DATASHEET

Fidelis Elevate®, an Active XDR Platform

Asset Risk Calculation

Understanding Your Cyber Risk with Fidelis Elevate

Most security teams function in a highly reactive environment, moving from one potential crisis to the next. Ultimately, these security teams need to get out of fire-drill mode and stop threats before they can do any damage. The goal is proactive cyber defense as provided by an Active XDR platform.

The Importance of Risk Assessment

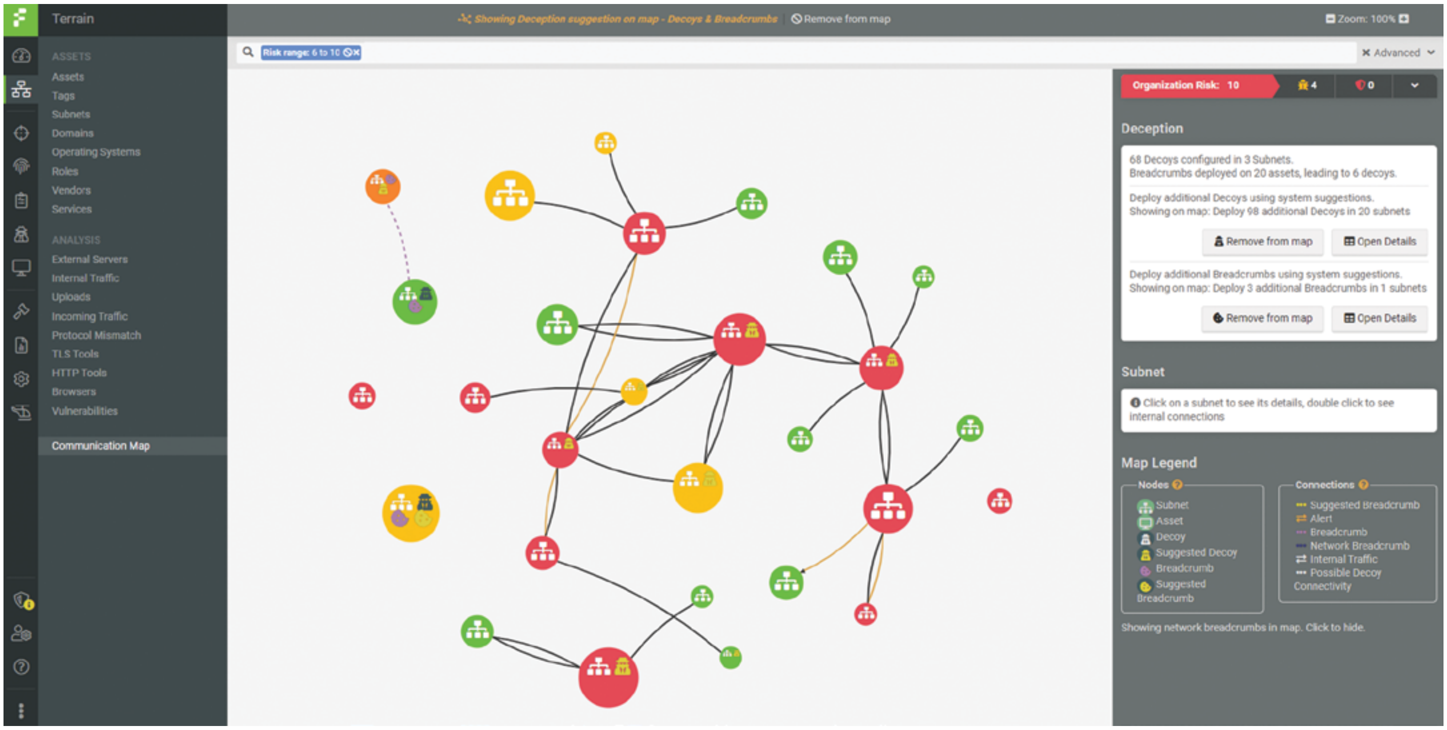
With the rapid adoption of dynamic hybrid and multi-cloud environments, the attack surface is constantly changing. Every new server, IaaS account, cloud service, container, endpoint, software installation, vulnerability, threat intelligence report, and network modification changes the risk to the enterprise. Risk must be calculated and recalculated constantly to keep security ahead of the next threat.

Security teams traditionally use a variety of tools to identify vulnerabilities, cyber alerts, and user behavior, notice potential threat activity, and react fast enough to minimize harm. Early detection is the key to their success, but not every alert warrants the same level of response. Risk assessment provides threat-informed intelligence that helps SOC teams work efficiently.

Risk assessment is pivotal to building a strong cyber defense strategy. It involves creating an asset terrain map, then calculating relative risk to prioritize assets and activities according to the likelihood of exploit or damage. In doing this evaluation, you will be better able to detect, prioritize, and respond to threats before the threat adversaries can cause damage to your organization. That may be in the form of data theft, business disruption, brand damage, or a variety of other means for the attacker to achieve financial, political, or competitive missions.

