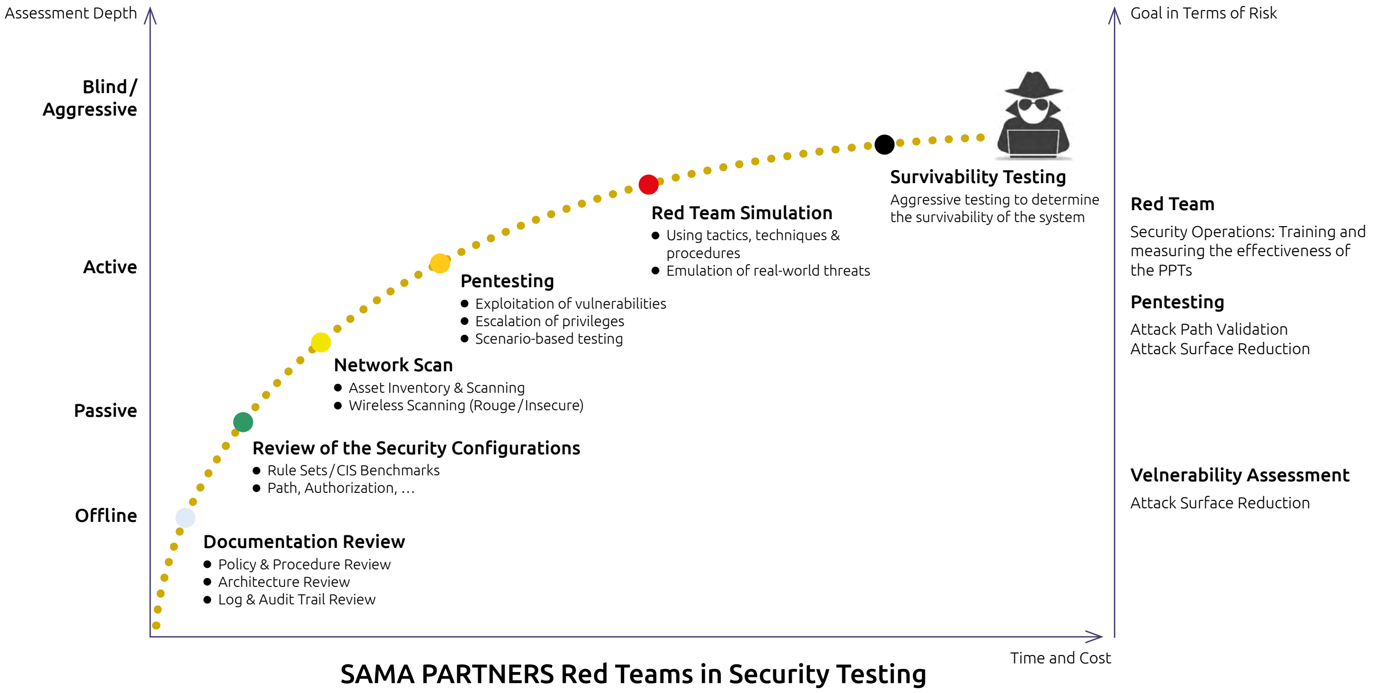
Vulnerability Assessment, Pentesting, and Red Teaming are commonly used by SAMA PARTNERS interchangeably and according to our clients needs.

SAMA PARTNERS Vulnerability Assessment is solid systematic examination of your information systems or products that determine the adequacy of your security measures and identify security deficiencies. We focus on finding vulnerabilities and prioritizing them by risk.

SAMA PARTNERS Red Team mission is to continuously improve the resilience of your organization against sophisticated attacks. Simulating adversaries conducting offensive security, our red team's goal is to simulate threats against your organization and effectively test the implemented security measures.

SAMA PARTNERS intelligence led red team testing involves the use of a variety of techniques to simulate an attack. It follows a rigorous procedure: Reconnaissance, Information Analysis, Execution, Exploitation, Control & Movement, Actions on Target.

Classical "Penetration Testing" means that tests are performed from the perspective of an attacker, and vulnerabilities are exploited to see "how far can an attacker get". However, this is not always the most effective way of testing because it often makes more sense to perform a Vulnerability Assessment: test in such a way that as many vulnerabilities as possible are found without wasting time trying to exploit them to see how far you can get. Finding more vulnerabilities is often more valuable because it allows to reduce risks more effectively: exploring wide, instead of (only) deep.


