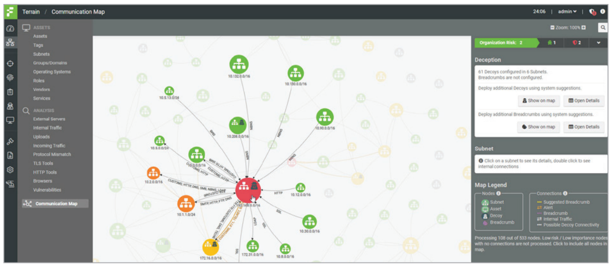
SC MEDIA EMERGING PRODUCTS



Deception

61 Decoys configured in 6 Subnets. Breadcrumbs are not configured.

Deploy additional Decoys using system suggestions.

Deploy additional Breadcrumbs using system suggestions.

Subnet

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

Processing 108 out of 533 nodes. Low risk / Low importance nodes with no connections are not processed. Click to include all nodes in map.

Fidelis Cybersecurity

Fidelis Deception v9.3

DETAILS

Product Fidelis Deception v9.3

Company Fidelis Cybersecurity

Contact fidelissecurity.com

Price $4 per user for a 36-month term

What it does Fidelis Deception provides complete visibility across all environment architectures and offers automated threat and data theft detection, threat hunting, and optimized incident and response capabilities.

What we liked This is a powerful, agentless solution that provides a deep understanding of all activity occurring within an environment and the automation necessary to respond to this activity effortlessly. We really like the high-level view of deception coverage provided during deployment that enables organizations to use deception protection with confidence.

Fidelis Deception is a fully integrated deception solution that provides complete visibility across all environment architectures. It offers automated threat and data theft detection, threat hunting, and optimized incident and response capabilities to combat almost any kind of cybercrime. The unique combination of adaptive intelligent deception, terrain analysis, and security visibility drives efficient threat response and comprehensive protection.

Fidelis offers more than one thousand OS and emulated decoys, each containing support for more than two hundred VLANs per server and covering everything from Active Directory deception to MAC spoofing. Analysts may configure these decoys themselves or allow the platform to create them automatically. To ensure the quality of automated emulations, Fidelis conducts thorough profiling and classification of an environment, gathering full visibility into all environmental activities. Fidelis may then autogenerate decoys based on this information and craft them so that they mimic real components. The system will continue to adapt the decoys as the network changes to ensure maximum realism.

Manually created decoys also have full flexibility so security teams may configure them however they prefer. Analysts may upload real files for realistic decoy construction and even control the ways in which adversaries access decoy services. Users should be aware that there is a steep learning curve with manual deception creation, but the process then establishes a stronger deception posture in exchange for the added effort. Sophisticated security teams will likely find that the work is worth the reward.

All interactions with decoys, whether created manually or automatically, are recorded and grouped according to correlations and several forensic elements and conclusions. Since Fidelis is an emulation-based solution, it provides all logged activity from the view of an attacker and paints a picture of all adversary activities during engagements, including credential collection activities and file uploads. All files uploaded to decoys are automatically sent to the sandboxing engine for analysis. Security teams may either permit automated responses to address these attacks or choose custom workflows to create attack responses manually. Both automatic and manual responses include attack validation, correlation, and expulsion, so analysts may elect the response type they prefer without sacrificing security.

A map shows a high-level view of all the communications within a network and the locations of the breadcrumbs and decoys deployed within an environment. Analysts may drill into each asset or subnet to see various asset risks and risk scores. Security teams may run red team simulations directly from this view in order to anticipate how attacks may progress. The platform maps all events onto the relevant MITRE ATT&CK framework tactic so that analysts may quickly filter through them and locate those that require their immediate attention.

Overall, Fidelis Deception is a powerful, agentless solution that provides a deep understanding of all activity occurring within an environment and the automation necessary to respond to this activity effortlessly. Fidelis Deception gives a high-level view during deployment so that organizations can use deception protection with confidence. Several reporting options reveal different views and levels of granularity, making them digestible for all team members and not just security experts. Because of its many enterprise-related capabilities, this adaptable solution will be a solid investment for organizations and environments of all sizes.

Pricing for the VLAN model starts at $50,000 for ten VLANs and increases $1,000 for each VLAN thereafter. Tiered pricing starts at $19 per user. Technical Account Managers are available to help operationalize the solution and ensure customer success.

– Katelyn Dunn

Reprinted from SCMagazine.com, October 2020 • www.scmagazine.com
(#S088211) For more information about reprints and licensing, visit www.parsintl.com/publication/sc/

Fidelis® Cybersecurity