Security Battlecards

Complete guide on solutions, selling tactics, provider shortlists and more.

Cybersecurity Training & Compliance

TBI Battlecard

Top Providers

AT&T

Corvid Cyberdefense

Lumen

Synoptek

Verizon

Add-ons to Training and Compliance

- Endpoint Security
- Email Security
- Managed Firewall
- Identity Access Management
- Penetration Testing
- vCIO/vCISO
- Vulnerability Scanning

Overview

Understanding employees' security awareness and competency is critical. With end users being one of the most frequent target for vulnerabilities, ensuring staff recognizes the various strategies threat actors employ is crucial to the operations of any business. Security awareness training should be required and should include any necessary industry compliance, such as PCI-DSS or HIPAA.

Companies can opt to offer online courses to employees or conduct classroom-based sessions with simulations in the office. Providing security training keeps employees informed and prepared, decreasing the likelihood of succumbing to common security pitfalls targeting businesses via the end user.

It is important to dispel common misconceptions with staff. Here are some cybersecurity myths –

- My firewall will keep my organization safe.
- We already have email filters in place.
- We are too small to be targeted for security attacks.
- We do not have an industry regulation that requires training so we do not need it.
- Our corporate data or PII is stored safe in the cloud.
- Our users know better than to click on malicious links or respond to suspect emails.

What to Look for in the Field

Businesses requiring security training to meet compliance and regulations, including:

ISO/IEC 27001 and 27002

Applicable employees, contractors, and third-party users receive appropriate awareness training and regular updates in organizational policies and procedures, relevant to their job function.

PCI-DSS

Educate employees (for example, through posters, letters, memos, meetings, and promotions). Require employees to acknowledge in writing that they have read and understand the company's security policy and procedures.

FISMA

Security awareness training to inform all involved parties of security risks associated with their activities and the responsibility to comply with agency policies and procedures to keep economic and national interests secure.

HIPAA

Implement a security awareness and training program for all members of the workforce including management to protect private patient information from malicious intent.

Discovery Questions

- Have you ever had staff fall for a phishing or impersonation email?
- Do you ever have users click on links they should not?
- How do you currently evaluate your employee's competency around security best practices?
- Has a user's actions on the corporate network ever caused a virus or malware infection?
- Does your organization require security training as part of compliance or regulation?
- Does your business handle sensitive company data or PII?

DDoS

TBI Battlecard

Top Providers

AT&T

Lumen

Telesytem
**included with circuits*

TPx
**included with circuits*

Verizon

Add-ons to DDoS

- Web application security
- Cloud Infrastructure
- Email and Web
- Threat Management and Response

Overview

Short for distributed denial of service, DDoS attacks are when a massive influx of web traffic from a multitude of IP addresses floods a machine or network resource. As a result, all systems shut down, preventing legitimate requests from being fulfilled. Think of it as a group of protesters crowding the entrance of a store to disrupt normal operations and keep buyers out; it's essentially the same thing.

DDoS mitigation protects attacked networks by passing internet traffic through "traffic scrubbing" filters. More specifically, it correctly identifies human traffic from bots and hijacked web browsers by examining attributes like IP address, cookie variations, http headers, and Javascript footprints. Because of how common DDoS attacks are these days, it's recommended for any business with public-facing IP addresses or DNS servers to have anti-DDoS technology and an anti-DDoS emergency response in place.

What are the implications of a DDoS attack?

- Revenue Loss: Downtime can affect bottom line up to and over $300k/hour (Gartner)
- Productivity Loss: Critical network systems become unusable, halting productivity of workforce Discovery Questions
- Reputation Damage: Customers lose trust because site is inaccessible, and their data has been stolen
- Theft: Funds, customer data, and intellectual properties can all be stolen

What to Look for in the Field

- Customers with self-hosted applications or websites.This could include their inventory or logistics applications, or phones.
- Customers relying on internet for their business.
- Customers that have been attacked before.
- Customers that falsely believe they are immune to a DDoS attack, too small to be targeted, are covered by cyber insurance or are protected by a firewall.

Discovery Questions

- What partnerships, technology and processes do you currently have in place to protect your environment?
- What is the status of your emergency response (incident response) plan?
- Do you have a business continuity plan in place?
- What in-house expertise do you have to react to an incident that occurs?
- Are you aware of the implications a DDoS attack can have on your business?
- Does your business rely on the internet, SaaS/Cloud applications?
- Can you withstand being offline? For a day or more?
- Do you have web facing servers, applications, websites, or other services reachable by the public internet?
- Do you have customers that would respond negatively to web services you provide being down an extended period?

