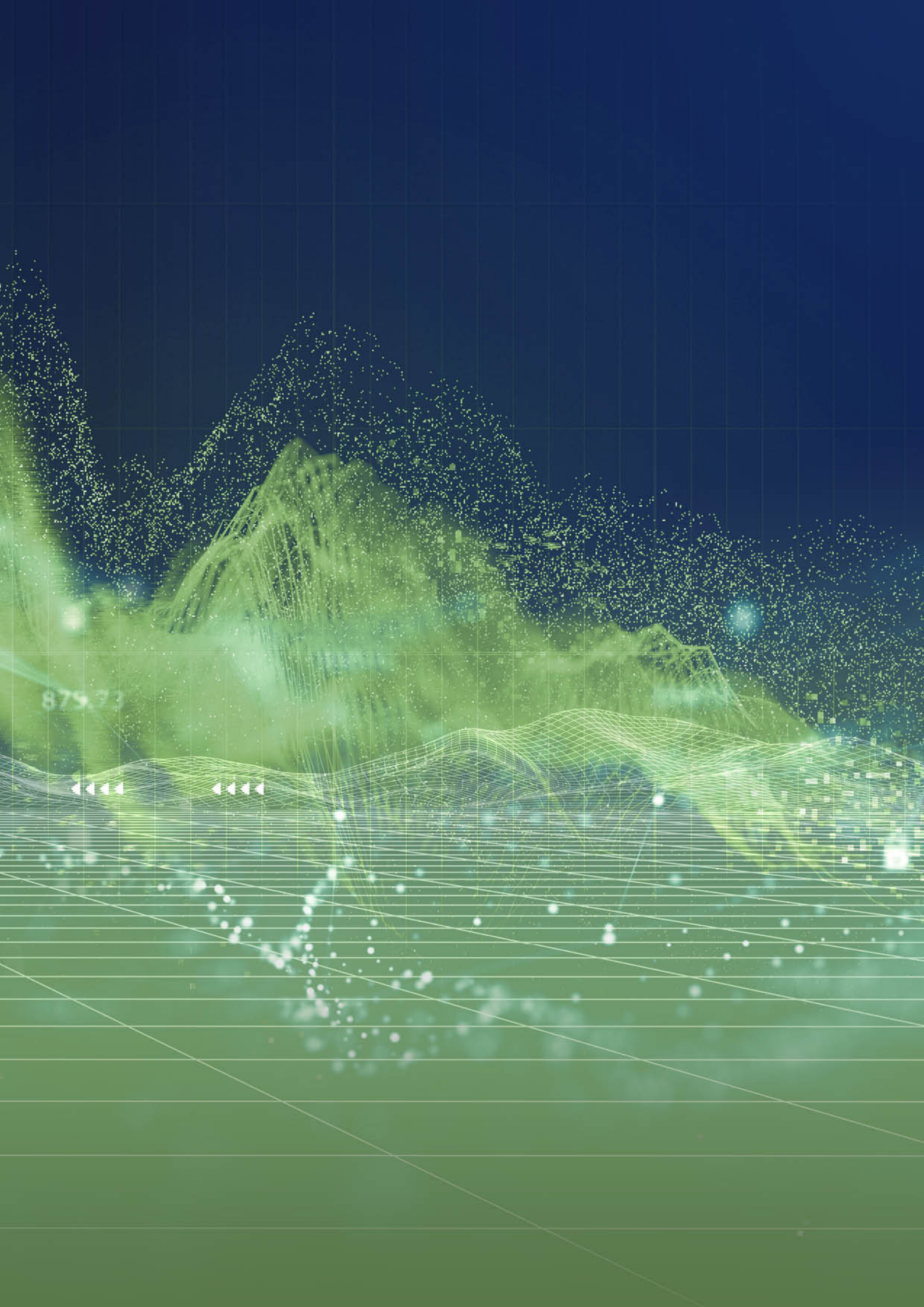
CYBER SECURITY

STM



STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş.

STM was established in 1991 for the provision of project management, system engineering and consultancy services to the Defense Industry Agency (SSB) and the Turkish Armed Forces (TAF).

The SSB continues to be the majority shareholder in the company, which has a workforce of 850 people, 63 percent of whom are engineers.

STM is among the leading companies operating in the defense sector, and is engaged in projects, particularly in the fields of naval platforms, tactical mini UAV systems, cybersecurity and IT services, command and control projects, satellite technologies, military aviation, radar and electronic warfare, and procurement and consultancy services.

Aside from its involvement in many national projects being conducted by the Turkish defence sector, STM is also engaged in export and business development activities for NATO with operations in more than 30 countries.

In addition to acting as the main subcontractor in the MiLGEM Project for the development of Türkiye's first national corvette, STM is also carrying out the detailed design as the main contractor in the project for the construction of TCG İSTANBUL (F-515), Türkiye's first national frigate.

