DATASHEET

Fidelis Elevate™

Asset Risk Calculation

Understand Your Cyber Risk

Most security teams are cyber firefighters – going from one firefight to another. Ultimately, the goal of these security teams is to get out of fire drill mode and stop threats before they can do any damage. To move from response to cyber defense.

The Importance of Risk Assessment

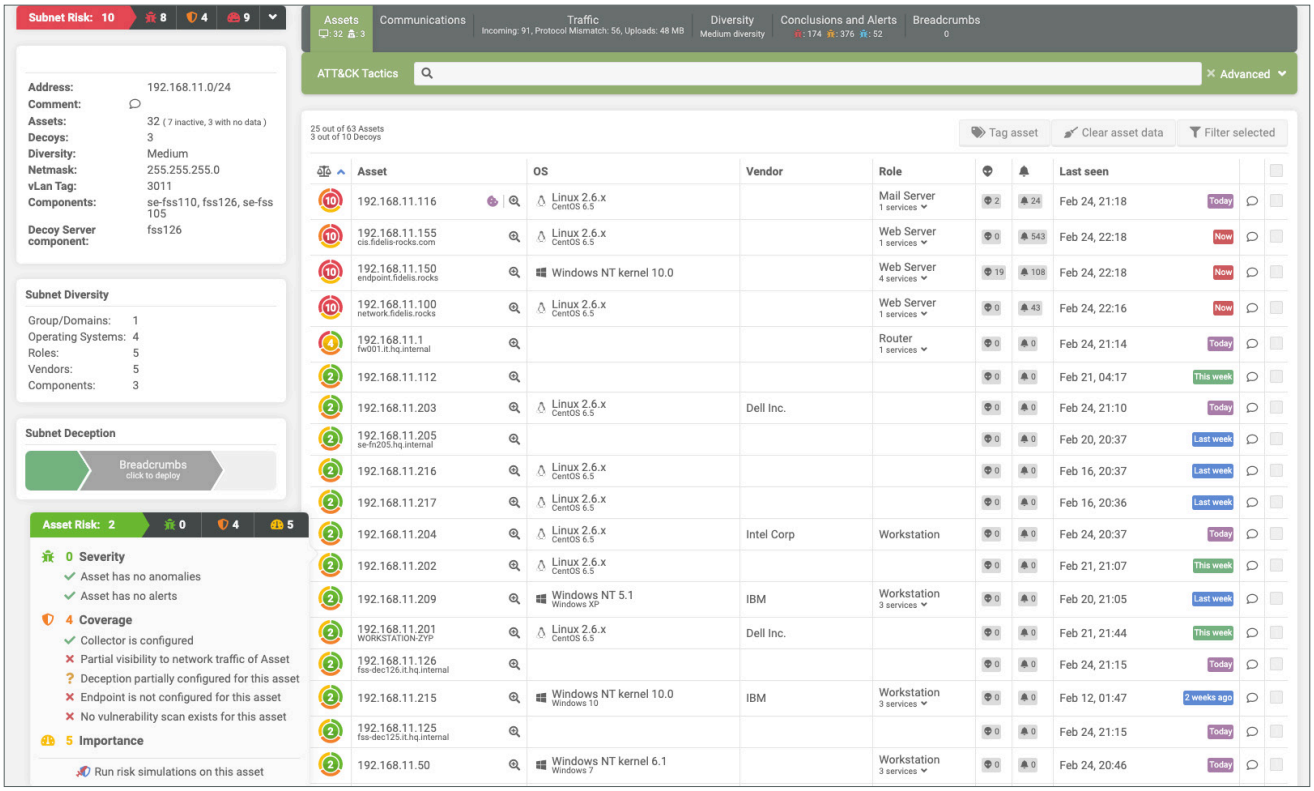
Security teams traditionally use a variety of tools to identify vulnerabilities, cyber alerts, and user behavior, notice potential threat activity, and react fast enough to minimize harm. Early detection is the key to their success. They try to stomp out small fires before they grow.

Now, the attack surface is constantly changing. With every new computer, software installation, cloud service, vulnerability, threat intelligence report, and network modification, the risk to the enterprise changes. Risk must be calculated and recalculated constantly as events unfold.

Risk assessment is a pivotal part of 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 defense uses risk to view the security of the organization from an attacker's perspective. By thinking like the attacker, you can identify weaknesses and fortify security before an attack is in progress. Proactive defense enables your team to plan for future cyber-attacks rather than react 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.



Real-time multi-dimensional risk calculation helps you prioritize and better protect your IT environment.

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 attacker)
- 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? Do we have network data analysis for the asset? Is Deception deployed on the subnet? The MITRE Shield Active Defense Matrix2 provides a description of active defense, which correlates to the cover aspect of Risk.

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 hold or have privileged access to critical data. We can derive importance based on asset tags to identify the potential for PII, customer data, source code, and other critical data. Importance is a 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.
- 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 improve protection, including patches 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 provides a streamlined security stack that integrates network (NDR), endpoint (EDR) and deception defenses, automates and orchestrates workflows, and correlates rich metadata across these security layers so you have continuous visibility across your environment.

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

- 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.

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 XDR ▶

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.

