Stellar Cyber File Integrity Monitoring (FIM)

A Component of the AI-Driven Open XDR Platform

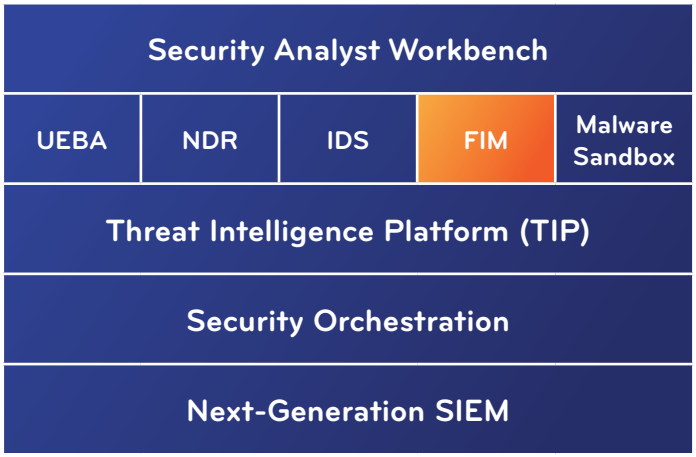
When an attacker succeeds in penetrating your environment, they are on the hunt for two things: 1). Valuable company data they can sell or hold for ransom and 2). files they can delete that track their activity. With millions of files in a typical environment, a security team can't monitor the files manually.

Stellar Cyber File Integrity Monitoring (FIM), a critical component within the Stellar Cyber Open XDR Platform, enables a security team to identify sensitive files across their environment to monitor for changes. When one of these files changes, Stellar Cyber automatically generates an alert, enabling any security analyst to perform a quick investigation and take decisive response actions if required.

With Stellar Cyber File Integrity Monitoring, you can:

- Select files or folders on Microsoft Windows and Linux servers for changes automatically.
- View and investigate alerts generated by FIM directly from the Stellar Cyber security workbench.
- Initiate response actions fast with hundreds of pre-built integrations.

Stellar Cyber Security Applications



Stellar Cyber FIM Benefits

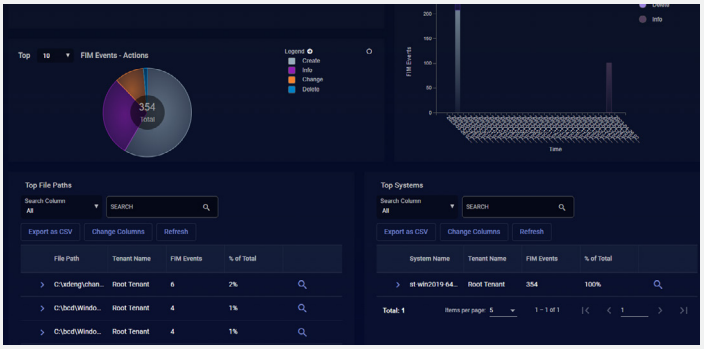
Maintain 24/7 visibility on your most sensitive files across your environments.

Quickly investigate identified changes to sensitive files to determine if an attack is underway.

Take decisive response actions directly from Stellar Cyber to mitigate active threats.

The Stellar Cyber FIM Dashboard

While identifying when sensitive files on servers are modified is essential, having the ability to visualize the changes quickly makes performing the investigation more effective. The FIM dashboard in Stellar Cyber gives security analysts the information to determine where to direct their investigation efforts.



Total Number of File Paths in Events	Displays the total number of unique file paths in the FIM events available
FIM Events – Action Trends	Graphs the quantity of FIM events by date
Top N FIM Events – Actions	Charts the Top N FIM event actions (create, delete, change) in either donut or pie mode
Top File Paths	Lists the top file paths with associated FIM events in a standard table format
Top Systems	Lists the Windows Server Sensors with the most associated FIM events
Machine Learning Correlation	Graph machine learning techniques combine seemingly disparate alerts into cases, providing security analysts with contextualized and prioritized threats to investigate
Guided Investigations	Correlated incidents include the underlying data and context a security analyst needs to complete investigations fast, increasing efficiency and effectiveness
Fast Incident Response	Security analysts can take decisive response actions manually or fully automate responses on the same platform using predefined response actions or customizable response playbooks

Take the First Step Today

Every security team should be able to deliver continuous, consistent security regardless of their skills or experience. With Stellar Cyber FIM, you get the necessary visibility to secure your business. Visit **www.stellarcyber.ai** to learn more.

Stellar Cyber Open XDR platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering an 8X improvement in MTTD and a 20X improvement in MTTR. The company is based in Silicon Valley. For more information, visit https://stellarcyber.ai.