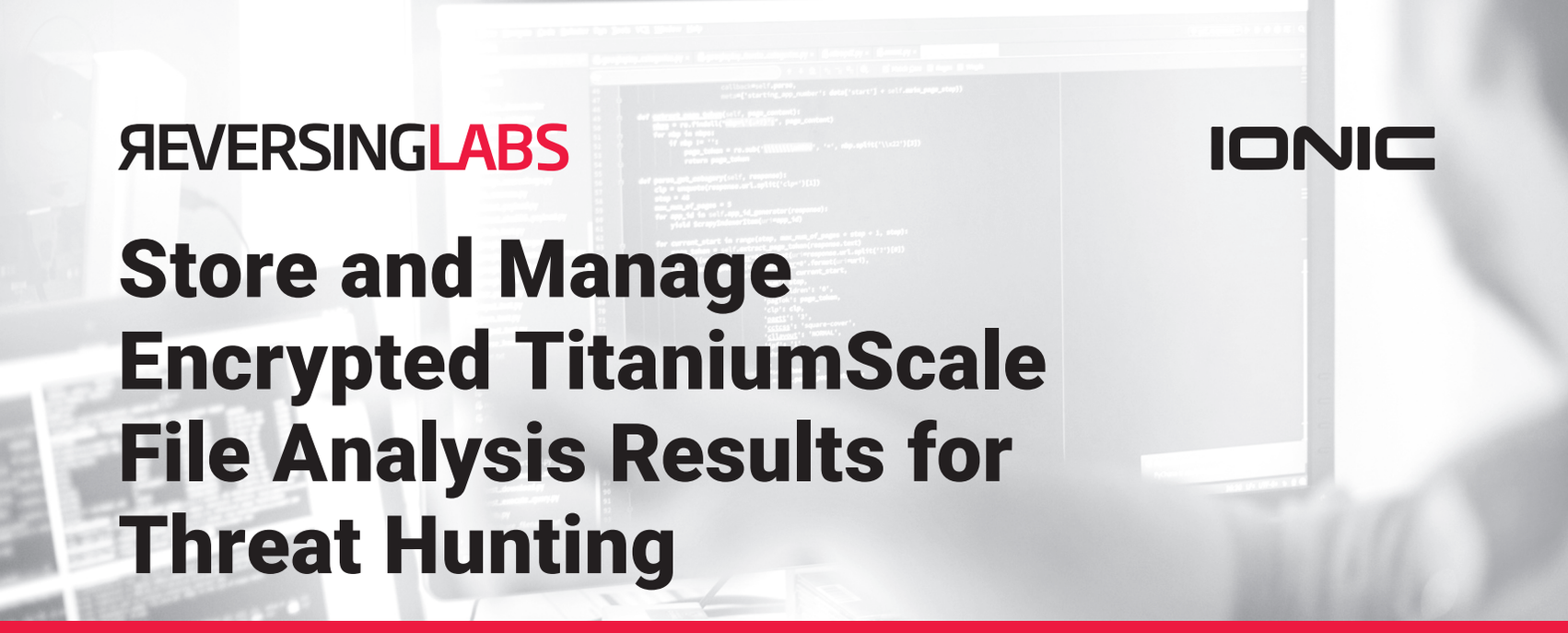


REVERSINGLABS

IONIC

Store and Manage Encrypted TitaniumScale File Analysis Results for Threat Hunting