STM has undertaken important tasks in submarine modernization and construction projects for the Turkish Navy, and is also responsible for Türkiye's first submarine modernization export, taking the lead role in the Pakistan AGOSTA 90B project.

STM developed KARGU, Türkiye's first indigenous attack UAV System, and launched Türkiye's first Cyber Fusion Center in 2016.

Through the INTEL-FS2 Project, STM ensures the flow of intelligence between all NATO headquarters around the world, and is successfully engaged in one of Türkiye's largest software exports to the Organization.

STM diversifies its technology-based activities to meet the needs of the public and private sectors – in particular those related to the Turkish defense sector.

STM is headquartered in Ankara, the capital of Türkiye, and continues its operations out of nine facilities, located in İstanbul, Gölcük and Ankara, as well as Pakistan.

STM was for three consecutive years listed on the Defense News Top 100 list of the world's top 100 defense companies.

CYBER SECURITY

STM CYBER SECURITY CAPABILITIES

- Cyber Threat Intelligence
- Cyber Situational Awareness
- Cyber Risk Management and Assessment
- Cyber Information Sharing and Warning Systems
- Cyber Decision and Process Support Systems
- Intelligent and Autonomous Cyber Security Infrastructures
- Penetration Testing Services
- Cyber Exercise and Preparedness Infrastructures
- Cyber Defence Interoperability
- Cyber Incident/Data Visualisation Infrastructures

CYBER SECURITY FIELDS OF ACTIVITY

- Cyber Fusion Center Services
- Research and Product Development
- Projects
- STM Academy Training
- Cyber Security Reports
- Capture the Flag (CTF) Competitions
- Common Criteria Test Center
- Web Application Security Training
- Secure Configuration Control
- Information Security for Managers
- Business Continuity and Disaster Recovery
- Social Engineering Attacks and Protection Methods
- ISO 27001 Implementation Training
- Ethical Hacker Training
- Applied Big Data Scientific Training
- Applied Big Data Engineering Training

STM ACADEMY

Theoretical and Practical Training

- The training provided at STM Academy includes theoretical and practical elements.

Cyber Security Basic Awareness

- The general awareness of information security is lacking.
- Theoretical and practical training on current modes of attack and the necessary precautions are provided.

Cyber Security Expert Training

- The training levels of personnel working in the field of cyber security need to be kept up to date to ensure coverage of new routes and modes of attack.

Advanced Cyber Security Training

- In addition to a wide range of topics, programs have been prepared for in-depth research and training of specific subjects.

Executive Training in Cyber Security

- TM Academy offers strategic-level cyber security training for executives.

Cyber Laboratory

- Malware analysis, threat analysis and penetration testing,
- Resilient network system engineering,
- High performance information processing and data analytics,
- Reverse engineering, vulnerability and gap identification, etc.

STM ACADEMY CYBER SECURITY TRAINING

- Intrusion Detection and Logging Management Training
- Cyber Incident Response Team Establishment and Management Training
- Hands-on Web Penetration Testing
- Cyber Security and Risk Assessment
- Centralized Security Monitoring and Incident Management
- Malware Analysis Training
- Basic Open Source Intelligence - OSINT and Cyber Threat Intelligence

Web Application Security Training

- Secure Configuration Control
- Information Security for Managers
- Business Continuity and Disaster Recovery
- Social Engineering Attack and Protection Methods - ISO 27001 Implementation Training
- Ethical Hacker Training
- Applied Big Data Scientific Training
- Applied Big Data Engineering Training

STM COMMON CRITERIA EVALUATION LAB (CCEL)

- Testing and evaluation of security products in accordance with ISO 17025 Standards (Common Criteria),
- Testing up to EAL 4+ level.

STM CYBER SECURITY REPORTS

- The quarterly “Türkiye Cyber Threat Status Report” provides general information on cyber incidents and contributes to the raising of cyber security awareness in our country.
- The reports include cyber threat assessments and information on possible cyber attacks, and are prepared in the light of forecasts.

CAPTURE THE FLAG EVENT

- The Capture the Flag event unites public, private sector and universities under a single roof for the creation of an information sharing network in the field of cyber security, and is held under the leadership of STM.
- Organized annually since 2015, it is the longest-running and most well-attended event of its kind in Türkiye, and plans are in place to continue the event in the years to come.

CYBER FUSION CENTER

The Cyber Fusion Center (CFC), which is involved in proactive and preventive activities for the protection of critical technologies and information assets, comprises three main holistic and integrated centers: the Cyber Threat Intelligence Center, the Cyber Operations Center and the Malware Analysis Laboratory (Z-Lab).

