Cyber Security

SOLUTION CATALOG

ÖLÇSAN
"kalitenin ölçüsü"

GENERAL

ÖLÇSAN, which has taken part in international projects and with its authority team in its field, is committed to leading finance, e- commerce, defense, education, industry and state institutions in our region; It provides the power and flexibility of domestic / national and open-source technologies with its world-class corporate support teams.

NIST Cyber Security Framework

360 Degree Field Domination in Your Networks

With the "ZeroTrust" paradigm, which accepts as insecure as the WAN in the LAN, the local and national solutions that allow you to focus your attention on what you really need to protect, and that can remain at manageable costs with the use of open-source components while doing this, differentiate with real defensive solutions in many corporate networks in Turkey. Today, the NIST Cybersecurity Framework has become mandatory for federal agencies in America. All institutions globally use and benefit from this framework as a guide. As ÖLÇSAN, we act with our " DETECT-PROTECT " philosophy by customizing this framework with our own experience.

APPROACH: "ZERO TRUST" and DEFENSIVE SYSTEM SECURITY

With the “SecOPS” approach, we provide security services independent of the operating system and application, and with sustainable processes in line with your needs, central and easily manageable. We help you build Zero Trust Network Architecture (ZTNA) with our authority expertise in this field, where there will be no gaps around the secure core in the corporate network. We support you in the implementation of your Monitor -> Analyze -> Detect -> Response processes, which allow you to monitor horizontal movements (Lateral Movement) in your networks.

SOLUTIONS

ÖLÇSAN offers solutions in all layers of cyber security (L1-L7) based on the principle "WE MUST DIRECT OUR DEFENSE ACCORDING TO THE THEORY WHERE ATTACKERS ALREADY ARE IN OUR NETWORK".

NETWORK AND INFRASTRUCTURE SECURITY

Network security can generally be summarized as protecting the data sources of the organization from simple user errors and malicious attacks.

In the field of network security; Security analysis, Security controls, Improvement and update, In addition to its services; We offer Firewall, Network-based IPS, VPN, Secure Web Gateway, Data Leak Protection (DLP), Dual Authentication (2F Authentication), Anti-Virus and Anti-Spam products selection, installation, configuration and management solutions.

APPLICATION SECURITY

Applications work with resources allocated to them. Applications determine the use of these resources through application users, respectively, in the way determined by application security. With the advancing technology, critical commercial applications of institutions have now combined with web technologies and started to be widely used.

With the advantages of this technology, the dimensions of the risks to be faced have also changed. Controlling the security of web-based applications and eliminating the detected security vulnerabilities have gained great importance. About Application Security; We offer Testing and Reporting, Application Firewall, Application Scanner, Application Configuration solutions.

DATA SECURITY

Data loss prevention (DLP) software and tools monitor and control endpoint activities. It filters data streams across corporate networks and monitors data in the cloud to protect data at rest, moving, and in use. DLP also provides reporting to fulfill compliance and audit requirements (KVKK, PCI etc.) and to identify areas of anomaly.

WEB SECURITY

Our Web Security Solutions protect your users against threats such as today's ever-changing malware, targeted attacks and ransomware variants, including WannaCry, with multi-layered integrated protection to protect your users' endpoint e-mail, web, SaaS applications regardless of network or campus. provides.

With adaptive DLP technology for web, social media and cloud applications, real-time monitoring and inspection can only prevent or remove confidential information from leaking, while allowing the rest of the web traffic to continue without annoying quarantines or false alarms. Optimized for data privacy and legal compliance. (PCI, HIPAA, GDPR, etc.).

While protecting employee privacy and safety, your brand should be protected from inappropriate social sharing. Social media communications are cleaned to ensure brand integrity, prevent confidential information leaks, and protect against targeted phishing and malware attacks.

END POINT SECURITY

It offers an effective defense against advanced threats that target your organization without straining your resources. Our multi-layered approach protects you from attacks, combining powerful protection, detection and response technologies in one rugged integrated solution. We offer antivirus, end-to-end encryption, logging, etc. solutions.

SECURE MESSAGING and COMMUNICATION

OLC-MSJ, an in-house professional messaging software that you can install on your own servers, is an indispensable solution for those who prioritize security with its military grade encryption feature.

All text and file forwarding messages are logged on both the client and server side, making jobs traceable. In addition, message delivery is provided precisely through ODAK Meet, which we have developed. You can remotely connect to the computers of all ODAK Meet users in your organization and support them. It gives full access to computers even when out of the office. FOCUS Meet allows you to import users from your Active Directory, LDAP server, or a pre-registered address book. All incoming and outgoing FOCUS Meet messages are encrypted using military standards AES256.

Accessing FOCUS Meet is safe when you connect to Wi-Fi, even in public areas such as airports, hotels, cafes.

