SOCURITY NEVER RESTS

SOCurity® is a trademark of SAMA PARTNERS

SOCurity®: SAMA PARTNERS 24/7 Managed Service Offering for Organizations and Companies of all Sizes

Explore how your organization can increase cyber resilience with our services

Partner with SOCurity®!

Real Facts

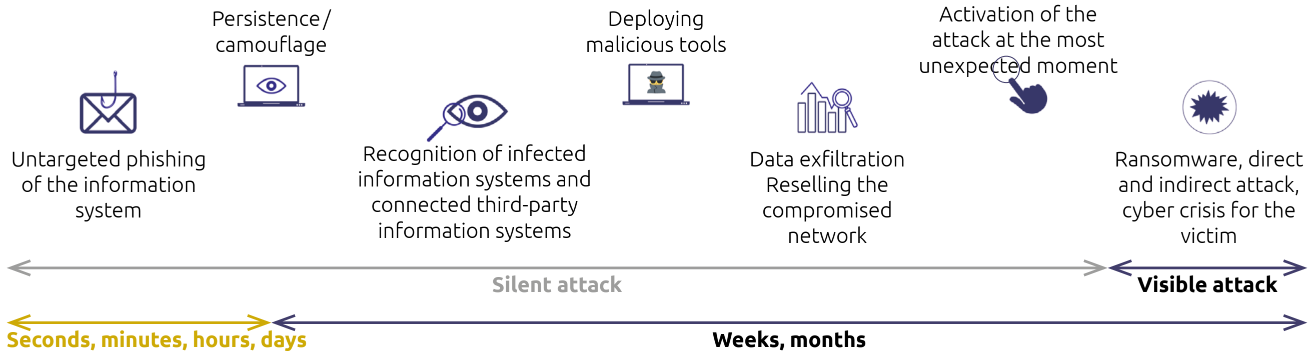
2019—2020—2021

- Cyber attacks have cost the german economy more than 100 billion euros and 40 million Euro was the damage suffered by a single company due to a ransomware attack.
- Death after hacker attack on Düsseldorf University Hospital, Germany.
- Ransomware at the Wismar public electricity utility company.
- Hacker attack on the german savings banks association.
- Cyber attack on online store of a major shipping company.
- and more!

Gaps by the numbers

- 30 days is the median time to create an exploit once a vulnerability has been released.
- 245 days is the average time to patch a vulnerability in the IT industry (150 days across all industries), see figure below.
- 90 % of organizations recorded exploits for vulnerabilities that were 3 or more years old.
- 60 % of organizations still see related attacks 10+ years after a flaw release.

Some companies consider contracting cyber insurance polices as an alternative for real security measures. Cyber insurance police is not a substitute for security and it will never be.


Untargeted phishing of the information system
Persistence / camouflage
Recognition of infected information systems and connected third-party information systems
Deploying malicious tools
Data exfiltration Reselling the compromised network
Activation of the attack at the most unexpected moment
Ransomware, direct and indirect attack, cyber crisis for the victim
Silent attack
Visible attack
Seconds, minutes, hours, days
Weeks, months

Proactively detect threat, reduce response time and react in a targeted way with our SOCurity®

Security Operations Center (SOC) is playing a critical role in cybersecurity. With quickly evolving threats and cyber-criminals using ever-more sophisticated techniques, a SOC bases on real time threat intelligence is critical. To establish a SOC is a big investment, to make it up to date and to have a high maturity including real time threat intelligence make it too expensive.

SOCurity®, SAMA PARTNERS SOC, is the best way to foster your return on investment.

Your Security Challenges

- The world today is comprised of two types of organizations: those who have been breached, and those who do not yet know that they've been breached. Whether they are able to detect sophisticated breaches and how fast this can be done.
- 90 % of german companies implemented measures such as segmentation of network, minimization of gateways, firewalls and antivirus solutions. However, most companies still focus on reactive measures (Federal Office of Information Security Germany).
- Small and medium size businesses (SMBs) are subject to security incidents just as much as larger businesses. In fact, more than a quarter of the victims of confirmed data breaches in 2020 were small businesses.