STM CYBER FUSION Center (CFC)

- A single, integrated approach to cybersecurity, combining traditional cybersecurity functionality with new capabilities
- A multifaceted approach that integrates cyber threat intelligence with security and technological responses
- Through this integration, proactive actions for the protection of critical technologies and information assets can be managed
- Integration of work, people, processes and technology

STM CFC SERVICES

- Cyber Operation Center Services
- Dynamic Risk Management
- Incident Response
- Cyber Threat Intelligence
- Malware and System Analysis
- Traffic Analysis and Monitoring

Cyber Operation Center (COC)

- COC Installation and Operation Consultancy
- 24/7 Security Monitoring Service
- SIEM Improvement and Optimisation Consultancy
- Use Case Consulting
- Incident Response Service
- Threat Hunting Service

Cyber Threat Intelligence Center (CTIC)

- Atak Surface Analysis
- Open-Source Threat Intelligence Analysis
- Cyber Threat Intelligence Platform
- Dark/Deep Web Analysis
- Threat Actor Analysis
- Customized Threat Reports

STM CYBER OPERATIONS CENTER

The Cyber Operations Center provides services beginning with the establishment of the necessary infrastructure for the detection of cyber incidents, the implementation and monitoring of security policies, incident investigation and on-site incident response. Depending on the needs of the institution, one or more of these services are provided as part of an institution-specific plan.

EVENT CORRELATION SERVICE

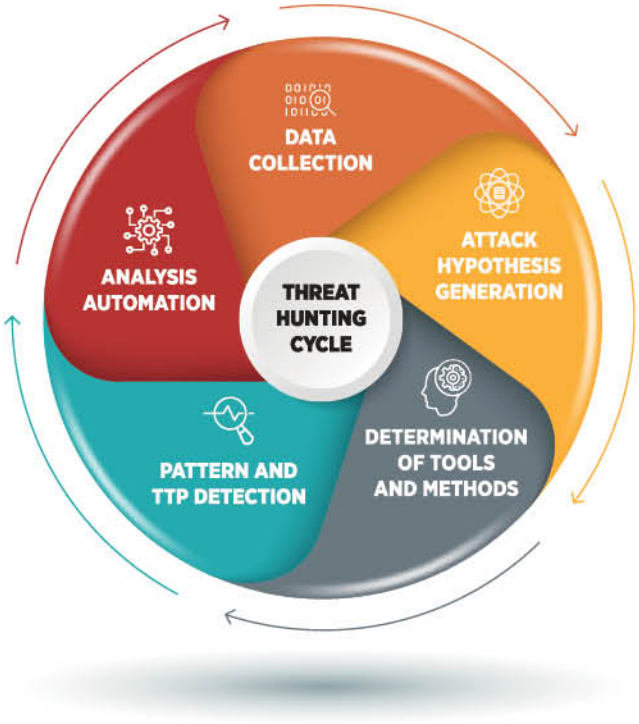
The correlation rules needed to correlate records and draw conclusions based on the sources of incident and the capabilities of the SIEM solution are identified and defined within the system. The causes of security breaches are investigated in detail through an examination of the alarms generated as a result of the defined rules.

SIEM MONITORING SERVICE

The records collected by SIEM are monitored, investigated, evaluated, and any necessary interventions are reported by cyber security analysts who make use of SIEM monitoring capabilities and other applications, including open source and commercial tools developed by STM engineers. Monitoring can be provided 5/8 or 24/7.

CONSULTANCY AND ON-SITE SUPPORT

After analysing the cyber security components of the institution to which the service is provided, necessary studies are carried out together with the institution to identify the needs and increase the security of the institution's systems. The goal is to ensure security in an integrated manner.



CASE STUDY

In incident investigations based on the Cyber Kill Chain methodology, the source, target, scope, attack vector and systems affected by the cyber attack are identified. After these studies, the obtained findings are reported in detail and the necessary measures are presented to prevent recurrence in the following period.

ON-SITE INCIDENT RESPONSE

When an attack is made against the resources of the institution being served, the incident is intervened and the necessary works are carried out together with the personnel in charge, and the authorities of the institution so as to eliminate or minimize the losses that may occur during the attack.

THREAT HUNTING

The presence of advanced cyber threats in the networks and systems belonging to the organization is proactively investigated considering different scenarios. Potential attackers, the techniques they use, the tools they use and the means of attack are actively

tracked and identified. In this way, the measures to be taken against Advanced Persistent Threats (APT) are identified and gaps in the organization's IT infrastructure are identified. Open source and commercial tools are utilized to create dashboards and reports for the identification of potential threats, suspicious and anomalous activities, malware, etc. Information from PCAP files, network flow data, applications and other security tools are analysed regularly and in depth.

STM CYBER THREAT INTELLIGENCE CENTER (CTIC)

To preemptively detect attacks in cyberspace and to take precautions, the STM Cyber Threat Intelligence Center carries out data collection processes from open sources, enriches the data, transforms the data into useable information, and analyses and transforms the information to create intelligence.

The data required for cyber threat intelligence is collected through a process that involves the identification and continuous monitoring of threats and the global threat ecosystem. In this process, threat data is collected from open sources, commercial sources and MISP-like platforms, transformed into actionable intelligence, and then presented through our own software.

At the same time, this intelligence data is transformed into sector- or organization-specific cyber threat intelligence by cyber threat analysts.