IDENTITY AND ACCESS MANAGEMENT

With our user and authentication solutions developed with advanced high security Open Switching Infrastructure (AAA), biometrics, smart card systems support and information security algorithms, we ensure that the systems used by both system administrators and end users are prevented from unauthorized use and access.

MOBILE SECURITY

Anti-virus, Web Control, Identity Protection, Anti-Exploit, Web-based central management console, easy-to-use and reporting features, Active Directory Integration Installation with GPO and Push Deployment, in-house update servers, Syslog and SIEM integration. With biometric facial recognition-based identity verification, our company offers the most advantageous solutions and services in determining and applying mobile security technologies according to the needs of the organization.

SECURITY OPERATIONS AND EVENT MANAGEMENT

Security information and event management (SIEM); It has been developed to include advanced analytics such as user behavior analysis (UBA), network flow instincts, and artificial intelligence to accelerate detection for incident response and remediation, as well as seamlessly integrate with security management, automation and response (SOAR) platforms. It also sets a good example for the use of SIEM in compliance with legislation and corporate standards. We offer solutions in this area with local, global and products developed by our company.

CLOUD SECURITY

Within the scope of cloud computing, we provide the highest level of prevention and pre-attack detection and prevention system solutions with secure data transmission, secure software interfaces, secure data storage, user access control and data segmentation against the possibility of capturing and deleting data stored online.

INFORMATION SECURITY and RISK MANAGEMENT

The Information Security Management System is an international system that helps companies protect their financial data, intellectual property and sensitive customer information. You can define your company risks, manage or reduce the risks of your confidential information in the Information Security Policy, which forms the basis of the Information Security Management System solution. With risk management and assessment, we can investigate and identify your risks, observe the effects of these risks on various activity stages, and rank these risks according to their priorities in order to protect them from possible damages and we offer a method and strategy development solution accordingly. We provide solutions for the ISO 27001 Information Security Management certificate in the preliminary, consultancy, internal compliance and audit topics.

FRAUD AND PROCESS SECURITY

Online fraud has become a problem for many different business sectors. Apart from the finance sector, program providers and e-commerce companies are also affected by this situation. It requires additional security measures such as minimizing fraud and ensuring internet security, improving the user experience and multi-directional authentication.

By analyzing behavioral and biometric data, device reliability and non-personal metadata, it provides an environment for the user to log in without any specific action during authentication. Site / program security and criminal data control take priority.

DIGITAL RISK MANAGEMENT

With the recent financial difficulties and the legal regulations issued, audits performed in the digital environment are becoming increasingly important today, rather than traditional audit methods. Continuous auditing takes place by recording, reporting and auditing transactions in real-time digital environment. It is observed that the security levels of companies have increased thanks to continuous audits. Internal and external audits are at an important point in digital risk management security.

IoT

We produce OT (Operational Technology) and Secure IoT (Internet of Things) solutions to identify extraordinary activities and possible threats within the scope of end-to-end security. With our expert team in the field of operations such as secure data communication from IoT devices that offer end-to-end encryption solutions, security of existing IoT systems, detection and prevention of existing security gaps, secure data logging of IoT devices, we offer special solutions according to customer and need on the basis of embedded systems and operating systems.

BLOCKCHAIN

The risks of exploitation, targeted attacks, or unauthorized access can be mitigated by immediate incident response and system recovery. We offer source code inspection, fraud and phishing protection solutions to prevent unauthorized access.

CYBER ATTACK INTELLIGENCE SYSTEM

Cyber intelligence is of vital importance for institutions and organizations in terms of improving capabilities in certain areas such as detecting, prioritizing threats or directing emergency response correctly. Cyber intelligence is defined as the information needed by the information technology departments of institutions and organizations to detect existing and potential threats in managed networks and to respond correctly to the incident. Cyber intelligence is obtained as a result of cyber threat research and analysis.

Why is cyber intelligence so important?

Considering the data breaches that have occurred to date, it is revealed that the activities carried out to prevent it do not provide 100% protection. Even institutions and organizations that allocate unlimited budgets on cyber security can suffer from data leaks. The new techniques and tactics that cyber attackers are working on are the most important reason for this. It is not easy to track attackers targeting critical systems, as a new strategy is witnessed every day. It should be noted that the information systems used are always likely to be targeted. At this point, the phenomenon of cyber intelligence, which includes the targets, tactics and techniques of attacks, is very important for institutions and organizations. Cyber intelligence is the most important weapon to prevent cyber-attacks.

Detailed threat analysis that requires expertise should be done to gather qualified cyber intelligence. When the data obtained with the threat analysis and the tools, tactics and techniques used by cyber attackers are combined, possible threats can be detected in the most accurate way and intervention can be provided.