Endpoint Security

TBI Battlecard

Top Providers

**Only available with other security services*

AppGate
Coeo
Corvid Cyberdefense
Cyxtera
GTT
HTG 360
Lumen
Masergy
NTT*
Synoptek
Telesystems
TPx
Zayo

Add-ons to Endpoint Security

- Managed Firewall
- Email security
- VPN/Identity Access management
- Mobile Device Management (MDM)
- Wireless Expense Management
- Consider asking about colocation and cloud connects

Overview

Endpoint security refers to a methodology of protecting the corporate network when accessed via any device—from laptop to desktop, printers and mobile phones. Each device with a remote connection to a network creates a potential entry point for security threats.

Endpoint security is a system that is typically comprised of security software, located on a centrally managed and accessible server or gateway within the network. In addition to client software being installed on each of the endpoints (or devices).

Although endpoint security software differs by vendor, most software offerings provide antivirus, antispyware, firewall, and they also host intrusion prevention system (HIPS).

Mobile Device Management platforms such as Airewatch and MobileIron have built in security functionality that overlaps and enhances endpoint protection platforms.

- Better control access management
- Remotely wipe devices to keep sensitive information out of the wrong hands
- Prevent potentially malicious apps from being downloaded
- Employ data loss prevention (DLP) policies

What to Look for in the Field

- Anyone deploying new devices to end users (laptops/desktops)
- Customers renewing Antivirus/endpoint contracts
- Customers expanding, adding employees/devices
- Organizations with a mobile or remote workforce and cloud connects

Discovery Questions

- Do any of your employees bring personal devices to work?
- What security risks are you most concerned about?
- How do you secure your endpoints today?
- What do you do to secure your network, from the edge to the endpoint?
- Do you have visibility to endpoints and security policies around them?
- How do you protect servers from viruses and malware?
- Have you considered deploying a zero-trust security model?
- How do you handle corporate devices if they are lost or stolen?

Identity Access Management

TBI Battlecard

Top Providers

AT&T

Corvid Cyberdefense

Cyxtera (AppGate)

Verizon

Add-ons to IAM

- Cybersecurity Awareness Training
- Email Security
- Endpoint Security
- Mobile Device Management
- Penetration Testing/ Vulnerability Scanning
- Managed Firewall

Overview

Through Identity Access Management, or IAM, IT managers and directors can manage the role of users to better protect corporate assets and segment their teams. It provides all the necessary tools and controls to manage users' identities, assignments, privileges, and authentication.

This provides easier, more efficient means to segment the business and protect against sensitive documents or resources being accessed by unauthorized users or outside parties, while easing the burden of user provisioning and account creation through controlled workflows. Along with enforcing user authentication policies and preventing breaches, IAM lets businesses grant controlled access to customers and partners without compromising security, making for better collaboration and efficiency.

What to Look for in the Field

- Companies with strict compliance regulations or subject to auditing can benefit greatly from on demand access to data and corporate information available through IAM.
- IAM works in conjunction with current AD or directory service to improve and ease ITs use of the service.
- IAM can be used for many different functions like maintaining org chart relationships, reports and analytics, and password synchronization.

Discovery Questions

- How do you currently control users' access to corporate resources?
- How difficult is it enforcing policies for user authentication?
- Does your business have any compliance requirements? How do you enforce them?
- Do you ever run into issues with gradual accumulation of unnecessary access rights, also known as privilege creep?
- Is directory service giving you the control and visibility you would like?
- Is there anything you would change about your current AD or directory deployment or domain controller?

Managed Detection and Response

TBI Battlecard

Top Providers

AT&T
Corvid Cyberdefense
CyberHat
Flexential
Lumen
Masergy
Synoptek
Verizon

Add-ons to MDR

- Cybersecurity Awareness Training
- Email Security
- Endpoint Security
- Managed Firewall
- Mobile Device Management
- Penetration Testing/ Vulnerability Scanning

Overview

Managed Detection and Response, also commonly known as Security Operations Center as a Service or SOCaaS, removes the burden for IT teams having to actively scan 24/7 for threats on their network by having the technical capabilities to not only respond to a threat, but remove it and prevent it from reoccurring.

An enhanced security control, MDR uses a combination of advanced technologies and human expertise to identify security threats and alert the organization. With MDR, a team of trained professionals ingests copious amounts of data, investigate incidents, and deploy responses at the host and network levels.

What to Look for in the Field

- Companies focused on strategic initiatives and those looking to eliminate hefty expense of expert security monitoring.
- IT looking to see all relevant threat information in a single intuitive interface to easily identify what's happening with network security at all times.
- Companies wanting non-stop protection for on-prem equipment as well as cloud environments and workloads.

Discovery Questions

- How does your security staff identify and respond to threats today?
- Are you confident in the cybersecurity skills of your staff to ensure threats do not get into your network?
- What is the response to threats once they occur?
- Do you currently have log management or a SIEM in place?
- What is the current coverage of your security monitoring (Mon-Fri 8am-5pm; 8am-5pm 365 day/year; 24 hours 365 days/year)
- Do you have trouble retaining competent security staff?

