

Fast Accurate Discovery for Incident Response

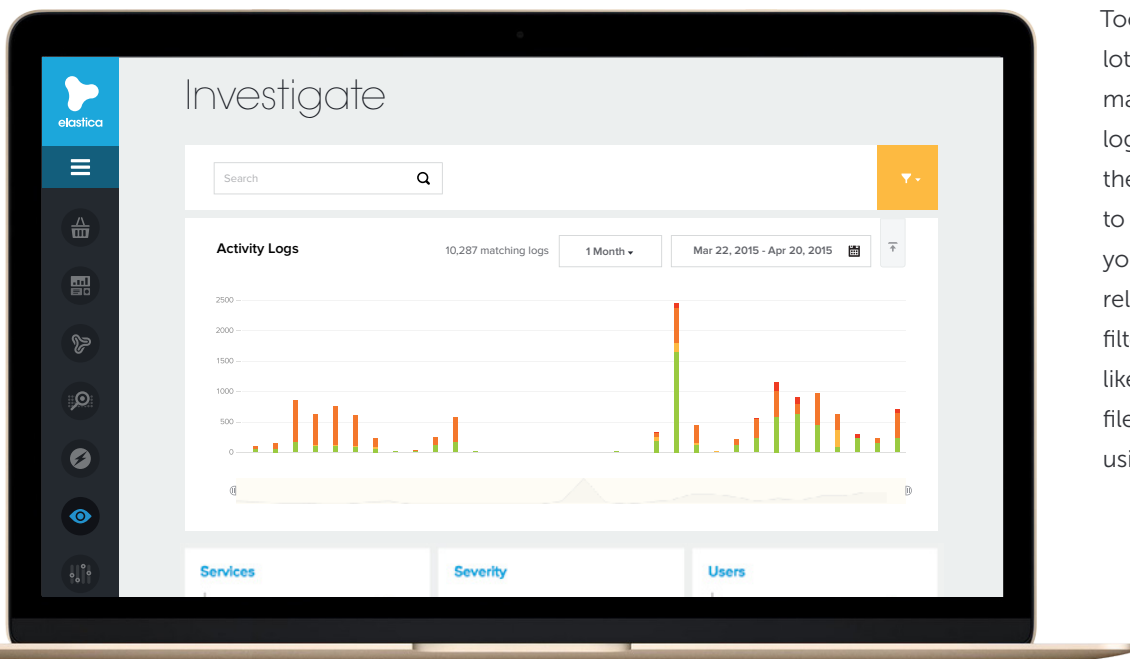
Discover and analyze what's been happening between your organization and cloud services through the Investigate app in Elastic CloudSOC.

The key to discovery and incident response lies in the ability to identify an area of concern and then to find the relevant data in enough usable detail to parse out what happened. You need a system that can quickly identify if there is an area of concern that requires investigation. You need to easily find just the information that relates to the issue you are investigating. Then you want useful information in enough detail to perform an effective analysis. And, finally, you may want to feed that data into a bigger SIEM system.

- › Which users are using which apps?
- › What have they been doing in those apps?
- › What files have been involved in cloud transactions?
- › What activities are associated with those files?

Only Relevant Logs Need Apply

Too often an investigation takes lots of time because there are too many irrelevant or unimportant logs to sift through in order to find the logs with information relevant to a security issue. In Investigate you can easily analyze just the data relevant to your investigation by filtering your search by attributes like cloud service, user, action, file, etc or get very specific results using the flexible query feature.



Quickly Identify Areas of Concern

Easily identify top services, users and severity of incidents implicated by logs through data visualizations that automatically pivot based on a specific query or filtered by specific attributes.

A Better Quality of Intelligence

Investigate collects data from multiple sources, including real-time traffic analysis via the Elastic CASB Gateway, in-app data via API integrations with Elastic Securllets™, and findings delivered via Elastic Detect to give you a comprehensive picture of your historical cloud activity. Additionally, you can store logs for up to a year without worrying about running out of storage because, unlike on-premises appliances, storage in the cloud is not a limited resource.

GATEWAY LOGS deliver highly useful, detailed information on cloud transactions, including a level of detail only possible through the data science-driven StreamIQ™ intelligence engine.

Office 365 Bob Jones sent an email to Alice Smith with the subject "Billings" using Exchange on April 12, 2016, 11:32 AM

Office 365 ALERT bob@company.com attempted to Share book.xlsx using Linux and Firefox v43 on April 12, 2016 11:34 AM

SECURLET LOGS deliver detailed information on user activities occurring in sanctioned cloud accounts and information on files in sanctioned cloud apps, including details only possible with via the data science-driven ContentIQ™ intelligence engine. The API integration architecture of Securllets means that this data is discovered regardless of the device or location from which a user accessed those cloud accounts.

Box File "book.xlsx" has risk of PII and PCI violations from user bob@company.com

Google Drive ALERT Bob Jones shared document "book.xlsx" on April 12, 2016 11:45 AM

DETECT LOGS provide data on risky activities performed by users and ThreatScore updates. When reviewing an Incident in Detect, click through directly into Investigate data filtered by the specific activities of the user that contributed to the Incident. This gives a top-down approach avoiding sifting through log volumes in a typical bottoms-up approach of SIEMs.

Across Services Bob Jones user ThreatScore is now 97, changed for "Too many suspicious location changes" on April 12, 2016 11:59 AM

Integrating with SIEMs

Many organizations use Security Incident and Event Management (SIEM) systems to do forensic analysis across logs from multiple sources. Investigate logs are easily exported to major SIEM platforms in CEF, CSV, and LEEF formats.