IMPORTANT SOLUTION TOPICS:

CYBER ATTACK DETECTION SYSTEM

IDS / IPS systems have functions such as frequently monitoring the network, identifying potential threats and keeping event records (logs) related to them, stopping attacks and reporting to security administrators. In some cases, these systems can be used to reveal weaknesses in the security policies of the institutions. IDS / IPS can also detect attackers' network-related information gathering activities, and they can stop the attackers at this early stage.

NETWORK PACKAGE CAPTURE AND ANALYSIS SOLUTIONS

Packet Capture is a network term used to capture a data packet that crosses a specific point in a data network. When a packet is captured in real time, it is stored for a certain period of time so that it can be analyzed and then downloaded, archived or discarded. Packets are captured and analyzed to help diagnose and solve the following network problems:

- Identifying security threats Troubleshoot unwanted network behavior
- Identifying network congestion
- Identifying data / packet loss
- Forensic network analysis

Packet capture can be performed sequentially or using a copy of the traffic sent by network switching devices to a packet capture device.

Full Package Capture can capture all packages or specific parts of a package. The complete package includes two things: payload and header. The payload is the actual content of the packet, while the header contains metadata, including the packet's source and destination address.

Analysis of packet capture data typically requires significant technical skills and is often performed with tools such as Wireshark.

EARLY WARNING WITH "HONEYPOT" AND TRAP / TRAP SYSTEMS

It is a method of early detection of any infiltration activity by placing vulnerable systems in the network.

Malware honeypot emulates software applications and APIs to invite malware attacks. The malware's properties can then be analyzed to perform anti-malware or close vulnerabilities in the API.

Spider Honeypot is intended to catch web crawlers (spiders) by creating web pages and links that can only be accessed by the crawlers. Detecting crawlers helps us learn to block ad network crawlers as well as malicious bots.

By monitoring the traffic coming to the honeypot system; We can control where cybercrime comes from, the threat level, what method they use, what data and applications they deal with, and how well our security measures are working to stop cyberattacks.

5651 and LOG SOLUTIONS

We provide solutions for filtering legal content on “Prevention of Crimes Committed Through the Internet” numbered 5651, collecting, signing and storing logs from Gateway devices, analyzing and reporting time stamped records created on Firewall, Hotspot and Mirror applications.

COMPATIBILITY MANAGEMENT

IT compliance management involves meeting regulatory requirements with required standards such as NIST, ISO or CSA. These can be difficult to complete due to the amount of specific content and often require organizations to bring in experts to complete reviews.

Our IT compliance management solution is primarily used as a risk and compliance management solution for professionals to help you address and improve cyber risk and non-compliance. Our platform allows you to choose any standard you need to comply with and generates an assessment for your team to complete without requiring a consultant.

CRIMINAL DATA COLLECTION

Big Data is the amount of data produced by human and machine, caused by huge information stores, that is too large to fit into a standard database for analysis and processing. Machine learning, which forms the building blocks of intelligence, takes advantage of big data.

Data collection is the process of gathering information from relevant sources in order to find an answer to the research problem, test the hypothesis, and evaluate the results. Data collection methods;

Secondary data collection; It is the type of data published in books, newspapers, magazines, online portals. There is a lot of data in these sources. For this reason, it is recommended to work by determining limitations and criteria while conducting research. For example, criteria such as date, author, reliability level of the source, quality of discussions, detail and depth of analysis can be determined.

Primary data collection is divided into quantitative and qualitative data collection types; Quantitative data collection method: Among the methods of quantitative data collection and analysis, methods such as surveys with closed-ended questions, correlation and regression methods, mean, mode, and median can be counted. Qualitative data collection method: Qualitative research aims to provide in-depth understanding and higher level of qualitative data collection methods; Studies such as interviews, questionnaires with open-ended questions, and observation studies can be cited as examples.

Our choice between quantitative and qualitative data collection methods depends on our research area and research goals and objectives. ÖLÇSAN offers fast online and offline research solutions, providing quality data collection, coding and tabulation services.

INCIDENT RESPONSE

Incident Response is a term used to describe the process of handling a data breach or cyber-attack, including the way an organization attempts to manage the consequences of an attack or breach. Ultimately, the goal is to manage the incident effectively so that damage is limited and that damages such as both the recovery process and costs as well as brand reputation are kept to a minimum. Incident Response plan is needed. A successful Incident response plan includes the following 6 stages:

- Preparation: Creating a Central Registry System, Time Synchronization, User Account Management, System and ServiceAccount Management, Asset Management, Secure Communication, Legal Transactions
- Defining: Preview, Assignment, Using Checklist
- Scoping: Taking Action - Data Collection - Isolation
- Destruction: Identify Root Cause - Identify Rootkit Potential - Strengthen Defense - VulnerabilityScan
- Recovery: Verification - Restore - Tracking
- Lessons Learned: Creating a Follow-up Report

Organizations should have at least one incident response plan. This plan should define what constitutes an incident for the company and provide a clear and guided process to follow when an incident occurs. It is necessary to identify the teams, employees or leaders responsible for both managing the incident response and carrying out each action specified in the incident response plan.

