Sustainable Security Solutions

Our Mission

The EITS mission is to “To understand each customer’s unique needs, guide them toward the right security investments, and provide the best possible professional services to defend their people and data.”

EITS

Enterprise IT Security

Our People

EITS believes the key to maximizing security investments is the right professional services (PEOPLE) supporting the assessment, design, deployment, and long-term enablement. EITS puts a heavy focus on manufacturers' certifications in order to deploy best-of-breed security solutions across the industry. It is the people who make the difference when it comes to any product or service, and our mission is to ensure we have the right people to best enable our customers' security programs.

What We Do

Security - we "do" security, and we do it well. For the technically minded, following SANS Controls provides a solid foundation for a secure infrastructure. Our service offerings align and address these controls, ensuring a cohesive all encompassing solution that is not only achievable, but sustainable. The icons in the below SANs list coincide with the EITS Offering icon that addresses the control.

Top 20 SANs Controls

1. Inventory Hardware	11. Configuration Management Unmanaged Systems
2. Inventory Software	12. Boundary Defense
3. Configuration Management Managed Systems	13. Data Protection
4. Vulnerability Management	14. Controlled Access Based on Need to Know
5. Identity & Access Management	15. Wireless Access Control
6. SIEM / MDR	16. Account Monitoring & Control
7. Email / Web Browser Protection	17. Skills Assessment & Training
8. Malware Defense	18. Application Software Security
9. Control of Network Ports, Protocols & Apps	19. Incident Response Management
10. Recovery Capabilities	20. Penetration Testing & Red Team Exercises

Offerings

Asset & Application Inventory

SANS critical security controls 1 and 2 define that an organization should have positive control of assets and applications to effectively develop a comprehensive security program. This challenge spreads far beyond managed servers and endpoints running modern operating systems (windows, mac, chrome, etc.) We typically find a large percentage of unknown devices on the network such as printers, cameras, sensors, thermostats, and a wide variety of production equipment (SCADA, ICS, etc.). Understanding these devices and their security posture is key to any organization's successful risk mitigation.

Assessment & Enablement

EITS assesses each customer's current security controls, supporting processes, skills base and potential risks/areas for improvement. Utilizing assessors with skill sets key to the industry and/or specific compliance requirements, we gain clear insight as to where customers stand within the Cyber Security Maturity Model. This enables EITS to tailor fit each customer's unique needs into a statement-of-work - ensuring expectations are understood and exceeded.

Incident Response

EITS has you covered 24/7 x 365 with an average onsite response time of less than 12 hours. Our team of GIAC Certified Incident Handlers expertly manage remediation activities, Threat Intelligence Experts rapidly discover and remediate threats across your enterprise, and GIAC Certified Forensics Examiners ensure the fastest time to unravel what malicious activity occurred. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

Pen Testing & Red Team Exercises

EITS has a proven process for assisting customers to test their current standing. Intelligence Gathering consists of service enumeration, network mapping, domain foot printing, live host detection, and operating system & app fingerprinting. Threat Modeling identifies assets and categorizes them into threat categories. Next, a list of attractive vulnerabilities, suspicious services, and items worth researching further is created and weighted for further analysis. Exploitation involves actually carrying out the vulnerability's exploit (i.e. buffer overflow) in an effort to determine if the vulnerability is truly exploitable. The reporting step

Offerings

is intended to deliver, rank, and prioritize findings in an actionable report, complete with evidence.

Application Security

Many customers are just getting started with the concepts of application security and the underlying support processes. Ensuring security is embedded in all states of the SDLC from requirements gathering, into design, throughout development, testing, and prior to implementation is vital. Application security becomes a program that allows our security team to continuously check apps to identify new vulnerabilities as they arise, enables our operational team to remediate, and allows a final security checkup to ensure the finding was addressed. Our team can fill the gap for many customers, the hybrid cross skill sets needed between both development/coding and security.