Equally important is being able to shift to a more proactive approach to cyber defense.

Proactive cyber defense uses risk to view the security of the organization from an adversary's perspective. By thinking like your adversary, you can identify weaknesses and fortify security before an attack is in progress. Proactive cyber defense enables your team to plan for future cyber-attacks rather than continuously reacting to time-critical events. Therefore, your ability to accurately calculate risk and prioritize fortification is a critical tool in your proactive defense against cyber-attacks.



Showing Deception suggestion on map - Decoys & Breadcrumbs

Deception

68 Decoys configured in 3 Subnets.
Breadcrumbs deployed on 20 assets, leading to 6 decoys.

Deploy additional Decoys using system suggestions.
Showing on map: Deploy 98 additional Decoys in 20 subnets

Deploy additional Breadcrumbs using system suggestions.
Showing on map: Deploy 3 additional Breadcrumbs in 1 subnets

Subnet

Click on a subnet to see its details, double click to see internal connections

Map Legend

Showing network breadcrumbs in map. Click to hide.

How do you calculate risk?

Risk is a multi-dimensional calculation based on:

- Asset coverage or protections
- Relative importance of the asset to the organization (and hence the adversary)
- Severity of current events

Let's look at each in more detail.

Coverage

Coverage reflects the protections in place for any given asset. Is there an endpoint EPP/EDR agent properly deployed on the asset? What software is installed? Does the asset have any known vulnerabilities? Is the asset "Shadow IT" and therefore not likely to have appropriate security settings in place? Are your cloud assets configured securely based on CIS benchmarks, regulatory standards, and industry best practices? Do we have network data analysis for the asset? Is Deception technology deployed on the subnet? These questions explore the security coverage for assets in your environment.

Importance

Not all assets are created equal. Importance can be implied by role — mail servers and file servers store critical data and are more important than workstations. However, the workstations and laptops in some departments like finance, HR and engineering store or have privileged access to critical data. Importance can be based on asset tags to identify the potential for PII, customer data, source code, and other critical data. It is a critical measure of what data would be the target of an attacker.

Severity of Current Events

This one facet of risk assessment looks at the severity of an event or potential vulnerability. It factors in:

- Vulnerabilities from Fidelis Endpoint® or a scanning tool that provide known issues with installed software used in the environment.
- Discovery and inventory of cloud assets updated in real-time across all connected clouds.
- Threat Score — an AI-based algorithm that considers cyber alerts and analyst feedback. Alerts are based on endpoint, network, and decoy behavior analysis.
- MITRE ATT&CK® tags on events map activity to the tactics and techniques detected in the environment.

Severity provides one measure of cyber risk, but not the full story. Many times, a critical vulnerability cannot be patched immediately. This may not present high risk if the asset is fully covered or if the asset is of low importance. Risk can be used to create a plan to prioritize actions and improve protection, including patches, IaaS/PaaS configuration compliance remediation, and network modifications to mitigate risk.

Risk Simulation

Based on asset risk and communication map, Fidelis Elevate XDR enables attack simulation.

- **Blue Team:** Ask how an attacker may gain access to a critical asset based on current risk and network connectivity. Conduct one-hop analysis, then two, three, and more to watch how it may move laterally to the critical asset.
- **Red Team:** Starting with a high-risk asset, ask how an attacker may move laterally through the enterprise based on current risk. Conduct multi-hop analysis through the enterprise.

Protect your assets with risk assessment

Trusted by the world's largest brands and government organizations, Fidelis Elevate is an Active XDR platform. It provides a streamlined security stack that integrates Network (NDR), Endpoint (EDR), Deception, and cloud security defenses. Combined, it can better automate and orchestrate workflows, and correlate rich metadata across these security layers so you have continuous visibility across servers, endpoints, and cloud.

Fidelis Elevate can help strengthen and engage a proactive cyber defense strategy by combining an asset risk map and communications map together with risk calculation and aggregation so security analysts can:

- View risk analysis of all assets in the cloud and on-premises in a single source.
- Identify vulnerabilities so that they can be patched as quickly as possible.
- Analyze and fortify shadow IT assets.
- Modify networks to isolate critical assets by changing firewalls, correcting zero-trust configurations.
- Discover users that exhibit risky behavior and direct them toward cyber training.
- Deploy a deceptive network of decoys and breadcrumbs to lure attackers that get past other defenses.
- Place network and endpoint sensors correctly to detect and react to early stages of an attack.
- Address cloud IaaS/SaaS configuration issues and vulnerabilities.

Risk assessment helps shift security analysts to proactive cyber defense so they can more quickly detect, hunt and respond to threats, while keeping sensitive data safe.

LEARN MORE ABOUT FIDELIS ELEVATE

Contact Us Today to Learn More

Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com

Fidelis Cybersecurity, the industry innovator in proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via rich, dynamic cyber terrain mapping and multi-faceted context and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. With Fidelis, organizations emerge stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit www.fidelissecurity.com