CORPORATE VULNERABILITY SCREENING FOR CYBER OPERATION CENTERS

The main purpose of the in-house Cyber Operations Centers (SOC) is; It is to neutralize the cyber-attacks that may come to the corporate network, if possible, and to take measures. For this reason, institutions periodically purchase in-house penetration testing services. However, these tests are generally performed only once a year, which is inadequate especially against newly emerging vulnerabilities and over time causes very basic but very important security vulnerabilities to be overlooked.

Enterprise Vulnerability Scanning Tool is a solution developed to meet this most basic cybersecurity needs of organizations:

- It scans the target networks and systems periodically and automatically in the specified time periods, and presentsall the critical findings separately on the main panel screen on a service-based basis.
- It completes scanning much faster than alternative vulnerability scanning tools.
- It also shows the vulnerabilities detected on that machine for the IP selected at the end of the scan.
- It has Turkish and English support, and presents the issues identified in the screening results together with theExecutive Summary as an understandable Result Report.
- It ensures that the detected vulnerabilities are assigned by the unit manager to the responsible person on the TaskAssignment screen, the relevant person is notified by e-mail and the process is followed.
- It offers clear solutions for the most common vulnerabilities detected.
- It keeps system awareness up-to-date by scanning inventory for basic devices and services.
- It can also work offline in the Corporate Closed Network environment without the Internet.
- If desired, it can be positioned as an integrated appliance.
- It can provide log feed to SIEM and other security products operating in the CyberOperations Center.

Services

THE FLEXIBILITY OF OPEN SOURCE AND THE POWER OF COMMERCIAL SOFTWARE

We build the most appropriate and accurate solutions with Big-Data and other innovative security products that we sell in Turkey, and our open-source expertise. With the events we attend abroad, we make the most applicable Cyber Defense infrastructures applicable in Turkey simultaneously with international developments.

We provide the projecting, installation, configuration and maintenance services of products, services and consultancies with our technical experts with international and domestic certificates.

CYBER SECURITY SERVICES

In the face of increasing cyber threats, all institutions and organizations increase their universal security and data security investments. Today, many organizations operate dozens of different security technologies in an integrated manner and have difficulties in monitoring security records and detecting events. Adding to the rapid change in technologies, the difficulty of finding, training and retaining competent personnel and budget constraints, all organizations feel the difficulty of operating an effective security monitoring and incident response infrastructure.

The Cyber Security Operations Center (SOME), which is structured to meet all these needs and to ensure that organizations get the maximum efficiency from their security investments with their existing personnel, is operated according to global standards where personnel specialized in various fields work.

For the uninterrupted operation of critical business applications, we monitor the system and network structure with service monitoring tools and ensure that problems that may occur in live applications are detected in advance and measures are taken against these problems.

CYBER SECURITY OPERATION CENTER (CSOC)

Cyber Security Operations Center (CSOC); It is a special field in the institution and organization that monitors and observes information assets, computer and communication infrastructure against violations on a 24/7 basis, evaluates the violations that have occurred or may occur, and defends the institution and organization against these violations. These centers are operated and managed by a team of experts in cyber security issues such as attack detection and record management, monitoring and incident management, vulnerability analysis and malware analysis. Access / attempts to this center by unauthorized persons are prevented. In this operation center, monitoring, analyzing, reporting of cyber incidents and generating alarms are carried out.

The services to be provided by the Cyber Security Operations Center have been developed to provide four basic competencies that organizations need in the field of cyber security:

- Prevention - Detection - Intelligence - Response

The aim of the Cyber Security Operations Center (CSOC) to guarantee the level of service it provides to its customers is to enable institutions and organizations to focus on real threats among thousands of information in the fastest way possible; To ensure that these threats are intervened in a way that reduces risk and potential damage.

Services provided in the Cyber Security Operations Center (CSOC):

- Intervention to security incidents - Information security weakness analysis - Vulnerability Management - Continuous penetration testing - Application security tests - Cyber Threat intelligence – VOIP security - Security of security infrastructure - Legal compliance reporting

CYBER INTELLIGENCE SERVICE

ÖLÇSAN attaches great importance to cyber intelligence service in order to collect qualified and methodological data about existing and possible cyber threats related to institutions and organizations. The main motivation of the cyber intelligence service is to ensure that institutions and organizations understand the possible cyber security risks. With cyber intelligence studies, detailed information will be obtained about attack preparations and attack types that may seriously harm your information assets and your brand.

Your organization will have a more preventive and comprehensive approach to the protection of information assets with advanced and effective cyber intelligence service. Our expert and experienced team will warn you before cyber attackers cause irreparable damage to your systems and data, so you can be prepared for threats.

