Stop Hackers from Deconstructing Your Defense and Build Cyber Resilience

Joe Kattner
Senior Manager, Systems Engineering
Fidelis Security

The escalating threat of cyber warfare means agencies are constantly reevaluating their cybersecurity policies. Often, these agencies operate with multi-layered security solutions, resulting in intricate and complex environments that can be difficult to navigate, especially if these tools aren't integrated to communicate with each other.

This scenario is a potential cause for alarm as cybercriminals wait for the slightest oversight, allowing them to penetrate systems undetected. Fidelis Elevate serves as a preemptive extended detection and response (XDR) solution, proactively safeguarding against threats before they impact security systems. Its revolutionary architecture incorporates deception technologies with endpoint (EDR), network (NDR), and cloud detection and response mechanisms in real-time, making it more efficient and effective in prevention of advanced threats.

Compared to other XDR solutions, Fidelis Elevate boasts patented Deep Session Inspection® that comprehensibly examines our customers' IT environments to evaluate potential compromises of any system. Additionally, it quickly restores any compromised systems back to normal business operations, ensuring uninterrupted organizational workflow.

Experience a host of additional advantages with Fidelis Elevate, including:

- Empowering users with a comprehensive visualization of their cyber terrain and real-time bi-directional traffic monitoring across all ports and protocols to better understand their risk posture.

- Going above and beyond traditional data protection measures by leveraging automatic generation of decoys and breadcrumbs to divert attackers away from the most valuable assets.

- Seamless integration with various third-party solutions and provision of a full-featured API, ensuring robust customization options.

Fidelis Elevate transcends the limitations of traditional security operations centers (SOC) and enhances your cybersecurity capabilities with unparalleled contextual visibility and dynamic cyber terrain mapping. This empowers security teams with the information they need to quickly investigate and respond to threats and reduce the risk of data loss or system compromise.