Following the enrichment, storage and verification of the data collected by the CTIC, the final cyber threat intelligence information obtained is provided as a service to institutions through the STM Cyber Threat Intelligence Platform (CyThreat).

PENTEST AND RED TEAM SERVICES

- Red Team Activities
- Web Application Testing
- IT and OT Network infrastructure testing
- Social Engineering
- DOS/DDOS Testing
- Wireless Network Testing
- Mobile Application Testing
- Validation Testing

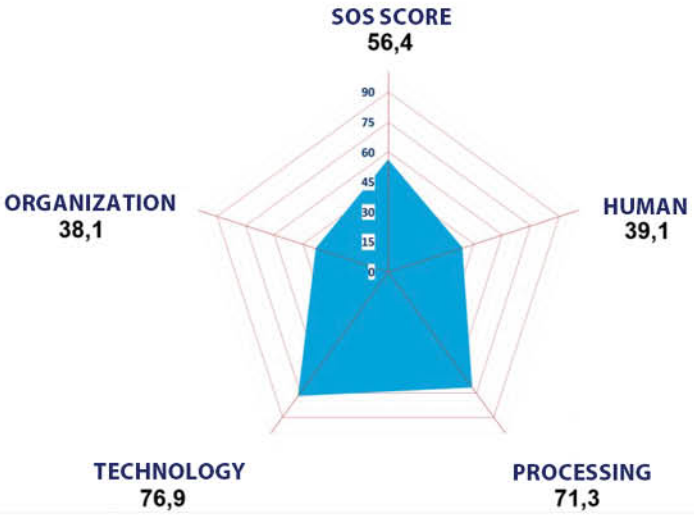
STM is a TSE-Approved Class A Penetration Test Company

COMPLIANCE AND AUDITING SERVICES

BIGR Consultancy and Audit Service (Information and Communication Security Guide)

Cyber Security Maturity Level Analysis

Our field experts evaluate your institution's organisational, technologies, processes and human-based cyber security approach through the application of our customized question lists, which have been compiled in line with national/ international standards, and then offer suggestions of how to increase of your cyber security maturity.



STM MALWARE ANALYSIS LABORATORY (Z-LAB)

In our Malware Analysis Laboratory, professional analysts analyse files that are considered or suspected to be malicious. These analyses seek to uncover such specific behaviours to identify whether the software is malicious, what the suspicious file does in the background, what its real purpose is and how it disguises itself.

In addition to the Windows, Linux and MacOSX operating systems, the **Malware Analysis Laboratory** can analyse malware running on the Android and iOS operating systems used in smartphones and tablet computers.

Based on analyses of independent networks and simulation environments by analysts, it is possible to simulate the Internet environment required by the malware or to carry out analyses in the absence of an Internet connection.