Our Socurity® Duties

- Our SOCurity® is your best way to overcome your own security whitespots. It works proactively to identify possible attacks and protect your business.
- Our SOCurity® helps you with 24/7 security and threat intelligence management to prevent breaches, mitigate risks and ensure safety and regulatory compliance.
- Our SOCurity® combines people, processes and technologies to provide secure access to business applications, over any network and from any device.
- Our SOCurity® provides you with an assessment and detailed analysis of security risks and threats of your business and your infrastructure including network, firewalls,servers and applications. Our experts help you manage your risk, reduce costs.

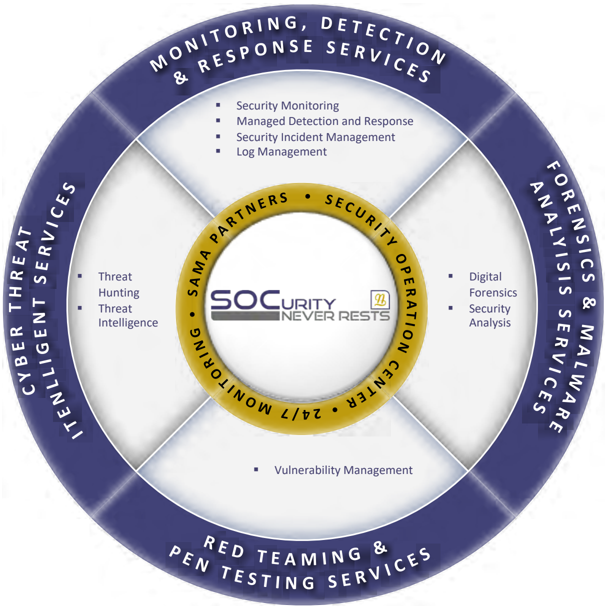
Have the best correlation on your monitoring activity without having to increase staffing
Enhance to a TRUE 24/7 OPERATIONS

Why not Inhouse Cybersecurity Operations

- An increasingly complex cybersecurity landscape is creating problems for businesses of every size: Severe alerts and regulation fatigue, and complex compliance issues.
- Growing skills gap: Tactics are changing, exploits are growing exponentially. The number of dedicated and specialized people needed is increasing.
- High cost and complexities of in-house cybersecurity operations.
- Cost of response time: Discovering an attack quickly is crucial for your organization. The longer the dwell time of an incident, the more difficult and expensive it is to retain, remediate, and contain.
- SMBs are an attractive target for cybercriminals because they often lack the resources to build and manage a SOC, and are ill equipped to implement, manage, and maintain a security information and event management (SIEM) solution.
- There is a large strategic framework and there is also individual responsibility: each SMB should act proactively!

Advantages of our SOCurity®

- Proactive monitoring of IT systems and ongoing analysis of the current threat situation. Many threat scenarios can be effectively prevented in advance.
- Cyber attacks are quickly detected, analyzed and fended off before major negative effects.
- Dynamically adapting security measures to the current threat situation.
- Identification of weaknesses in IT security and their elimination.
- Central security management for the different devices.
- Alerting for detected attacks and threats.
- Direct defence measures to limit the damage of cyber attacks.
- Implementation of security assessments.
- Technical support for all security-related issues.
- Reporting the Security Information Center on all security-relevant systems.


MONITORING, DETECTION & RESPONSE SERVICES
Security Monitoring
Managed Detection and Response
Security Incident Management
Log Management
FORENSICS & MALWARE ANALYSIS SERVICES
Digital Forensics
Security Analysis
RED TEAMING & PEN TESTING SERVICES
Vulnerability Management
CYBER THREAT ITENLLIGENT SERVICES
Threat Hunting
Threat Intelligence
SAMA PARTNERS • SECURITY OPERATION CENTER • 24/7 MONITORING •
SOCURITY
NEVER RESTS

SOCurity® Spectrum of Expertises

SOCurity® identifies cyber threats in real time using log data analysis from myriad data sources within the organization's partner. This up-to-the-second analysis of log data is essential to maintain a strong security posture. The set-it-and-forget-it solutions of old have long been obsolete, as modern business networks need constant monitoring in order to protect their assets. SOCurity® provides the technology, process and expertise you need to deliver dynamic 24/7 security and a cost-effective monitoring.

