MANAGED SECURITY SERVICES PLAN

In today's complex network environment system security is quickly becoming the most important and critical need for all companies regardless of size. Our Managed Security services were built to support the dynamic landscape of cyber security.

THE TRANSFORMYX DIFFERENCE

In Transformyx's 30 years in business we have combined our skills and years of experience to continuously adapt to the ever-changing technology industry and respond to the needs of our customers. Our ever-changing business, has propelled us forward to be at the forefront of what modern enterprises need today and allow us to be a forward-thinking, agile organization.

SCOPE OF WORK INCLUDES (BUT NOT LIMITED TO):

- vCISO
- Information Protection Program creation and annual review
- Monthly Scan for Vulnerability Assessment (Remediation actions sent to MSP team)
- Annual Penetration Testing (Internal and external)
- Unlimited Phone Support (M-F 6am-6pm)
- Service availability Monitoring Maintenance 24/7
- Security MSSP Tool Optimization and Management
- New Configuration or Deployment not Included

SEE BACK FOR MORE INFO

Transformyx

DATA CENTER · VOICE · IT SECURITY

vCISO:
CISO consultation covers executive-level initiatives such as program/plan/policy creation and review, budget creation and analysis, analysis of processes and security controls, workforce security training, communication practices, identification of security objectives and metrics, supplier risk management, oversight of risk management activities and penetration testing, manages the incident management program, and other CISO related activities. Also represents the client's interests for any 3rd party audits that may occur as needed.

Information Protection Program (IPP):
An Information Protection Program is a documented set of information security policies, procedures, guidelines, and standards that apply to your business. The IPP will help customers ensure the confidentiality, integrity, and availability of client and customer information, as well as the organization's essential data. The program will establish the policies and processes that will be used to protect company information. An incident management plan, enterprise security architecture, and threat and vulnerability management are all components that will help customers understand where their data lives and what processes are in place to protect it. The IPP will have multiple components and subprograms to ensure that your organization's security efforts align to your business objectives.

Monthly Vulnerability Management:
TFMX uses Rapid7 Nexpose for vulnerability scanning. Software (Adobe, MS Office, Java), Operating systems (Windows, Mac, Linux), networking devices (routers, switches, firewalls, wireless access points), and any other devices that connect to a customer network have new vulnerabilities that are discovered almost every day. In order to maintain a secure computing environment, these vulnerabilities must be detected and remediated regularly. TFMX will conduct monthly scans of all assets to detect these vulnerabilities, including required patches and updates, weak passwords, and insecure configurations. A report will be provided each month describing discovered vulnerabilities and remediation steps.

Penetration Testing:
Annual Technical network penetration test which will utilize social engineering and common exploits. A Penetration Test, or PENTEST, is a security testing in which evaluators mimic real-world attacks to identify ways to circumvent the security features of a network. Penetration testing often involves issuing real attacks using the same tools and techniques used by actual attackers. Most penetration tests include looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. A detailed report of the test results will be provided to the customer with remediation recommendations.

Incident Response:
Unfortunately, in today's landscape, even the most heavily protected networks can occasionally experience an incident. This can include a virus or malware outbreak, stolen credentials, email hijacking/spamming, or ransomware, among others. TFMX cybersecurity experts will use an organized approach to address and manage the aftermath of a security breach or cyber-attack, also known as an IT incident, computer incident, or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. The phases of the incident handling lifecycle are: (1) Preparation; (2) Identification; (3) Containment; (4) Eradication; (5) Recovery; (6) Lessons Learned. TFMX will provide an incident report to the customer explaining how it was resolved, and recommendations to prevent a similar incident going forward.