Technology Integration Partnership

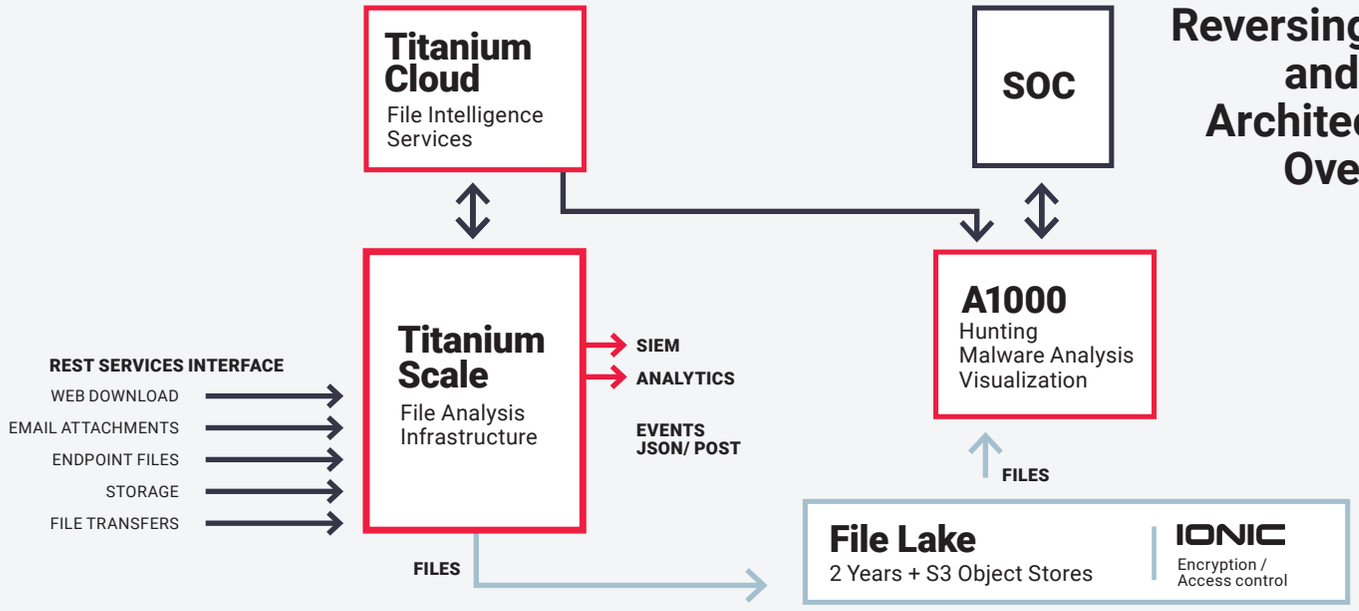
The Ionic Security and ReversingLabs partnership helps organizations transform their hunting capabilites by securely storing and managing malware analysis results on all files in a file lake for them to access later. SOCs that are responsible for processing large volumes of files to hunt and respond to malware can now securely pull data back out of the file lake for further analysis and to identify malware.

Through the ReversingLabs' TitaniumScale Enterprise-scale Visibility platform integration with Ionic Security's Data Trust Platform, TitaniumScale automatically generates Ionic encryption keys on every file to securely store and manage file analysis results in a file lake with safe, granular and risk-averse controls - regardless of classification.

TitaniumScale's static analysis results are also automatically pushed to a SIEM, Elasticsearch and/or analytics platforms for efficient event reporting and incident management.

Partnership Solution Description:

- The integration allows TitaniumScale customers who build a file lake to securely store and manage file content based on file classification and risk level using the Ionic encryption technology and granular access control policies.
- The solution provides an added level of security by isolating the files and preventing them from harming the enterprise or corrupting the storage.
- TitaniumScale removes manual key management by automatically generating a content key at scale which would be nearly impossible to do manually, by leveraging IT's general purposed storage arrays for all sensitive, potentially malicious and other content subject to policy controls.
- Applying strong encryption, unique key management and policy control on all sensitive and potentially malicious content as it is being shared with partners, law enforcement and/or regulators.
- The joint solution leverages Ionic's encryption and just-in-time policy engine to provide strong data leakage controls over large storage repositories used in support of TitaniumScale's deep file inspection and static analysis platform.



Solution Highlights

- Automate discovery and deep analysis of files
- Securely store files with automated content key generation and key management at scale
- Apply strong encryption, unique key management and policy control over all your file assets
- Quickly analyze unknown binary content and hunt for threats
- Optimizes event reporting and incident management

About ReversingLabs

Malware routinely evades detection and lurks within corporate infrastructures causing damage and loss. Unique automated static analysis technology and authoritative file intelligence services power our innovative solutions that enable security teams to combat unknown malware. TitaniumScale high volume analysis and classification creates local threat intelligence across all internal objects and empowers security teams to identify and neutralize malware that evades detection.

About Ionic Security

Based in Atlanta, Ionic Security accelerates and simplifies trust in a machine-scale world, helping clients systematically reduce the likelihood and impact of a data breach while simplifying information governance and the management of today's borderless enterprise. The Ionic Data Trust Platform consistently protects and controls data from creation through consumption everywhere it travels and anywhere it resides, preventing inappropriate data handling with real-time policy, and enabling customer-managed trust —across clouds, environments, and data silos. Learn more at https://www.ionic.com, or connect on LinkedIn or Twitter.