PLATFORMS FOR MALWARE ANALYSIS

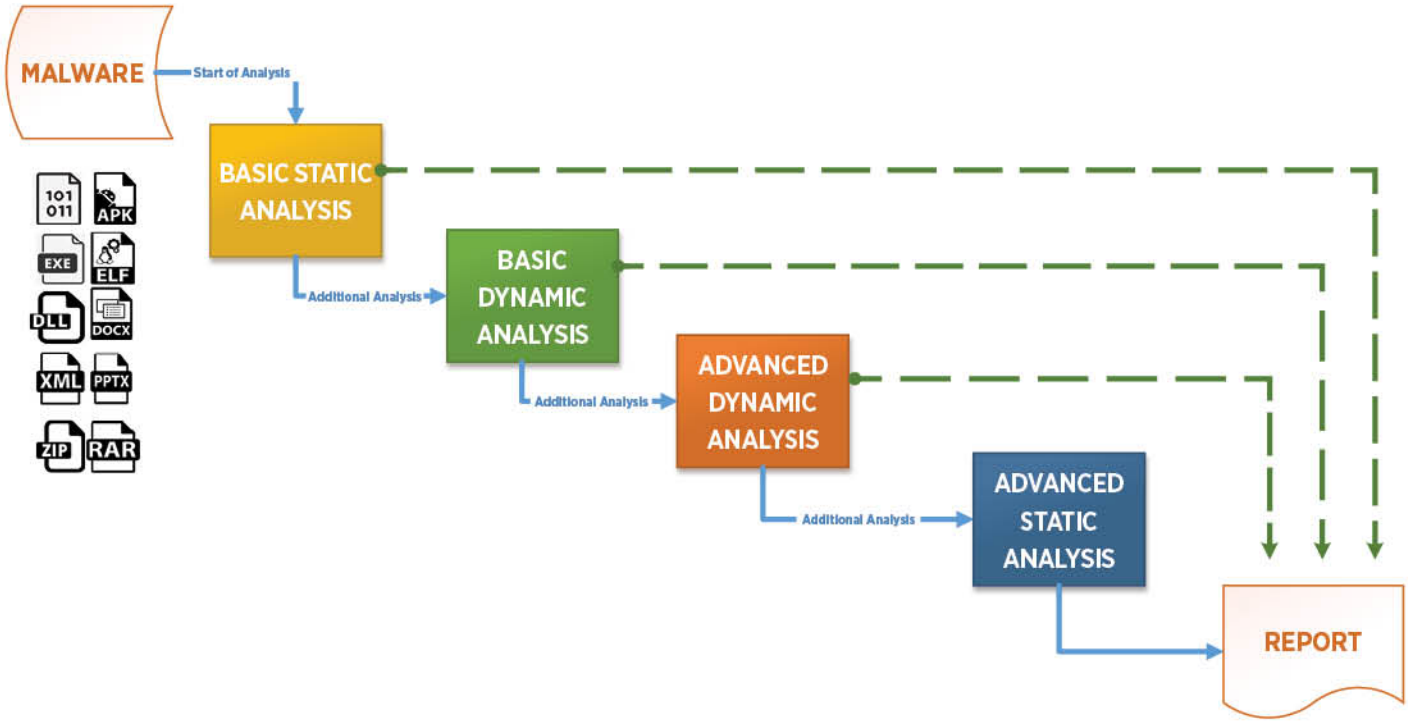
- Windows
- Linux
- OSX
- iOS
- Android

ANALYSIS METHODS

- Basic Static Analysis
- Basic Dynamic Analysis
- Advanced Static Analysis
- Advanced Dynamic Analysis

ANALYSIS CHANNELS

- Analysis on virtual computers
- Analysis on sandboxes
  - Using commercial sandboxes
  - Using open-source sandboxes
- Physical devices
  - Mobile phones
  - Tablets
  - Computers

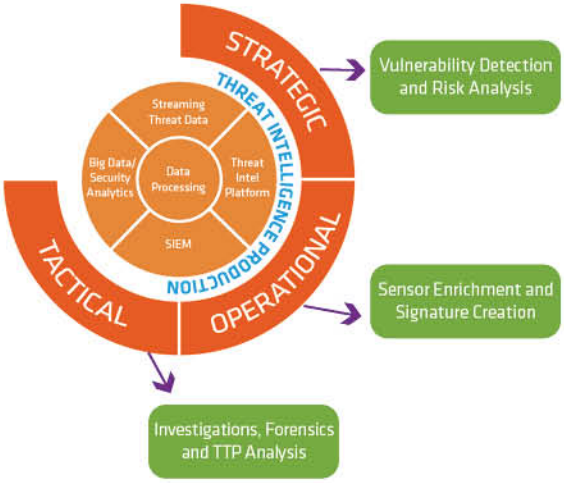


DevSecOps Consulting Service:

- Consultancy services are provided to add a cyber security perspective to DevOps processes.
- Consultancy services are provided to add SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) solutions to existing workflows.

Malware Analysis Laboratory Installation Service:

- Malware Analysis Laboratory installation and consultancy services are provided for large-scale institutions allowing the performance of on-site malware analyses.



Capture The Flag (CTF):

- The infrastructure service required for the Capture The Flag competition is provided.
- A CTF platform installation service is provided.
- The STM CTF competition is organized every year as a means of raising cyber security awareness.

Malware Analysis Services:

- After a cyber security incident, suspicious files appearing after the incident are analysed as potential malware, and a detailed reporting service is provided.

DDOS:

- A distributed denial-of-service attack simulation service is provided from different geographical regions for the configuration control of network security products.

Product Development:

- Product development services are provided to meet customer needs as part of our cyber security projects,
- Customized malware simulation services are provided to test the configurations and detection capabilities of cyber security products.

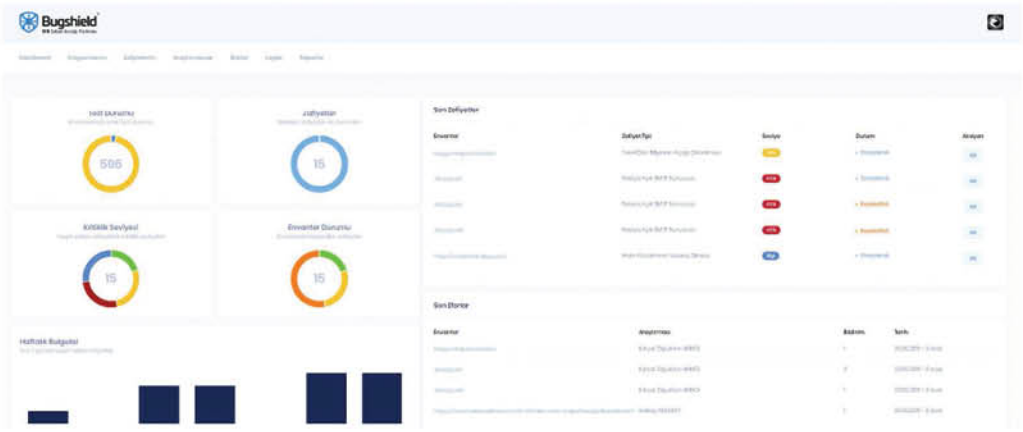
BUGSHIELD

Uninterrupted Cyber Security

STM Bugshield is a Continuous Penetration Testing and Bounty Hunting Platform through which vulnerabilities in customer resources are investigated from a “hacker” perspective, and any identified vulnerabilities are reported.