Managed Firewall

TBI Battlecard

Top Providers

AT&T
Corvid Cyberdefense
Hypercore
Masergy
TPX
Verizon
Airespring
Forsythe
Lumen
Telesystem
Windstream

Add-ons to Managed Firewall

- SD-WAN
- DDoS mitigation
- Secure web gateways
- Endpoint security solutions
- Wireless backup/routers
- Enhanced email security
- Management and analytics software
- Web application firewalls and delivery controls
- Cloud instant security (public and private cloud security solutions)

Overview

With so many cyber security threats, it makes sense to invest in a managed firewall solution.

Traditional firewalls include:

- Packet Filtering
- Network Address Translation
- URL Blocking
- Virtual Private Networks (VPN)
- Access Control Lists
- Packet Filtering
- Stateful Traffic Inspection
- VPN Capabilities

A managed firewall solution takes on management, maintenance and reporting. It includes:

The Device

A centralized virtual or physical appliance, now part of a monthly contract moving it from CapEx to OpEx. As needs grow and a larger device is required, scale the solution without having to purchase a new device.

Firewall Maintenance

Updates, patch management, change management and other maintenance is handled 24x7x365 by the vendor. This service will occur within an agreed upon SLA to ensure needs are met in an acceptable time frame.

Portal

Continuous visibility into perimeter security for monitoring, logging and reporting all done through a cloud-based portal. View data and analytics, assess trends, utilize logs for audits and compliance requirements.

What to Look for in the Field

- Customers looking to do a firewall refresh
- Customers who have been/recently attacked
- Customers who can not remember the last time they updated/patched their firewall
- Customers with compliance needs
- Customers with little understanding of security
- SMB customers (usually huge targets, typically think they are too small to be breached)

Discovery Questions

Use these discovery questions to talk to your customers about their security policy, upcoming needs and how they plan to evolve their security posture in our ever changing, high threat environment.

- Do you have a security policy? An acceptable use policy? What does it include?
- Do security policies include: data protection, destruction, passwords and reporting procedures?
- What regulatory and compliance standards do you have to adhere to?
- Do you employ any security staff or IT employees with security duties?
- Where would you say your biggest vulnerabilities lie? What challenges do you face as it relates to security?
- Do you run audits on your security, who do you use, when was your last audit?
- When was the last time you completed a security assessment?
- When was the last time you updated your firewall?
- How old is your firewall? Can you provide make and model "I have resources (TBI) who can verify if the device is still supported"
- Do you have application visibility and control?
- How do you handle security attacks, before, during and after?

Managed Firewall

TBI Battlecard

Debunking Myths

I have a firewall that's all I need.
Response: While definitely a critical part of your security posture, a firewall does not protect against all threats.

I bought a firewall years ago and its running fine.
Response: When was the last time it was updated/patched?

Firewalls protect against all threats.
Response: No, although it is crucial, it is only one part of a complete security posture to fully protect a company against threats. Look to Endpoint protection, DDoS Mitigation, Cloud/mobile security, etc..

Firewall logs are just false alerts.
Response: While many alerts are false positive, it can be very difficult to catch the ones that ID true threats. This opens the conversation to SIEM.

I bought a firewall years ago and its running fine
Response: Does it have next generation capabilities such as app awareness or DPI? More and more of the internet is becoming encrypted and using ACLs to block specific traffic is becoming much more difficult.

The Next-gen Firewall

With a next-gen firewall, additional features are layered on with QoS and no additional devices are needed. Additions can include:

Intrusion Detection System (IDS)
IDS identifies malicious traffic targeting the network and provides alerts. Activity is logged to provide an audit trail available for review in a portal.

Intrusion Prevention System (IPS)
IPS works in conjunction with IDS to block malicious traffic and quarantine suspicious traffic. Parameters can be set through the cloud-based portal.

Antivirus
Antivirus software/applications protects inbound and outbound traffic against viruses, worms, trojans and other malware. Protection is at the edge of the network and in real time. Threats are logged in the same SIEM portal.

Content Filtering/URL Filtering
Often the last piece of the security puzzle, content filtering protects your internal network. This web filtering blocks access to web sites outside of a company's Internet "Acceptable Use Policy", ranging from social media sites and YouTube to gambling and drugs.

Deep Packet Inspection (DPI)
DPI grabs pieces of each packet to thoroughly inspect and identify anomalies or violations of normal protocol/communications.

Application Awareness
Log and track application use throughout the network to create a baseline and use these parameters to set policy around which users can access what.

Active Directory/LDAP Integration
This integration allows a higher level of content/URL filtering based on the user's roles within Active Directory.

