DATASHEET

Fidelis Elevate™

Know Your Cyber Terrain

Understanding Your Environment is the First Step of Cyber Defense

A successful battleplan always starts by understanding the battlefield. You really don't want to go in blind. The same goes for protecting your turf. You need to understand what you have, points of exposure or vulnerability, and critical areas to prioritize.

Your adversaries take a similar approach. Their ability to understand and exploit the terrain often dictates the outcome.

Understanding is the first step in both offense and defense.

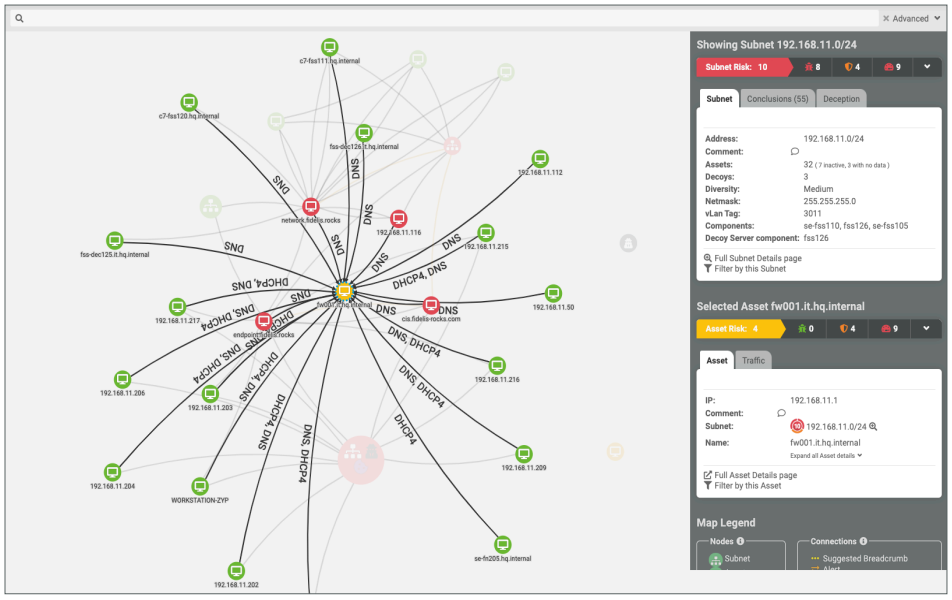
What is Cyber Terrain and Why Should I Worry About it?

Cyber terrain is the cumulative topography of an organization's IT infrastructure. It is comprised of all operational IT and data assets, network connections, and security controls.

Cyber terrain mapping is essential in its influence of cyber decisions about operations, investments, and architecture to improve defensibility, resiliency and security. It helps better identify your assets and assign value to each. But why is it important to know one's own terrain?

To reduce cyber security risk, NISTs Cyber security framework recommends a number of actions. One of those requirements is "to identify, prioritize, and focus resources on the organization's high value assets (HVA) that require increased levels of protection—taking measures commensurate with the risk to such assets."[1] Cyber terrain mapping gives you insight into all of your IT assets, so you can identify the most critical to your operation.

[1] Risk Management Framework For Information Systems And Organizations, NIST Sp 800-37, Revision



Dynamic cyber terrain mapping based on automatic profile and classification of asset and services enables holistic visibility and control.

Terrain-based Defense Advantages

- **Discover assets** using passive network monitoring of on-premises and cloud assets.
- **Identify assets** by role, operating system, connectivity, and more.
- **Identify unmanaged assets** to fortify and defend assets without endpoint protection on your networks including BYOD IOT devices where it's not always possible or feasible to install endpoint EPP/EDR agents.
- **Identify Shadow IT** by analyzing all traffic. Often IT networks are created by business units without the knowledge of the security team creating "shadow" networks that are not properly secured.
- **Create a deception network** based on a terrain map that enables decoys to be automatically installed, moved, and adapted as the terrain changes.
- **Define your most important assets** to prioritize fortification and protection of the most critical assets. Because, in an environment of thousands of computers, some are more important than others (i.e., email servers, file servers, and application servers are bigger targets than user laptops, and CFO and HR systems are more valuable targets than marketing.)

The Cyber Terrain Problem

When an attacker targets your enterprise, one of their first tasks is to map your environment. They will discover your assets, the asset's role in the organization, operating system, communication paths, installed software, vulnerabilities, users, and more.

Often, enterprise security teams don't fully understand the terrain they're trying to defend. Instead, they rely on static network drawings and asset information which is not updated at the speed in which networks adapt with people and technology changes throughout the enterprise. That is a problem. Particularly since the security perimeter is now dynamic – changing constantly as new cloud services are added and removed. XaaS, shadow IT, BYOD, IoT are all complicating the role of security professionals.

Cyber Terrain describes the security battleground. Mapping cyber terrain in real-time enables security teams to better understand and protect the environment, to discover security weaknesses, and to fortify them before an adversary can exploit any vulnerability.

The Cyber Terrain Solution

Fidelis Elevate XDR provides deep, contextual data and asset visibility that enables advanced cyber terrain mapping across your entire environment. This mapping provides a complete and continuous inventory and assessment of attacker movements and methods to more effectively thwart nefarious activities. It applies a risk analysis algorithm to highlight potential weaknesses, and it presents assets within a communication map displaying open protocols and ports between computers, networks, and subnets. In doing so, Fidelis Elevate XDR shifts security analysts to a more proactive approach to anticipating and shortening time to detect and respond to threats.

Learn more about Fidelis Elevate XDR ▶

Cyber Terrain Mapping using Fidelis Elevate XDR

- Monitor all network traffic over all ports and all protocols to help identify and assign roles to endpoints based on observed communications.
- Detect the operating system of the asset.
- Monitor and manage assets detected within the environment. Active Directory integration provides knowledge of assets and users.
- Identify asset roles (e.g., Workstation, Web Server, File Server, Mail Server, Doman Name Server, IOT devices, and more) and assign importance based on the data stored and potential for business disruption as the result of a cyber-attack.
- Review communication paths between your assets, including which ports and protocols are used, and subnet definitions.
- Understand the existence of an endpoint agent, vulnerabilities of installed software, and the vendor of the asset.
- Update vulnerabilities when new software is detected and via daily updates to the Common Vulnerabilities and Exposures (CVE) database.
- Assign vulnerability information from supported common vulnerability scanners.
- Create uncertainty for attackers by automatically creating and modifying a decoy network to modify the terrain. Constantly changing environments make it difficult to distinguish real assets from decoys, allowing the defender to detect and investigate active attacks early in their life cycle.
- Take a multi-dimensional risk analysis approach to assets based on importance, available security coverage and threat score computed based on known vulnerabilities and alerts.

Refer to our Risk datasheet for more information on mitigating your cyber risk ▶

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.