SOAR: Security Orchestration, Automation, and Response

Bottom line is siloed "best-of-breed" security solutions are just not enough to combat todays attackers. Implementing the automatic handling of security operations-related tasks without human intervention is crucial. Orchestration consists of connecting security solutions and integrating siloed security systems - the layer that streamlines processes and enables automation - and lastly, responding to threats proactively and timely while maintaining best practice procedures. Let our professional service team help you build or leverage API's to achieve the highest level of automation possible and get the most out of your team day today.

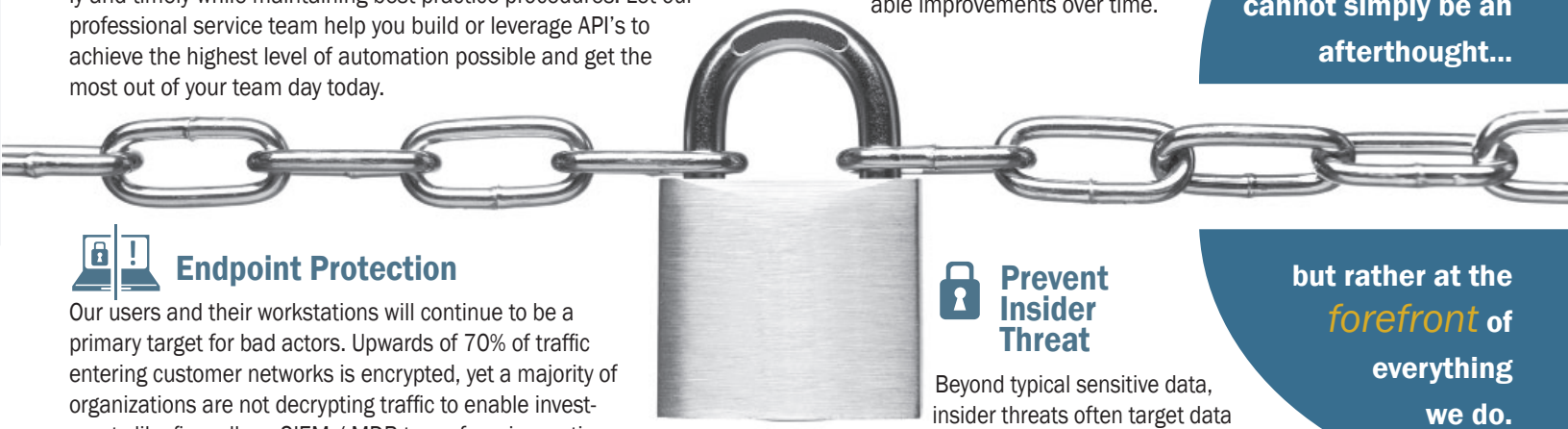
Network Segmentation & Inspection

Our network segmentation services can help customers identify the resources holding critical data we need to protect, and the underlying systems that power and access them, ensuring traffic passes through security inspection investments. This is achieved by working with customers to monitor traffic and building granular application level (layer 7) rules based on what is needed. The assessment we perform upfront enables us to eliminate subnet wide rules and legacy IP/Port-based rules.

Firewall Health Check

EITS' NGFW HealthCheck service starts with analyzing the configuration and performance of firewalls and transforms what can be an overwhelming array of data into a structured plan to get the most out of your Palo Alto firewalls. We utilize best practices, observe the types of traffic in each environment, and work with customers to understand their existing network security topology. This applies a structured, repeatable process that is tailored to each customer's environment and priorities. The HealthCheck brings visibility to opportunities for improvement, prioritizes them, enables structured remediation where needed, and reports on quantifiable improvements over time.

Because threats are *continuously* evolving, security cannot simply be an afterthought...



but rather at the *forefront* of everything we do.

Endpoint Protection

Our users and their workstations will continue to be a primary target for bad actors. Upwards of 70% of traffic entering customer networks is encrypted, yet a majority of organizations are not decrypting traffic to enable investments like firewalls or SIEM / MDR to perform inspection. Endpoint solutions are front-line defense, but like a musical instrument, it will require tuning. Our team brings industry leading hands-on experience with industry leading solutions like CrowdStrike, Microsoft ATP, and Palo Alto Cortex and can help you identify the right solution for your unique needs.