Scanning SECURITY alerts is easy, but focusing on the right incidents is MATTER EXPERTS

What SOCurity® is providing

- **Filtering Out the Vast Majority of False Alarms:** Socurity® platform uses multiple detection engines and human analysts to eliminate false positives.
- **Supplying Threat Intelligence Reports:** Socurity® correlates events with multiple threat intelligence sources.
- **Guaranteeing Threat Lifecycle Visibility:** Socurity® has visibility into the entire lifecycle—where the threat came from, with which systems did it interact.
- **Provide Customized Options:** Socurity® is able to monitor a broad range of log sources, and creates custom rules for your unique environment.
- **Remediating Threats:** Socurity® offers fast, proactive incident investigation, along with remediation and the ability to validate that the threat has been neutralized.

SOCurity® Spectrum of Service and Capabilities Deliverables

SOCurity® orchestrates the multiple roles, processes and technology needed to enable efficient incident detection, analysis and response. Comprising a set of processes, technologies, and a team of trusted security analysts and R&D specialists, SOCurity® provides complete visibility of both an enterprise's IT and its security system.

SOCurity® spectrum and playing field are adapted to methodically develop customer-oriented services.

Digital Forensics

Almost every crime leaves behind digital data. Anyone who is able to evaluate them can convict offenders. In order for them to be effectively prosecuted in cyberspace, the traces on digital devices must be traced back to their source and secured in such a way that they can also be used as evidence in criminal proceedings in court. In differentiating itself from IT security, which asks: "What could happen?", digital forensics deals with the question: "What happened?" The procedure of an IT forensic analysis is always the same, both in terms of structure and methodology. It comprises the steps of identification, data backup, analysis, documentation and preparation. Results can also be used to analyse and resolve IT malfunctions or failures.

Log Management

Logs are the outermost sensors of a system, which provide valuable information in real-time. This information allows a SOC to create an overview of the current state of health of an IT system and to assess the danger situation. Operational management urgently needs a differentiated and complete system view. On the one hand, to ensure the availability of critical business processes while mitigating the risk, but also to see the risks and dangers on the radar as early as possible. And to carry out forensic analysis afterwards, as required.

WE KNOW HOW TO STAY AHEAD OF THREATS!

SOCurity® the central point for all SECURITY-RELEVANT SERVICES in the IT environment

Managed Detection and Response

Provided as a service, Managed Detection and Response (MDR) is a comprehensive and efficient defense against all kinds of potential cyber-security threats. When set up, MDR provides complete visibility, monitoring and alerting in your networks. MDR identifies possible threats and react accordingly and orchestrates. Orchestrate security response quickly and purposefully. Part of the response is informing the client and acting based on standard operation procedures. Inclusion of machine learning methods is essential to overcome even completely unknown challenges.

Security Analysis

Real-time monitoring is worthless without an underlying security analysis that enables gathered data to be scrutinized by subject matter specialists to identify potential threats to customer environments. The analysis is enhanced by cyber intelligence insights, threat triage, malware dissection and forensics services. Socurity® uses state-of-the-art technology to detect and analyze security events. Both manual and automated procedures are in place to enable an efficient security analysis, as well as feedback-loop towards the customers in form of awareness building, situational awareness, and optionally definition of countermeasures to respond to detected threats.

SOCurity® Capabilities

Security Incident Management

Security Incident Management involves incident monitoring, reporting, impact assessment, incident escalation and post incident review. SOCurity® incident team is responsible for analyzing and handling the security threats and impact of information security incidents and to drive the process as efficiently as possible.

Security Monitoring

Real-time visibility into a company's entire network and security environment. Continuous Monitoring of critical context, malware and suspicious traffic, new systems and unusual connections and abnormal behavior within your network. Includes the definition of behavior that should trigger alerts and the implementation of alerts when required. Also determines the current security status and visualizes it for management.