Assessment Depth
Blind/ Aggressive
Active
Passive
Offline
Goal in Terms of Risk
Survivability Testing
Aggressive testing to determine the survivability of the system
Red Team Simulation
● Using tactics, techniques & procedures
● Emulation of real-world threats
Pentesting
● Exploitation of vulnerabilities
● Escalation of privileges
● Scenario-based testing
Network Scan
● Asset Inventory & Scanning
● Wireless Scanning (Rouge/Insecure)
Review of the Security Configurations
● Rule Sets/CIS Benchmarks
● Path, Authorization, …
Documentation Review
● Policy & Procedure Review
● Architecture Review
● Log & Audit Trail Review
Red Team
Security Operations: Training and measuring the effectiveness of the PPTs
Pentesting
Attack Path Validation
Attack Surface Reduction
Velnerability Assessment
Attack Surface Reduction
Time and Cost

SAMA PARTNERS Red Teams in Security Testing

SAMA PARTNERS Basic Pentesting

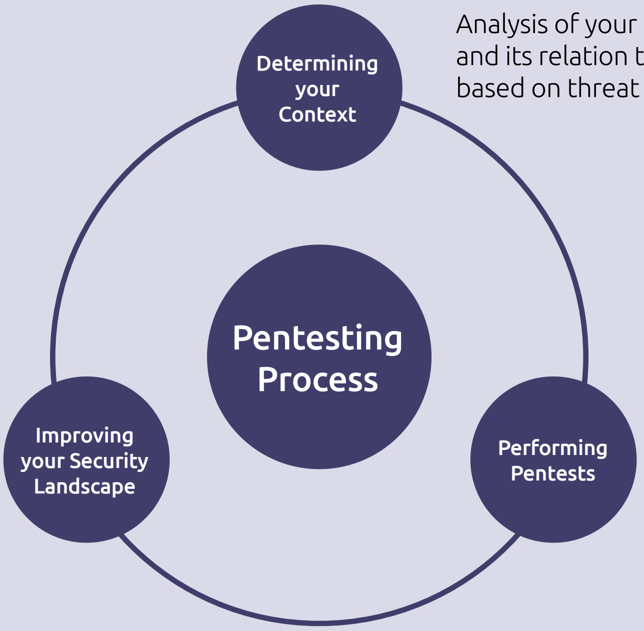
Our basic Pentesting is the practice of evaluating an IT infrastructure to seek out security vulnerabilities that an attacker can exploit. The primary objective is to spot security weaknesses in IT infrastructure. Our pentesting is also a strong method to test your organisation's security policy, its ability to spot and answer security incidents and its employees' security awareness.

The IT infrastructure being evaluated might be a software application or network. The vulnerabilities could include configuration errors, software bugs, design flaws and risky end-user behavior, to say a couple of.

Classical Pentesting is not enough to solely rely on reactive defensive mechanisms like stronger firewalls and passwords anymore. Instead, you need to know yourself and your enemy in an intelligence-led proactive approach.

SAMA PARTNERS Intelligence Led Pentesting Process

Classical Pentesting has, in general provided a detailed and useful assessment of technical and configuration vulnerabilities, often within isolation of a single system or environment. However, they do not assess the full scenario of a targeted attack against an entire entity. Instead of standard Red Teaming offers, that are based on general objectives and attack surfaces, SAMA PARTNERS intelligence red teaming concept starts with the context of your organization. Our focus is on what is probable rather than what is theoretically possible. SAMA PARTNERS serves as a springboard for taking real-life examples of cyber-attacks, including motivations, objectives and methods of existing attackers, relevant to customer context.
This allows us to offer an efficient and effective Intelligence Led Pentesting (ILPT) service in both Threat Intelligence Teams and corresponding reports as well as Pentesting Testing Teams.
Our ILPT service consists of three main steps, which can be offered as a package or individually. Those service components are described in the following sections.



Analysis of your organization context and its relation to probable attacks, based on threat intelligence facts.

Simulation of real attack vectors based on legal and contractual permissions.

SAMA PARTNERS consulting expertise to increase your organizations security, based on previously conducted pentests.