ÖLÇSAN develops the most effective products and services in order to prevent possible attacks by conducting detailed examinations on threat actors. In addition, effective steps are taken in order to eliminate threats before they start by benefiting from the work of our cyber intelligence experts in order to reduce risks, improve the ability and capacity to respond to cyber incidents, and improve the security measures of institutions and organizations.

Your achievements thanks to ÖLÇSAN cyber intelligence service:

- Evaluating the risks for your organization, analyzing the incoming warnings and ensuring your safety,
- Increasing the quality and efficiency of cyber security operations,
- Complete information on current cyber threats,
- Analyzing your system for possible vulnerabilities,
- Understanding the tactics and techniques used by cyber attackers,
- Holistic integration of cyber intelligence with security procedures.

The cyber intelligence service provides benefits in five main headings:

- Real-time cyber threat detection,
- Gaining taxonomic capability to identify cyber-attacks,
- To be able to analyze the techniques and tactics used by cyber attackers correctly,
- Performing realistic and detailed analysis about cyber threats,
- Gain key insights into your organization's overall cybersecurity.

TEST SERVICES

ISO 27001 Compliance

In your ISO 27001 work, before your application or in your periodic audits, we support you to carry out the security audits and improvement works that you need within the framework of your quality standards. We present our reports to complete the pre-audit security studies, to provide a penetration test report, to create your security roadmap if needed, to maintain your current quality and to make security improvements in periodic audits, and we follow up on open closures.

Vulnerability scanning services

Vulnerability scanning is carried out with licensed software that has an up-to-date database. It is the scan study to see if the current vulnerabilities in the scope of security exist in your network. Devices in your network are scanned for known vulnerabilities, and any detected vulnerabilities are evaluated and reported by our expert team.

Penetration testing services

Penetration test is a screening and vulnerability detection tool that includes many tests. Social Engineering, network security, DDoS tests, application tests on the internet, etc. Testing by a team of experts on information technologies in many areas is one of the most common protection and vulnerability analysis tools in detecting security gaps.

External network penetration test

This work is carried out from outside the institution, on the internet, is controlled and harmless, and there is no disruptive attempt. It is determined whether the vulnerabilities originating from basic points such as operating system, software, driver running in the server and virtual clients within the scope of security allow unauthorized interference into your network and, if any, the deficiencies found are reported together with general recommendations.

Internal network penetration test

It is a scanning study carried out by performing penetration tests on servers, network devices and clients in the network in order to take precautions against attacks that may be carried out on the internal network. Considering the structure and location of the network to be tested and the number of servers, network devices and clients in the network, the study is carried out by connecting to the institution via the internet or visiting the institution via the local network, and closing suggestions and expert team opinion for the detected gaps are reported.

Wireless network test

It includes the simulation of the attackers who are following the signals of your wireless networks, trying to penetrate the network. The wireless network is gradually tested according to different levels of attack risks, if any, vulnerabilities and improvement suggestions are reported.

Website security audit

Web application security risks specified in the lists of programs used in penetration testing such as OWASP are examined and analyzed. According to the work flow of the web page, mixed attacks are organized, vulnerabilities are detected and reports are made to close the gaps.

DDOS Test

DDoS simulation is based on bandwidth capacity, service type, infrastructure, software structure and / or architecture etc. it contains different topics. This simulation protects your traffic capacity from investments such as different attacks, unnecessary bandwidth investments, unnecessary bandwidth upgrades and / or attack routing, and helps to find the real weak point and to invest in the right spot and save costs.

Application Load and Stress Test

In order to reveal the findings that cannot be obtained with DDOS tests, the software features of the application are determined by security experts who are software expertise, load and stress tests are performed, application errors and weaknesses are determined at the code level and made safe.

Inspection of Specially Written Applications

It is one of the critical areas for security audits. It is important to perform manual inspection of specially written applications. With the knowledge of secure software development by our software development team, the features that should be found in secure software are reviewed, software audit is performed and reported.

Social Engineering

Considering that the weakest link in the security chain is human and carries weakness, we identify possible security risks with social engineering audits, and help establish procedures and rules against risks with awareness trainings.

GDPR Compliance

We support the discipline that your institution develops within the scope of GDPR law with our penetration test studies and GDPR audits. In addition, while conducting all of our work with sensitivity to personal data, we take care to ensure that the data is stored in the right areas, access is controlled and not disclosed during the work.

Awareness Trainings

Apart from the systemic measures that can be taken against the reported gaps, human measures are of greater importance. Information security trainings for all users who take place in humanitarian measures and institutions and who may cause vulnerability in the system, from the most basic level; Informative trainings are provided up to the problems we may encounter in our daily life.