STM Bugshield has role-based management capability with customer, analyst and researcher profiles. In a researcher role, cyber security experts with competencies in different fields carry out vulnerability studies, and the analyst verifies the identified vulnerabilities and informs the customer on the platform after the approval process, allowing the customer can respond quickly to any identified vulnerabilities. Through the ticketing mechanism integrated into the platform, any findings and status changes can be monitored in real time. In addition to the alerts sent via Bugshield, notifications can also be sent via e-mail and SMS.

- The testing of systems based on a “Continuous Penetration Testing Methodology” by different security researchers at time intervals determined by the customer facilitates the rapid detection of any new vulnerabilities. Detected vulnerabilities are subjected to a two-stage approval process, and those whose accuracy is confirmed are communicated to the customer via push notifications. This shortens the time between the identification of the vulnerability and its closing.
- The status of tests, the identified vulnerabilities, the criticality levels of the vulnerabilities, the actions taken against vulnerabilities and the vulnerability inventory can all be monitored via the portal.
- Organizations can request vulnerability studies after determining their inventory lists and test policies.
- Organizations can generate reports of automatic vulnerability research results in the pdf, word (docx), csv and json formats, and by applying the desired filtering.



Test Status
This is the screen on which the inventory being tested or planned to be tested is displayed.

Vulnerabilities
This screen contains the approval status of the reported vulnerabilities.

Criticality Level
This is the screen showing the vulnerabilities detected at critical, high, medium and knowledge levels.

Inventory Status
This screen shows how many applications, IP addresses or domains have vulnerabilities.

HIGHLIGHTS

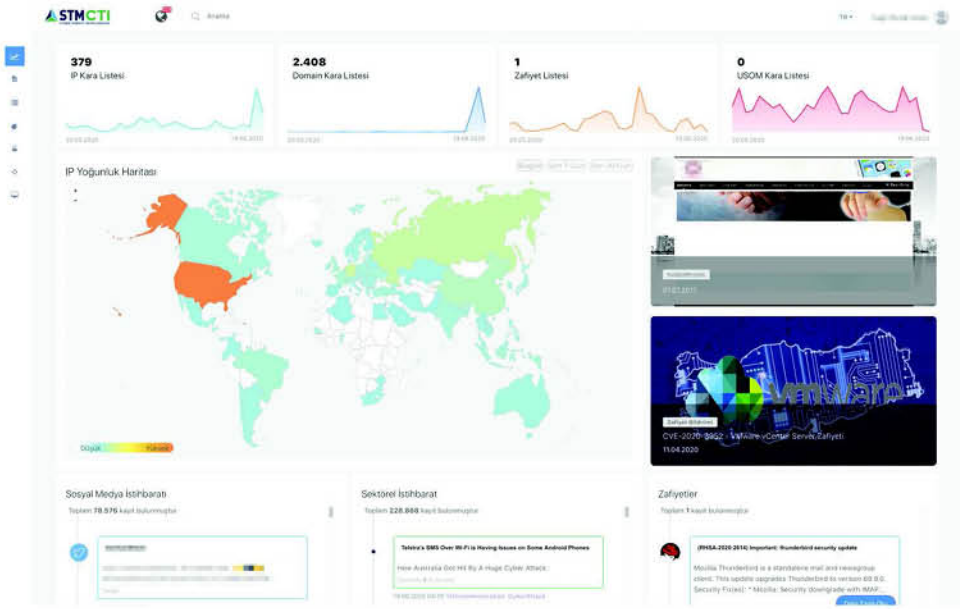
Reliability: Vulnerabilities are identified by a trusted group of researchers who have signed a confidentiality agreement
Quality: The inventory is checked by more than one researcher, and any identified vulnerabilities are checked and approved by STM analysts
Agility: Instant notifications of all detected vulnerabilities are sent to allow action to be taken
Continuity: Tests can be performed at more frequent intervals, as opposed to periodic penetration tests

Bugshield
STM Bug Bounty Platform

CyThreat

Cyber Threat Intelligence Platform

CyThreat provides clients with cyber threat intelligence data collected from various sources (deep/dark web, social media, blogs, forums, etc.) automatically, enriched with the subject- and incident-based reports of STM analysts. In this way, it is possible to detect the activities of cyber threat actors, to prevent cyber attacks before they occur and to take protective measures. The financial losses and reputational damage that may occur as a result of possible attacks can thus be prevented. Intelligence data (blacklist IP addresses, domain names, malware hash values, vulnerability data) can be integrated into security devices via API and STIX/TAXII. The task management feature allows tasks to be defined manually/automatically for the customer related to the detected findings, thus facilitating incident tracking.