Threat Hunting

Threat Hunting aims to use machines to pro-actively search for vulnerabilities in networks and identify possible attack patterns before they are applied. Find possible infiltration points based on hypotheses and specific clues and to translate these findings into automated rules and scripts that are fed into the security infrastructure. Supported by Machine Learning (ML) to examine huge amounts of data in shortest time, check for deviating patterns and take defensive measures.

Vulnerability Management

Attackers follow their own economy; they prefer easy targets. Protective measures should therefore be aimed at improving to a high level of digital resilience. This requires a structured setup of various security solutions and carefully maintained IT systems. Vulnerability Management provides a continuous overview, helps to classify newly found security holes. Derivation of the necessary need for action with corresponding recommendations for measures and the prioritization of security gaps.

Threat Intelligence

SAMA PARTNERS Threat Intelligence Service collect, filter and analyze data on IT security threats from various sources and deliver it in a usable form. Focused on informing decision-makers and improving their decisions.

Types of Cyber Threat Intelligence

Strategic	**Tactical**	**Technical**	**Operational**
Intelligence explains threats for a non-technical audience.	Intelligence describes threat conditions for technical audience.	Intelligence focuses on specific threat techniques.	Intelligence details hacker information and intent.

Security Assessment

We help you to quickly understand how to mature your security monitoring and incident response capabilities to take it to the next level and enhance your cybersecurity defenses and stop breaches from impacting the business.

Get your free Security Assessment!
Schedule some time to review the results and discuss next steps.

Success Stories

- Financials
- Energy
- Pharma & Chemicals
- Industrials
- Logistics & Transport

Never Rest SOCurity® 24/7 Staffing

Security analysts, security engineers and a SOCurity® Leader are all on-site. In addition, eyes-on-glass 24/7 staffing to catch intruders and malicious insiders before they impact your business.

Risk Management Committee

Impact and risk assessment of incidents, management of risk, compliance and governance, alignment of risk management with business needs and qualified risk ranking.

SOCurity® Manager

- Management of resources personnel: budget, shift scheduling and technology strategy
- Communication with management
- Organizational point person for business critical incidents
- Overall direction for SOCurity® and input to the overall security strategy

Emergency Response Team

- Knowledge and experience with network threats, their detection and mitigation, and indepth experience
- Immediate corrective action to restore services and attack mitigation
- Handling Major (High Priority) Incidents and escalations

Threat Intelligence & Vulnerability Management

- Network and Vulnerability Scanning
- Situational Awareness
- Security Consulting
- Ethical Hacking
- Gap Analysis
- Develop intelligence from their past incidents and from information-sharing sources

Forensics Team

- Expert of Security Technology and process, attacks and threat matrix
- Extremely good at reaching to root cause
- Thinking out of box
- Deep-dive incident analysis
- Advising on remediation
- Providing support for new analytic methods for detecting threats

Security Monitoring

- Continuous monitoring of the alert queue
- Triage of security alerts
- Monitoring health of security sensors and network elements
- Collecting data and context necessary to initiate Investigate and Analysis work

Security Management Team

- Expert of Security, OS, Network, Web technology, Database
- Implementation of security policies
- Handling day-to-day operations of the device administrations
- Configuration of management as per the change request policies
- Device Configuration Backups

24/7 eyes-on-glass coverage, we pair our Security® Team directly with your security staff to take on threat hunting, alert prioritization, security posture, reviews and risk management.

Rely on our SOCurity® as your cornerstone of the overall CYBERSECURITY defense chain

SOCURITY NEVER RESTS

SOCurity® is a trademark of SAMA PARTNERS

Why SAMA PARTNERS

- Certified according to **ISO/IEC 27001** (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 Cybersecurity.
- SOCurity® experts are armed with up-to-date and specific **threat intelligence skills.**
- CREST accreditation in process.
- Our practice is comprised over 10 years 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 sectors.

10+ Years in Operation | 70+ Professionals | 250+ Successful Projects | 6+ Languages

Our SOCurity® experts are ready to help.

Contact us:

Haithem Derouiche
✉ haithem.derouiche@samapartners.com

Peter Groß
✉ peter.gross@samapartners.com

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

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY

samapartners.com