MAINTENANCE AND SUPPORT SYSTEM

IT Security Products and Systems Maintenance and Support; It is the technical support services provided in accordance with certain service levels in order to ensure the continuity, data integrity, accuracy and confidentiality of the IT systems of service users, the establishment of information security support products and systems, to eliminate hardware and system problems and to ensure smooth operation. It is executed on a call-based and service-level basis. It can be given "remotely" or "At Service User Site".

Maintenance and support services to be provided to information security products and systems may also cover the issues of determining information security processes and making the information flow within organizations reliable, depending on the content of the service contract between the service provider and the customer.

IT Security Products Maintenance and Support services; It can be used by all companies that are responsible for keeping the information of their business partners and customers confidential, and may be damaged by problems that may arise from information technologies, which include information technologies as an important part of their workflow, impairing the continuity, integrity and confidentiality of their workflows.

Consultancy

CYBER SECURITY FRAMEWORK CONSULTANCY

Cyber security and information security consultancy aims to protect institutions from internal and external threats. Cyber security; The institution aims to verify the confidentiality, integrity and accessibility of the information and to carry out the necessary procedures for the correct implementation of information security policies during transmission and storage. In order to ensure the continuity of these processes, cyber security consultancy has become mandatory during the developing technology and renewed cyber-attacks. Within the scope of cyber security consultancy, the techniques used by malicious people who are also defined as "cyber attackers", the tools they use to detect vulnerabilities on the target system, the exploit codes used to seize the systems and attacks against web applications and the psychology of the attackers are discussed.

This service includes the service of intervening in a possible cyber incident (information theft, blackmail, hacking, etc.) and obtaining the necessary numerical evidence to be used in the resolution of the relevant incidents within the customer, analyzing these evidences and preparing the necessary reports. The general framework of the consultancy service to be provided as a result of the interviews made within the scope of cyber security consultancy is determined in line with the requests from the customer and the inventory of the institution and its presence in the internet environment is mapped by the expert staff of ÖLÇSAN Cyber Security. Then, methods such as penetration tests, web security or local pentest are applied. The results of these methods and tests are analyzed and the cyber risk map of the institution is drawn and the most accurate guidance and suggestions for the security investments that need to be made are provided by our experts. In this way, the institution is enabled to take direct measures against cyber-attacks against itself, and irreversible expenses are prevented.

SECURITY INSPECTIONS AND LEAKAGE TESTS

Penetration Testing (penetration test) is mandatory to detect potential security vulnerabilities before risk occurs. Therefore, security audits and / or penetration tests are required in all regulations such as PCI, ISO27001, SoX / Cobit.

ÖLÇSAN offers two different services under the headings of penetration testing and security audits with information security experts with Certified Ethical Hacker (CEH) certification. Security audit tests are often used for regulatory compliance, and do not include DoS / DDoS, system penetration, proof or evidence release.

Our audits are as follows;

- Internet security audit
- Web application control (including web applications that can be entered with username and password)
- Security product jump controls
- Third party testing (domain name, google hacking)
- DoS / DDoS inspection
- Local security audit
- Wireless network security audit

SECURE CODE DEVELOPMENT CONSULTANCY

In today's world, 75% of the applications are web applications and most of them are critical applications such as banking and e-government sites. It is of great importance that these applications, which save money and time, are user-friendly, always accessible, performance and "reliable".

The importance of the concept of secure software development is well understood today, and this concept has been accepted as a factor that reduces software development cost and time and increases the quality of the software. In addition, it is the most effective way to prevent many security incidents that may occur during the use of software.

ÖLÇSAN provides consultancy services to institutions in order to establish the "Secure Software Development Life Cycle". Knowing that it is necessary to create a security layer as soon as the application starts to be written, it ensures that the application is both accessible and reliable by analyzing source code, and analyzes the performance with load tests. It also performs security tests to detect vulnerabilities in currently developed applications.

In addition, it provides "Secure Code Development Trainings" to ensure that the teams developing code are knowledgeable about this issue and that the security factor is always taken into consideration.

INFORMATION SECURITY MANAGEMENT SYSTEM CONSULTANCY

ISO 27001 Information Security Management System (ISMS) is a management system based on security controls determined by risk management and the continuous improvement of these controls. In order to protect the confidentiality, integrity and usability of the information of the institutions, it is necessary to prepare and implement the risk management and risk processing plans, business continuity plans of duties and responsibilities, emergency incident management, information security operational procedures and their records. Within all these activities, a series of Information Security (BG) policies and procedures should be published and the personnel should be made aware of information security.

ÖLÇSAN Information Security prepares your company for ISO 27001 certification audit by implementing all ISMS processes together with you with ISO 27001 Information Security Management System consultancy service. This service starts with the determination of the scope document and ends when the company receives the document. The ISO 27001 Standard defines the requirements for organizations to establish an information security management system. ISMS requires the evaluation of all information assets in your organization and a risk analysis that takes into account the vulnerabilities of these assets and the threats they face.