BLACKLISTS

- IP Addresses
- URL & Domain Names
- Malware Hash Values
- USOM* Harmful Links (*National Cyber Incident Response Center)

VULNERABILITY LIST

- Vulnerability definition
- CVSS score
- Products affected by the vulnerability

ANALYSIS REPORTS

- Malware analysis reports
- Cyber threat status reports
- Attack surface analysis reports

POTENTIAL PHISHING SITES

- Identifying domain names that may be used for phishing attacks against the organisation and presenting them to the relevant customer

SOCIAL MEDIA MONITORING

- Presentation of customer-oriented data obtained on social media platforms

TASK MANAGEMENT

- Allows event tracking through manual and automatic task definitions.

SECTORAL CYBER INTELLIGENCE

- Threat data related to the clients areas of operation are collected from open sources in various forums, news sources and the deep/dark web.

BRAND MONITORING

- Brand data is collected from blogs, forums, news sites and the deep/dark web and presented to users through the interface.

VIOLATION DATA

- Through this interface, detected corporate e-mail addresses are presented to the user. Information on leaks from each e-mail address, from which address it was leaked, and the date of the leak are shared.

REPORTING

- Through the reporting feature, users can create one-time or scheduled reports by filtering data presented by the interface.

API

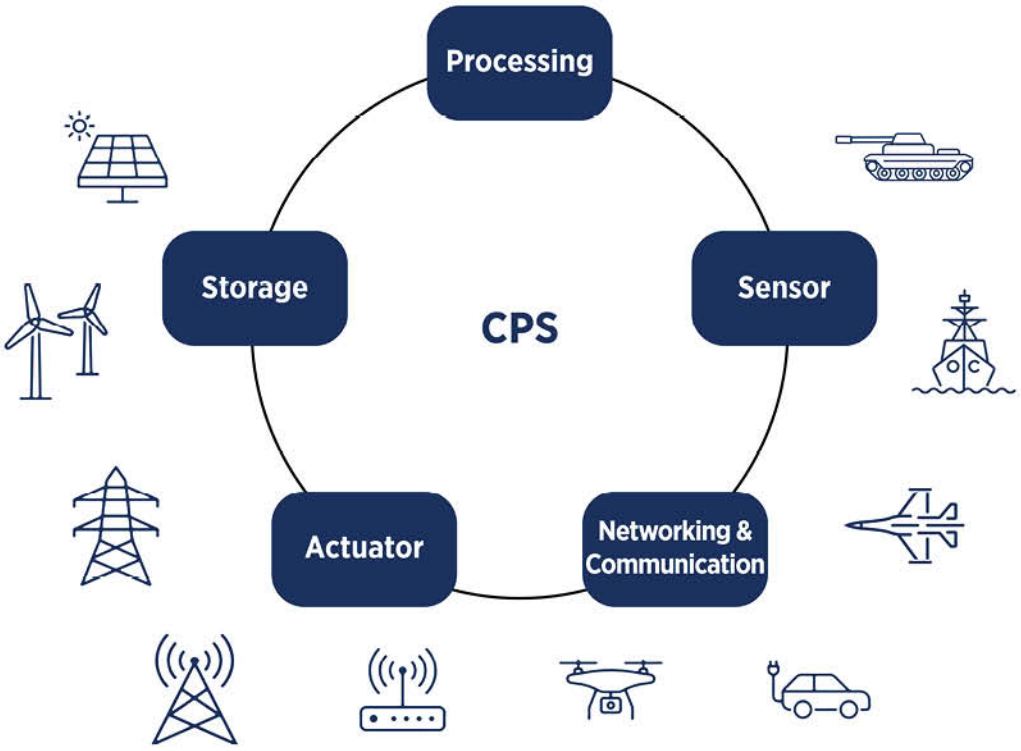
- Blacklist IP addresses
- Blacklist domains
- USOM malicious links
- Malware hash values
- Product-based vulnerability data
- Presentation of customer data obtained from social media platforms

CYTHREAT
CYBER THREAT INTELLIGENCE

CYBER SECURITY CONSULTANCY SERVICES FOR PLATFORMS, HARDWARE AND CYBER-PHYSICAL SYSTEMS

For land, air and sea platforms:

- Consultancy Services for Cyber Security Analyses, Architecture, Requirement Determination and Audits
- Verification, Testing and Remediation Services Consultancy
- Laboratory Installation/Operation Consultancy
- Platform-Specific Product Design/Development Services



NATIONAL/INTERNATIONAL COLLABORATIONS

CCDCOE NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

We are among the institutions providing personnel for exercises and conferences organized by CCDCOE.

