EDGE TEAM TECHNOLOGY

CYBERSECURITY SERVICES

MANAGED FIREWALL

Administered by certified Security Engineers, this best-in-class threat prevention service can be delivered in conjunction with a newly-provided firewall or with existing customer hardware.

- **24x7 Monitoring:** Round-the-clock prevention and detection of threats.
- **Device Management:** Configuration changes, policy audits, patch management, control rules customization, device backups.
- **Threat Response:** Resolution or mitigation of risk in the event a vulnerability is discovered or a security event occurs.
- **Compliance Standards:** Reporting to ensure that implementation meets all necessary compliance requirements such as PCI DSS, HIPPA, Sarbanes-Oxley, etc.
- **Tier 1 Partners:** Palo Alto Networks, Fortinet, Juniper and Cisco

PENETRATION TESTING

A simulation of real-world attacks to provide a point-in-time assessment of vulnerabilities and threats to your network infrastructure. CVE and community-sourced exploit databases are utilized to probe selected devices on the customer network. Multiple tools are harnessed to attempt access via either a code bug or by brute force.

Rules of engagement are developed to ensure no business impact occurs during the testing. Our Security Engineers will not engage in test attacks that may have a drastic impact on business, such as Distributed Denial of Service attacks.

Any hosts discovered to have vulnerabilities are documented and exploited to gain access to systems outside of the intended network or segment.

VULNERABILITY SCANNING

Detection of network vulnerabilities via the scanning of selected devices and reporting of potential exposures.

External vulnerability scans are performed by our partner Tenable for PCI ASV from our data centers or cloud servers. Internal scans are performed via a VPN tunnel or onsite appliance. Scans are configured based on customer timing preferences.

Reports are generated and reviewed by Security Engineers after each scan. An evaluation is performed to ensure the network is secure and a mitigation plan developed in the event of a discovered anomaly.

PCI-ASV scanning for quarterly compliance is also available

MULTI-FACTOR AUTHENTICATION

- **Network IDS:** Automated inspection of all network traffic
- **Host IDS:** Inspection of servers for intrusion attempts and integrity changes of critical system files

These services are accomplished through the use of a lightweight agent that is installed on each network server. Based on predefined policy sets, the IDS system alerts our Security Engineers who analyze, validate, and remediate the incident, including customer notification and consultation. Low level alerts will be compiled and submitted in regular monthly reports.

CONTENT FILTERING

We have partnered with OpenDNS to provide a DNS-based solution which allows for various categories of websites to be blocked from corporate users. Policies are configured based upon customer requirements which block traffic from unallowed DNS servers. If a user attempts to access an unauthorized site category, a redirect notice offering a method to contact the support team is offered.

Corporate security is enhanced by the blocking of known botnet hosts and phone-home mechanisms. Monthly detailed reports with blocked attempts are available to the customer.

GDPR CONSULTING

There are four major sections of the GDPR: Governance, Monitoring, Data and Metadata Classification. Each of these sections will be addressed and evaluated including the right to be forgotten.

Data Protection Impact Assessments are conducted to validate compliance with the GDPR regulation. An investigation of current security in place and data handling procedures is performed and findings compared to the standards.

The deliverables set includes recommendations on the correct policies, procedures and systems for each enterprise.

ADVANCED MALWARE PROTECTION

We utilize Cylance, the best-in-class platform for protection against zero-day malware, privilege escalations, scripts, system and memory based attacks or programs for accessing malicious files or systems.

A Cylance software agent is installed on each defined workstation or server. The program utilizes Artificial Intelligence to detect abnormal behavior of customer programs or files. Once behavior patterns of suspected attacks have been confirmed, the software will halt the process and alert our Cybersecurity team.

Implementation, monitoring, updates, and threat and status reports are provided.

MANAGED EMAIL SECURITY

We have partnered with Mimecast to provide a complete Email security platform. Mimecast's Advanced Email Security with Targeted Threat Protection uses multiple sophisticated detection engines and a diverse set of threat intelligence sources to protect email from spam, malware, phishing, and targeted attacks.

The Mimecast services defend against email-borne impersonation attempts, malicious URLs and attachments, threats that are internal to the organization, and attacks from¬¬ the inside that are destined for external recipients.

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

Our SIEM system scans all nodes on the customer network and the interactions between them. Aggregate logs are obtained and processed through a database of known vulnerabilities and interactions.

The SIEM system utilizes its correlation engine on these events to assign a risk rating and determine whether events within a time window may be related. The system utilizes multiple resources to generate a comprehensive threat database including:

- Enterprise Vendor Threat Databases
- Open Source Threat Databases
- High Interaction Honeypot
- Community contributed threat data

Machine learning is utilized to create a trust score for all external IP ranges, URLs and traffic patterns individualized for each environment.

Threats, alarm conditions, and compliance anomalies are detected, assessed, and remediated, with regular reporting on network security health.

SECURITY AWARENESS TRAINING

Through our partnership with Knowbe4, employee Security Awareness Training is provided to help protect the integrity and confidentiality of company information.

Rules of engagement are established and customized phishing and social engineering campaigns are created. These campaigns are randomly sent to employees to assess their current awareness of common tactics used by malicious users. Based on those interactions, employees will then be enrolled in specific training which will review security best practices.

A second level of training includes a detailed and customized training for the customer's industry. Employee interactions with these email campaigns will be tracked and provided to the administration group for review. Remediation and training recommendations are provided by the Edge Security team to ensure understanding of the results and for preparation of ongoing campaigns.

SECURITY ASSESSMENT SERVICES

We offer security assessments ranging from firewall configuration checks to company-wide policy reviews. PCI-DSS compliance can be guided by our security team who will review the controls and processes.

Our engineers possess a keen understanding of the specific regulations pertaining to local compliance based on geographic location. We will assist in data mapping and in the creation of data flows.

In preparation for a potential security event, the consultant will assist in the formation of a Data Breach Response Plan. This document will detail how to act swiftly, mitigate losses and perform proper reporting to regulatory boards.

INCIDENT RESPONSE & FORENSIC SERVICES

Early detection and response is the key to protecting critical assets, so when an attack happens, your response must be swift. In the unfortunate event of an incident, we provide on-demand incident response teams to quickly help clients manage and contain damage.

Our On Demand Incident Response team provides:

- Immediate needs taken care of to ensure your organization is back up and running as quickly as possible
- A team of cybersecurity analysts and incident responders when you most need them
- A breach remediation plan based on the nature and scope of the attack