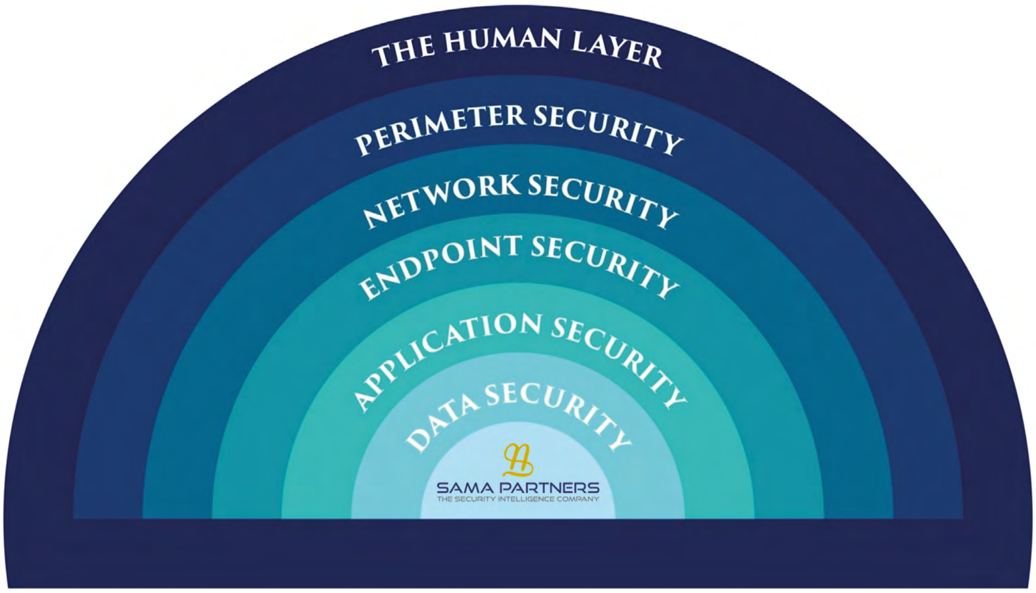
SAMA PARTNERS Pentesting Process

SAMA PARTNERS approach is supported by our reliable developed Vulnerability Assessment Methodology over 10 years. Our methodology is continually updated to deal with new and emerging threats. It consists of a structured approach to conduct network and application vulnerability testing such that network devices and applications are subjected to assessments against well-known and lesser-known vulnerabilities using a combination of commercial, public and proprietary tools.

WE INVITE YOU TO PARTNER WITH US!

SAMA PARTNERS Pentesting Capabilities

Our services and solutions are designed in layers, in accordance with the "layered security" concept from the cutting-edge security technologies to a comprehensive range of support.



Layered Security with SAMA PARTNERS

Examples of fields in Pentesting:

Cloud	■ Detailed assessments on the cloud service provider configurations those allow to use cloud services with the confidence that security configurations are set correctly
Networks	■ Pentesting for Firewalls, IDS/IPS, Switches, Routers, Load Balancers, Dial-up ■ Using handcrafted, manual processes, those over hackers' creativity to obtain additional information and evaluate misconfigurations as well as vulnerabilities ■ Using automated scanners to identify vulnerabilities ■ Attempting to bypass sensors, through manual and automated techniques, in order to test the effectiveness of countermeasures ■ Establish automated ARP redirectors and network sniffers to capture and decrypt secure and insecure network communications ■ Using automated phone line scanners (A.K.A. war dialer)
Operating Systems	■ Using automated scanners to identify host vulnerabilities ■ Using automated host-specific server-based scanners to evaluate the host configurations and related vulnerabilities ■ Using manual processes and scripts to evaluate the host configurations and vulnerabilities ■ Examining hosts with different functions and processes
Social Engineering Pentesting	■ Attempting to persuade users to give their sensitive information, e.g. passwords and usernames. Our pentesters use: Phishing attacks, Smishing (SMS), Imposters, Vishing (Voice), Pre-testing, Tailgating, Namedropping, Dumpster Diving, Gifts, Eavesdropping
Web-Based Applications	■ Combining social engineering with web-based pentesting approaches ■ Using automated scanners to identify web-application vulnerabilities ■ Using automated web-application scanners, scripts, and perform manual processes to obtain additional information and evaluate the internal web-application configurations and vulnerabilities

SAMA PARTNERS Pentesting Approach

The efficiency and outcome of testing is heavily influenced by the information available to testers upfront. We generally make a distinction between black, grey and white box testing:

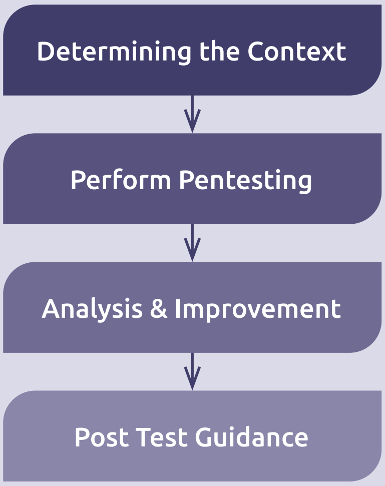
Black Box: SAMA PARTNERS tests the externally visible infrastructure or application from an attacker's perspective without information or login credentials upfront. This kind of test give a simulation of how an attacker without any information, such as an internet hacker, organised crime, presents a risk to the environment.