Penetration Testing & Vulnerability Scans

TBI Battlecard

Top Providers

AT&T
Coeo
Corvid Cyberdefense
Cyberhat
Lumen
Masergy
Synoptek
Verizon

Add-ons to Penetration Testing and Vulnerability Scans

- Managed Firewall
  > On-prem or Cloud
- Endpoint Security
- End user Security Training
- SIEM
- DDoS Mitigation

Overview

A **penetration test**—typically referred to as pen test—evaluates IT infrastructure security by safely identifying and exploiting vulnerabilities found in appliances, operating systems, services and applications. Vulnerabilities may exist within the environments themselves or from improper configurations or risky end-user behavior.

Penetration testing assessments are also useful in validating the efficacy of defensive mechanisms and determining how well end-users adhere to security policies.

Note: Best practice would be to change up the provider each time a test is run for maximum effectiveness.

Vulnerability scanning detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures. Vulnerability scanning lets you take a proactive approach to close any gaps and maintain strong security for your systems, data, employees, and customers. Vulnerability Scans are typically an ongoing service.

There are distinct differences between the two. A vulnerability scan searches a system for known vulnerabilities via a passive process where a device or collector is placed on your network to perform a scan.

A penetration test attempts to actively exploit weaknesses in an environment via an individual or group of white-hat hackers attempting to gain entry into the network. Both are critical components in a comprehensive network security protocol and cybercrime prevention.

Data breaches are often the result of unpatched vulnerabilities, so identifying and eliminating these security gaps, removes that attack route.

What to Look for in the Field

- Customers with regulatory compliance requirements have prerequisites for testing and employing security policies.
- Any customer who has been attacked or scared of being attacked.
- Customers looking to do a firewall/security refresh, and want a baseline on their environment
  > This can apply to customers who recently upgraded/updated and want to ensure they have minimized any security risks.
- Customers with small IT staffs or lacking security skills to effectively identify vulnerabilities.
- Customers who have conducted vulnerability scans and would like to verify the measures they've taken

Discovery Questions

- Do you have regulatory or compliance requirements you are obligated to meet?
- How confident are you of your ability to demonstrate compliance?
- Do you have a clear picture of your overall security posture and of how it relates to industry best practices?
- Do you currently conduct security assessments, such as penetration tests on a bi-annual basis?
- How realistic is your plan to address the security gaps that you might have today?
- Do you have an established process to address computer security breaches?
- When was the last time you tested your security polices? How did you do it?
- (IF THEY ALREADY CONDUCT PEN/VULN SCANS) - Do you rotate your vuln scan / pen testers on a regular basis?
- How do you handle patch management of servers and endpoints in your organization?
- Do you currently have cybersecurity insurance of some form?
- Are you adequately protected from ransomware?

SIEM & Advanced Threat Protection

TBI Battlecard

Top Providers

Corvid Cyberdefense
Cyberhat
EvolveIP
GTT
Lumen
Masergy
Synoptek
TPx

Add-ons to SIEM

- Email Security
- Endpoint Protection
- Identity Access Management (IAM)
- Managed Detection and Response (MDR)
- Managed Firewall
- Security Awareness Training

Overview

Security Information and Events Monitoring, or SIEM (pronounced "sim"), is a security focused technology that combines security information management and security events management into one system to collect and analyze alerts and data from across the network environment. Multiple data sources can include network devices like routers, firewalls, servers, endpoint solutions, and much more.

A tool like SIEM allows data from disparate security solutions to be unified into a single interface to prioritize and triage identified threats, allowing IT staff or managed providers to quickly address and prevent lasting damage. When an issue is detected, SIEM systems can gain more information, generate an alert and trigger security controls to stop activity. Using SIEM in conjunction with security solutions for preventing or catching vulnerabilities provides a much greater degree of protection against advanced threats such as malware and hacking attempts on the network.

What to Look for in the Field

- SIEM can manage large volumes of logs and rapidly assess data 24/7 freeing up IT, but still requiring them to manage the device.
- SIEM provides users with alerts like an intrusion detection system and does not remove viruses or block connections.
- Businesses with regulations and compliance requirements like Payment Card Industry Data Security Standard (PCI DSS) or concerned with advanced persistent threats (APTs) can benefit greatly from the centralized logging that SIEM provides.
- SIEM can assist business audits, quickly showing paper trails and historical data.

Discovery Questions

- Are you currently collecting and analyzing log traffic in your organization and if so, how?
- Do you operate or host a SYSLOG or SNMP server currently?
- Does your organization have the manpower to analyze the various logs and data generated by devices on your network?
- Do your current security solutions provide visibility into advanced threats like malware, ransomware, or hacking attempts?
- Does your team struggle to identify safe vs malicious logs or are experiencing log fatigue?
- Has your business ever suffered due to an undetected breach?

Visit

https://www.tbicom.com/solutions/security/
to learn more about available security solutions,
top providers and resources.