Prevent Insider Threat

Beyond typical sensitive data, insider threats often target data such as customer contacts from sales management tools or code for e-commerce sites prior to launch. EITS works with organizations to identify what information could be detrimental if lost in order to define processes for who needs access, what access levels, and what is normal functionality for those users. Identifying normal is crucial to recognizing abnormal activity.

Vulnerability & Patch Management

Vulnerability management is the combination of identifying, classifying, prioritizing, remediating, and mitigating" software vulnerabilities, a process requiring continuous development and improvement. EITS approaches vulnerability management by first ensuring we have an accurate asset inventory of all devices on the network and remediating the vulnerabilities IOT, SCADA, and ICS systems can introduce. EITS has the experts you will need to assess where your vulnerability management program is, identify / prioritize gaps, and tailor fit the right technology solutions.

SIEM (Security Information & Event Management) / MDR (Managed Detection Response)

Gathering log/event data from a firewall and endpoint protection solution is only a part of the visibility possible. We believe maximizing your SIEM/MDR requires integration between the variety of security controls within the customer environment. From Network Access Control, to Privileged Access Management, down to our Data Loss Prevention solution (DLP), our ability to enable our SIEM/MDR with the right data is key. This applies if you are looking to build and maintain a Security Operations Center (SOC) in-house or migrate toward a managed provider.

Offerings

Configuration Security Standards

National Institute of Standards and Technology (NIST) defines security configuration management as “The management and control of configurations for an information system with the goal of enabling security and managing risk.” The bad guys search for low hanging fruit like default settings, which they exploit and change. We depend on configuration management endpoints to default settings that introduce vulnerabilities, but more importantly, build process to identify and notify when these default settings change.

Email / Web Browser Protection

EITS assists in configuring ATP policies to achieve strong email and web browser security. Office ATP is a set of policies within Exchange and SharePoint online that provide greater configuration and control over an organizations data than the default policies. These policies provide advanced phishing detections, spam protections and allows an organization to train their organization against phishing attacks using simulated exercises. Defender ATP builds on top of the Windows Defender platform, bringing cloud-based detections and advanced EDR protections not available by default installations. The cloud-based dashboard correlates data such as software vulnerabilities, active attacks, and incident handling reporting.

Identity & Access Management

Enable the visibility to see and control what your users have access to using protections for Identity and Access Management from Microsoft. Active Directory on prem or in Azure serves as your source of truth while features such as Single Sign On, Multi-Factor Authentication, and Conditional Access provide ease of use and integrated security for all your local and SaaS applications.

Data Protection & Recovery

Identifying the actual data we need to protect is often more challenging than customers realize. We often see this data in network shares, random backup folders on servers, and down to end user workstations. Our assessment services support customers with automated industry leading tools that enable identification of sensitive data ensuring we can build and enable people with the right processes and technologies to protect it long term. Approaching recovery as an all or nothing approach, a common thought process, leads to astronomical expenditures that can lead to reduced retention windows across all data. The right answer is to identify what is critical, then ensure we have a short-term and long-term strategy to recovery these critical workloads and achieve RTO and RPO objectives.

Are you ready to step up your security posture? To learn more about offerings, and how EITS can make your life easier, contact a team member today.

Products

EITS consistently studies and tests the latest technologies in the market to ensure we offer customers the best-of-breed solutions. Below is our partner network:

Partner Network

Cisco	Infoblox — Control Your Network	splunk>
CrowdStrike	Microsoft Partner Network	Tanium
EMC² — where information lives	paloalto Networks	tenable
f5	proofpoint.	tripwire
FORESCOUT	SecurityScorecard	VARONIS
Gigamon	silver peak	vmware

Contact Us

EITS

Enterprise IT Security

5105 John J Delaney Dr., Ste D32
Charlotte, NC 25277
(704) 900-8042
www.eits.com