SAFE PROCESS MANAGEMENT CONSULTANCY

Information Security should be operated as a part of the business processes of the institutions and should be carried out within the framework of corporate policies and rules. ISO / IEC 27001 Information Security Management System (ISMS) is an international standard that defines the needs. It ensures that information security is included in the business processes of the institution, that information security becomes a living process, that policies and compliance are monitored, improved and developed, and the information asset of the organization is protected. The ISO 27001 framework offers a customizable framework according to the information systems infrastructure of the institutions. In order for your organization to successfully integrate ISO 27001 processes within the scope of ISMS, the ÖLÇSAN Cyber Security Consultancy team observes your current situation, determines your needs and provides your needs to be ISO 27001 compliant.

COMPLIANCE CONSULTANCY WITH THE LAW ON PROTECTION OF PERSONAL DATA

The Law No. 6698 on Protection of Personal Data, which entered into force on April 7, 2016, aims to protect the fundamental rights and freedoms of individuals, especially the privacy of private life, in the processing of personal data, and to regulate the obligations and rules to be followed by natural and legal persons who process personal data. The provisions of this law are applied to real persons whose personal data are processed, and real persons and legal entities who process such data completely or partially automatically or by non-automatic means provided that they are part of any data recording system. Relevant persons should

be informed in the most transparent way about the ways in which personal data are collected, the purposes for processing, legal reasons and rights.

In terms of crimes related to personal data, the provisions of Articles 135 and 140 of the Turkish Penal Code No. 5237, dated 26/9/2004, are applied. According to the law, those who violate personal data are sentenced to imprisonment from 1 to 3 years. In addition, a prison sentence of 2 to 4 years may be imposed on the person who obtains this data through violation.

Relying on our experience in data security, we provide all the consultancy services and necessary products you may need regarding the Personal Data Protection Law. We offer solutions to take technical precautions in the most appropriate way, taking into account the legal aspect of the issue. It is our priority to help our customers to be compliant without penal sanctions stipulated by law.

EKS / SCADA SECURITY CONSULTANCY

It is used in all critical infrastructures such as energy and natural gas infrastructures, water networks, health systems, defense industry infrastructures, nuclear facilities and production facilities, and the concept of security emerges as an important concept that should be considered in the design and operation of these systems. In scenarios where the systems in question are damaged and become inoperable, it is possible that large-scale material and moral damages may occur. Based on its experience in cyber security, ÖLÇSAN offers comprehensive services to ensure the security of EKS / SCADA systems. Security analysis to be made on these systems requires a versatile and meticulous work.

- Security Tests are subjecting the components on the infrastructure to the security test with the least information with an attacker point of view. These tests include the inspection of all possible infiltration points associated with EKS / SCADA networks. In addition, EKS / SCADA components are subjected to penetration testing.
- Configuration audits are the auditing of the components that concern the security and continuity of the EKS / SCADA infrastructures within the infrastructure, through the eyes of the system administrator.
- Process audits are the auditing of operating processes from the point of view of security. Within the scope of this audit, basic processes such as change management, record / log management, capacity management, physical security, human resources security are audited according to generally accepted standards such as NIST SP800-82, ISO 27019, ISO 27001.
- Physical audits, control rooms serving critical functions within the infrastructure, data centers and the overall security situation of the enterprise are audited according to best practice examples.
- EMRA Industrial Control Systems Information Security Regulation Compliance Services are provided with consultancy services on inventory taking, risk analysis and risk action plans as stipulated by the regulation, and organizations are ensured to comply with the regulation.

TRAINING

ARTIFICIAL INTELLIGENCE USAGE IN CYBER SECURITY

It is known that artificial intelligence and machine learning provide some important advantages for modern cybersecurity applications over traditional applications. The power of machine learning applications to present the findings on experience-based learning and how to follow a strategy when faced with similar problems in the future can be considered as an advantage over traditional passive applications. Machine learning plays a role in helping organizations improve their capabilities across all five security categories, such as prediction, prevention, detection, response, and tracking.

It can learn from existing data to make decisions when encountering new data in areas such as machine learning, network traffic analysis, fraud detection, and user behavior. This allows it to detect different types of attacks across security layers, from network to application, endpoint, and user level.

Our training titled "Artificial Intelligence in Cyber Security" is intended to teach institutions how and where artificial intelligence and machine learning methods can be used in the field of cyber security. It is aimed to rearrange the data with pre-processing, to obtain prediction and classification models by applying machine learning algorithms, then to apply the testing and evaluation processes of these models on real data sets and to create awareness. In education, especially focusing on deep learning algorithms, algorithms such as Recurrent Neural Networks = RNN, LSTM and Autoencoders based on Tensorflow, Keras libraries are applied on datasets.

