IT Security Search

On-the-fly IT search and analytics

Seeing the unseeable can be a challenge for IT. With billions of events to collect and review from a variety of disparate sources, it's difficult to find relevant data and make sense of it. Until now.

IT Security Search, a web-based interface of InTrust, correlates disparate IT data from numerous systems and devices into an interactive search engine for real-time search and analysis. The tool uses simple, natural search language to help IT administrators and security teams quickly investigate insider attacks.

With a quick search, you'll be able to find out who did what, when and where, whether it's a change to critical Active Directory objects, elevated privileges granted to a user or group, or access to critical files and folders. Rich visualizations and event timeline provide more valuable insights.

> IT Security Search uses simple, natural search language to help administrators and security teams quickly investigate insider attacks.

BENEFITS:

- Reduce the complexity of searching, analyzing and maintaining critical IT data scattered across information silos

- Speed security investigations and compliance audits with complete real-time visibility of your privileged users and server/file data in one searchable place

- Troubleshoot widespread issues should an outage or security breach occur

- Restore corrupted or maliciously changed AD objects with ease and speed
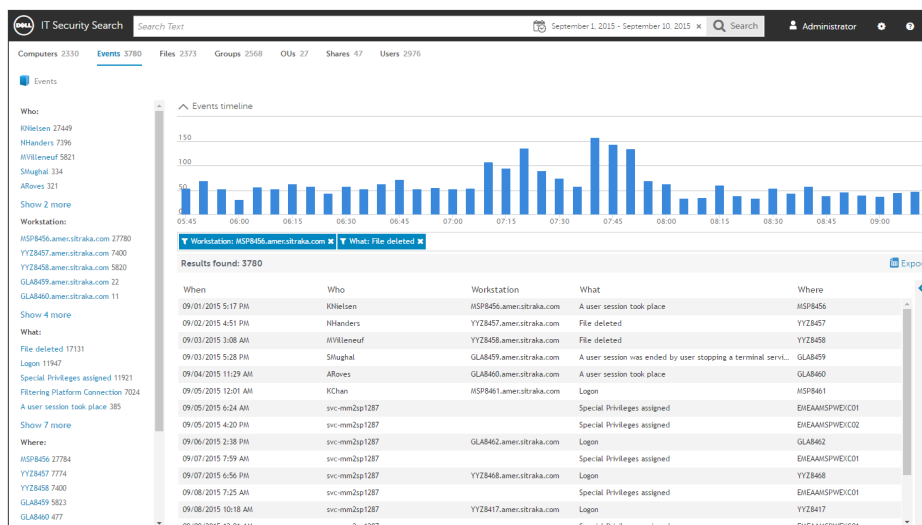
Perform on-the-fly compliance and security investigations using historical data.
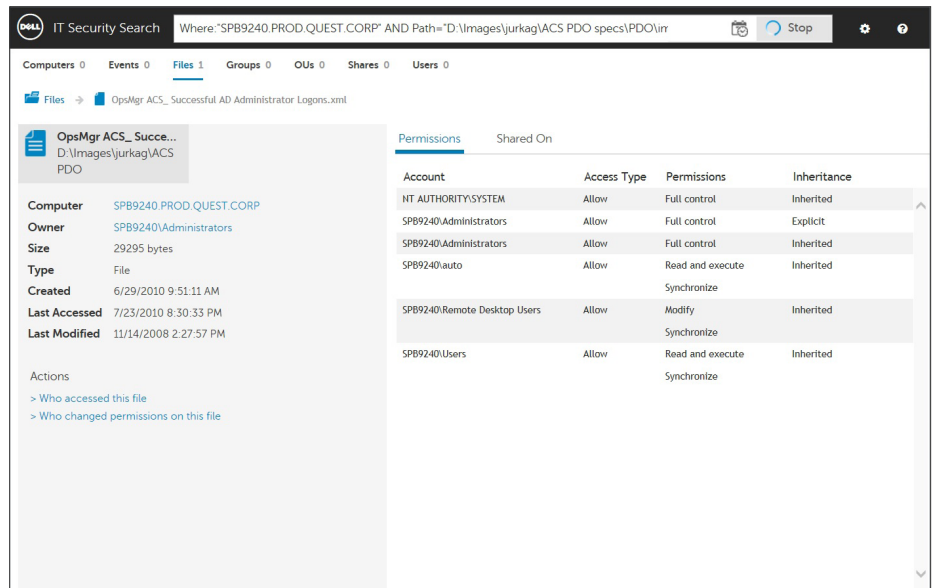
Easily understand the who, what, where and how of user access.

FEATURES

- **State-based data** — Gain critical insights into user/group memberships, file/folder ownership, installed software (including hot fixes and patches installed) and much more.

- **Audits** — View real-time information about changes to critical objects and sensitive data.

- **Object recovery** — Discover which AD objects have changed, including before and after values, and restore them with a few clicks.

- **Improved insights** — Correlate IT data from numerous, disparate systems and devices into an interactive search engine for real-time search and analysis.

- **On-the-spot security and compliance view** — Simplify the audit process and security incident reviews as well as reveal any malicious insider activity in less time and with more confidence.

- **Dynamic investigation paths** — Easily launch investigations into users, groups, shares, files or events, and quickly pivot into other views as new details emerge for a more complete investigation.

- **Compressed, indexed, online repository** — Conduct full-text search on long-term event log data and other server data for compliance and security purposes, saving time spent looking for events.

- **Diverse systems support** — Generate a unified view into state-based, audit and event data from Windows, file and other data sources.

ABOUT MERGER IT

Merger IT helps customers with solutions to assisting their organisations, providing the innovation of products which will enhance M&A activities delivery, and provide outcomes, through tried and tested toolsets and processes.

This ensures customers' requirements and outcomes are expedited leveraging the experience provided by Merger IT.

---

merger IT

Phone: +44 (0)1480 877 188
Email: mergers@mergerit.net
Web: mergerIT.net

Quest