Grey Box: SAMA PARTNERS tests from an authenticated perspective, which vulnerabilities can be found in the application, including relevant APIs. A grey box test is a blend of black and white box testing techniques. Clients provide us with snippets of information to help with the testing procedures.

White Box: SAMA PARTNERS is provided with access to, and configuration details of, infrastructure components. This strategy provides a simulation of how an attacker with information (employee) could present a risk to the environment.
Together with your engineers, we will review the security settings of the targets, and compare them to best practices.

SAMA PARTNERS Pentesting Deliverables — Post Testing Dissemination and Advice

SAMA PARTNERS would proudly provide the strongest deliverables within the industry. We recognize that finding vulnerabilities and areas for exploitation is critical.
Our Security Testing services, and deliverables have been inspired by the well-known frameworks CBEST and CREST. Our ILPT is designed to cover even more domains.



Determining the Context	Reporting: Digital Footprint, compliance requirements and risk management.
Perform Pentesting	Realistic scenarios, realistic attacking vectors, including utilisation of tools and tactics applied by real-life attackers. Close possible security gaps.
Analysis & Improvement	Security Improvement Plan.
Post Test Guidance	Remediation Phase: Disseminate, discussion, fully understanding of the findings and possible SOCurity® support.

Post Test Guidance with SAMA PARTNERS

The best way to be sure that the recommendations you implemented were effective is to test again. Quite often, as methods used to attack IT environments are always evolving, this may uncover new weaknesses.

After a pentesting, we would take time to disseminate, discuss and fully understand the findings. You should also relay the results of the test and actionable insights to your organization. Ensure that you emphasize the risks these vulnerabilities pose and how remediation will impact your business.

Our clients that engage with SAMA PARTNERS pentests get for a period, a complimentary access to our Security Operations Center (SOC). The SOCurity® team of SAMA PARTNERS provides you a level of assurance through the remediation phase of the testing.

Let us challenge with you the security assumptions between what it is and what it should be!

Pentesting Benefits with SAMA PARTNERS

- Adoption of best-in-class methodology e.g. CBEST and CREST frameworks, known from the financial industry.
- Carefully adapted to a wider range of profit and non-profit organizations.
- Identification of new vulnerabilities and reduction of the overall expenses.
- Efficient and effective work roadmap, focusing on current security threats instead of trying to improve everything.
- Collaborative knowledge, e.g. vulnerabilities and threats typical for the context of your organization.
- An appropriate level of assurance of protection against technically competent, resourced, and persistent adversary attacks.
- Our methodology is supplemented by testing scripts developed and tested in SAMA PARTNERS laboratories in key locations around the world. This allows us to offer a diversity of testing approaches beyond the routine functions offered by most commercial tools.
- Incorporating scenario-based testing into the threat detection process allows your organization to obtain additional insights into the true effectiveness of detection, response controls and procedures by benchmarking performance against the attributes of specific types of attacks.

Success Stories

Financials

Energy

Pharma & Chemicals

Industrials

Logistics & Transport

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY

Why SAMA PARTNERS

- Certified according to **ISO/IEC 27001: 2013** (TÜV-SÜD).
- SAMA PARTNERS, labeled **IT Security made in Germany** & **IT Security made in Europe,** one of the few providers in the EU, those are highly skilled and specialized in the domain of Cyber Security.
- SAMA PARTNERS testers are armed with up-to-date and specific **threat intelligence skills.** All testers are certified to a minimum standard (eWPT) while most have multiple certifications such as OSCP, OSCE, eCPPT, GIAC GPEN.
- SAMA PARTNERS operates its own „SOC-as-a-Service" (CREST accreditation in process).
- SAMA PARTNERS has been providing Vulnerability Scanning and Network Pentesting for over **10 years**. Our practice is comprised of **70 dedicated professionals**, most of whom carry several professional designations and significant information risk management and security experience that can be called on for support when required.
- SAMA PARTNERS Security & Privacy Practice is a national practice under the SAMA PARTNERS advisory framework.
- Familiarity with the context of your organization and long experience in consultancy for various branches.

Check your resilience with SAMA PARTNERS Intelligence Led Pentesting (ILPT)

Headquarter

SAMA PARTNERS Business Solutions GmbH
Hermsheimer Straße 3
68163 Mannheim
Deutschland
Phone: +49 621 10759977
E-mail: info@samapartners.com

Tunisian Office

SAMA PARTNERS Business Solutions SARL
Immeuble Le Coral, B11-3
Centre Urbain Nord
1082 Tunis – TUNISIA
Phone : +216 71 947 457
E-mail: info@samapartners.com

SOCURITY NEVER RESTS
SOCurity® is a trademark of SAMA PARTNERS
samapartners.com