IDENTITY MANAGEMENT TRAINING

It is aimed to discuss the different systems and strategies that can be applied in performing authentication control in large-scale institutions and public spaces requiring access control, to explain the appropriate solution options and to raise awareness.

Main Topics:

Existing Identity Management and Access Control Systems, Examples from Turkey and the World - Vulnerabilities of existing methods and the problems encountered in applications - The first step of end-to-end security Authentication - Two and three factor authentication methods - Strong authentication - Hardware system elements and technical features - Software scope and Multiple campus group management - Visually controlled access systems (person recognition, movement, second person presence detection, image optimization, black list / black list applications) - The importance of physical and virtual access integration.

END POINT (EDGE) SAFETY TRAINING

With the development of technology, the prevalence of electronic IOT (Internet of Things) devices is increasing rapidly. The security of your data on the device is very important for the users as well as the use of the devices. One of the most concentrated issues of companies and entrepreneurs who want to create a new IOT product is that the data of the device is encrypted and sent during data communication and the access is blocked by third parties. In our "Arduino and IOT device design and security" training, our entrepreneurs who want to produce a new IOT device and use the product for commercial purposes, what is an arduino card, how to program it, creating a circuit with arduino and producing an IOT project, understanding of encryption and security in IOT communication with various applications. it is aimed to achieve the gain.

IT AWARENESS TRAINING

The primary risk that threatens information security is the lack of awareness of the employees about security. When the information security violation incidents experienced by world-renowned IT companies in recent years are examined in detail, it is revealed that the main source of the problem is the lack of

information security awareness of the employees.

One of the most important items in raising the awareness level of the employees is to provide regular training and attack applications that include awareness scenarios after the training.

For this purpose, the following trainings are applied:

- Information Security Awareness Training
- ISO 27001 Information Security Management Training

LINUX OPERATING SYSTEMS SECURITY TRAININGS

Understanding security settings and tightening methods in Linux and Windows environments, increasing the security of user privileges and accounts with sample scenarios, preventing attacks, blocking accounts, installing and configuring, file encryption, encrypted communication, creating access lists and scanning for vulnerabilities. User Accounts and Security, Authorized users, Linux Password Compression, Compression of the Linux Firewall, Encryption Technologies, SSH Security, File and Folder Authorization Management, SELinux, ClamAV, RootkitHunter, Log Management and Log Security constitute the content of the training.

BASIC CYBER DEFENSE TRAINING

The Cyber Operations Center, Network Security Monitoring, Cyber Security Monitoring and Endpoint Security are explained in a holistic framework supported by sample scenarios.

SOME Processes;

National Cyber Security Strategy and Action Plan, SOC Objectives and Activities, SIEM Solutions, Defense Tools and Solutions, Modern Defense Mechanisms, Attacker Based Detection, Network Security Monitoring, Honeypot Systems, Continuous Security Monitoring, Situational Awareness, Application Monitoring and Tracking, Configuration Change Management, Log Management and Monitoring, Endpoint Security, Manager Accounts Monitoring and Management, Threat Hunting, Cyber Intelligence, Authorization, Post-Authorization, Reputation Based Detection, Anomaly Detection and Analysis, Packet Analysis, Signature Based Detection, Session Analysis, Sensor Platforms Risk Management and Planning, Threat Hunting and Threat Intelligence Concepts constitute the content.

WEB APPLICATION SECURITY TRAINING

At the end of this training, the participants will learn how to detect and use vulnerabilities in web applications.

Web Application Technology and Security Components, Database Systems, Web Application Vulnerabilities, Authentication, Injection Attacks, XSS, NoSQL Applications, Javascript Based Web Applications, Malicious File Upload Attacks, CSRF, IDOR, Backdoor Creation, Information Gathering Methods, Web Vulnerability Scanning Tools, Web Application Firewalls, WAF / IPS / IDS Avoidance Techniques, Web Services, LDAP Injection.

SECURE SOFTWARE DEVELOPMENT

It is aimed that the participants learn about the security vulnerabilities by experiencing them personally and then write code that does not cause these vulnerabilities.

Secure Software Development Architecture and Cycle, Threat Modeling, Risk Quantification, Verification Tendency and Skeptic Approach, Identification of Basic Web Vulnerabilities, Input Controls, Authentication / Authorization Difference, Content Isolation Logic, Inheritance of Origin, Life Outside Same-Origin, Content Identification Mechanisms , Libraries from Uncertain Sources, OWASP-10, Implementation of the Whitelist Approach, ESAPI Architecture and Methods, Using Prepared Statement / Parameterized SQL, Object Relational Mapper, Secure File Upload, Secure Authentication, Using Secure CAPTCHA and Avoiding It and Secure Session Management content constitute.

www.olcsancad.com info@olcsancad.com T: +90 (212) 216 5080

ÖLÇSAN
"kalitenin ölçüsü"

CYBER_TR.03 / 2021