LOCKED SHIELDS

Locked Shields is a unique opportunity to encourage experimentation, training and cooperation between members of the CCDCOE

NCI AGENCY

NATO Communications and Information Agency

TÜRKİYE SİBER GÜVENLİK KÜMELENMESİ

Turkish Cyber Security Cluster

EOS EUROPEAN ORGANISATION FOR SECURITY

European Organisation for Security

ECS EUROPEAN CYBER SECURITY ORGANISATION

European Cyber Security Organisation

CYSPA EUROPEAN CYBER SECURITY PROTECTION ALLIANCE

European Cyber Security Protection Alliance

TÜRKAK Personel TS EN ISO/IEC 17024 AB-0021-P

ISO 17025 - Laboratory and Testing

CERT AUTHORIZED TO USE CERT — CARNEGIE MELLON UNIVERSITY CERT IS A REGISTERED TRADEMARK OF CARNEGIE MELLON UNIVERSITY

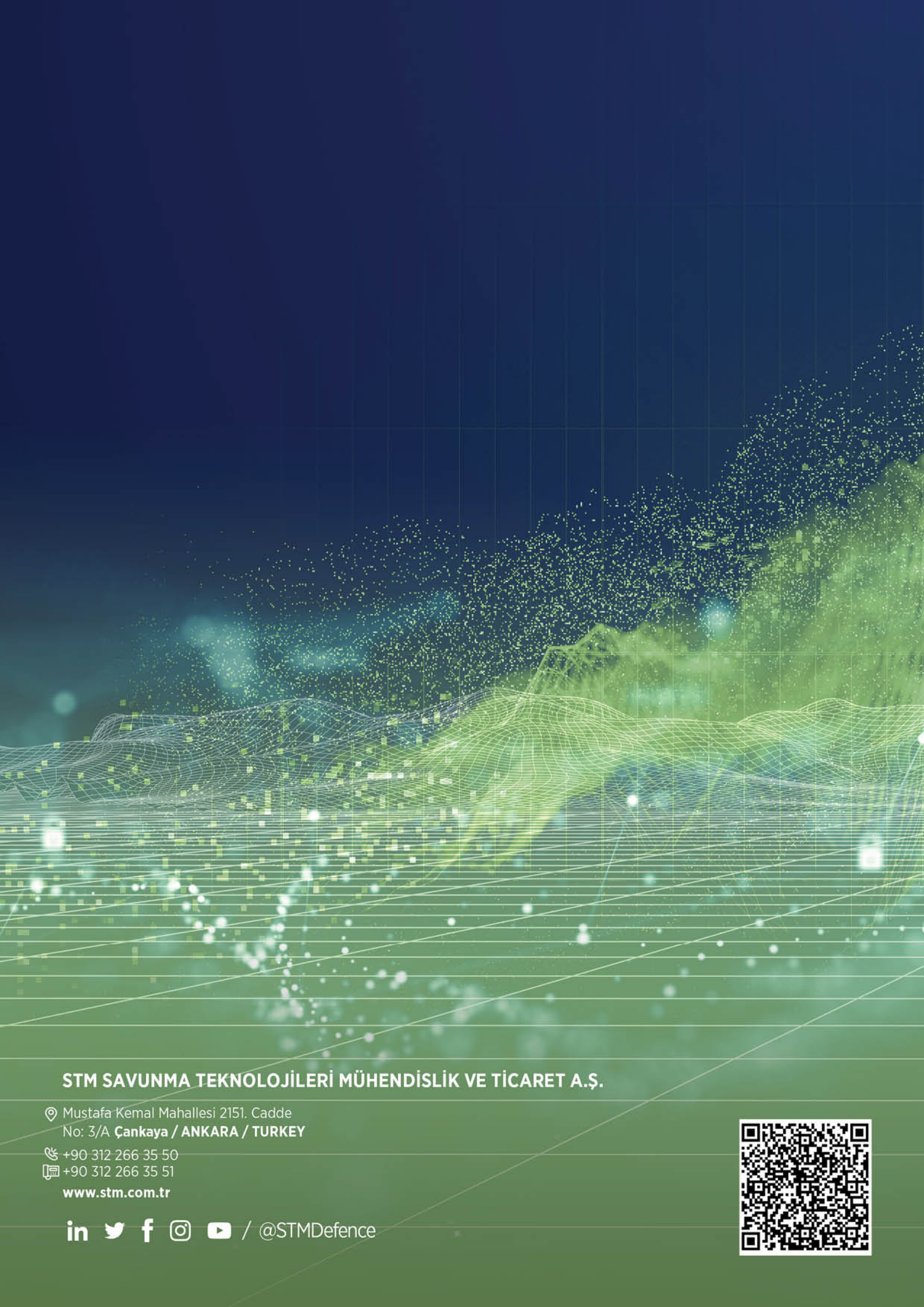
Computer Emergency Response Team (CERT)

TSE

TSE Penetration Test Company Certificate

MISP Threat Sharing

MISP Threat Sharing



STM SAVUNMA TEKNOLOJİLERİ MÜHENDİSLİK VE TİCARET A.Ş.

Mustafa Kemal Mahallesi 2151. Cadde
No: 3/A **Çankaya / ANKARA / TURKEY**

+90 312 266 35 50
+90 312 266 35 51

www.stm.com.tr

/ @STMDefence