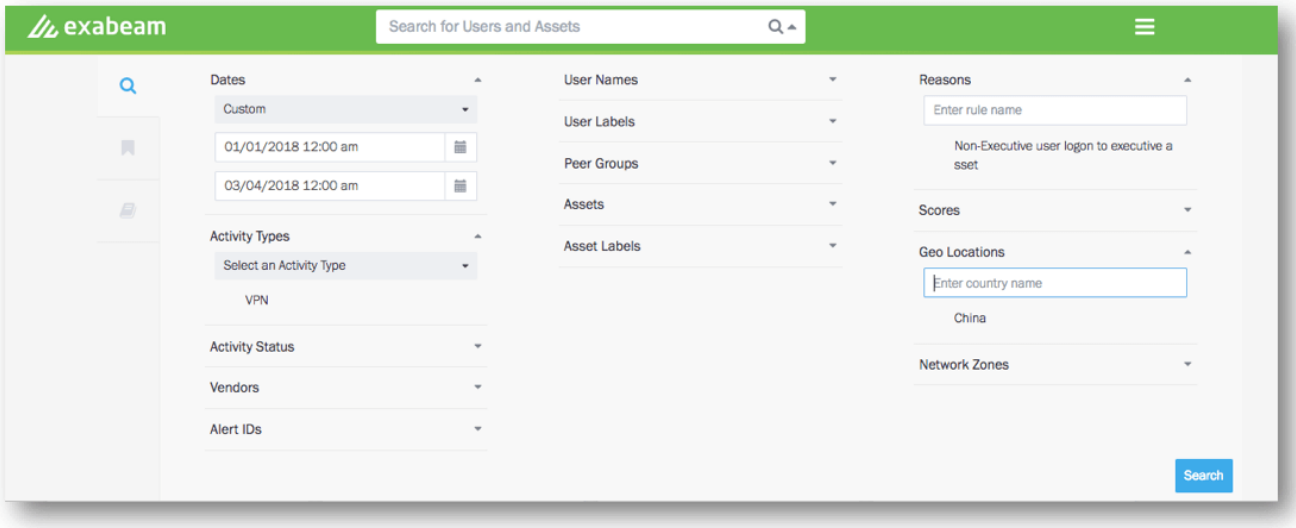
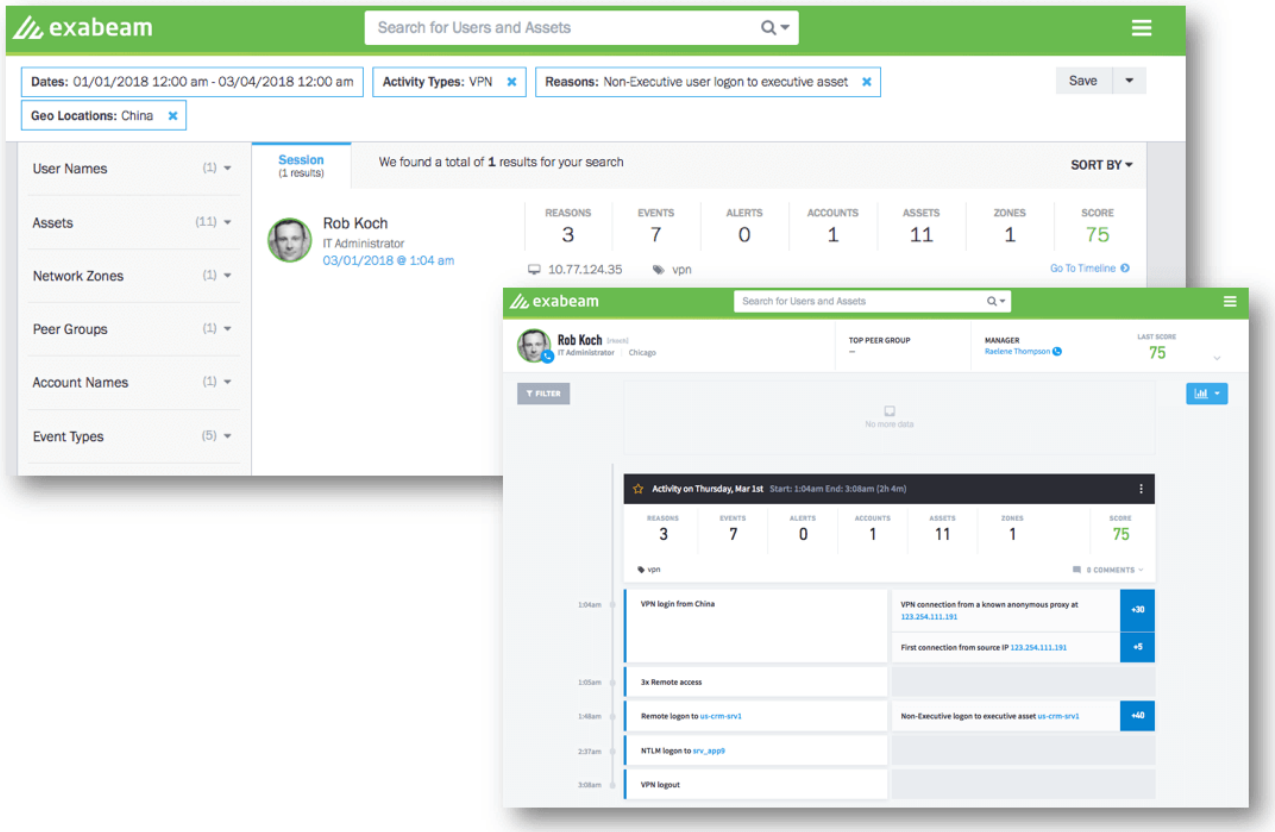
Exabeam Threat Hunter

Point and click search for efficient threat hunting



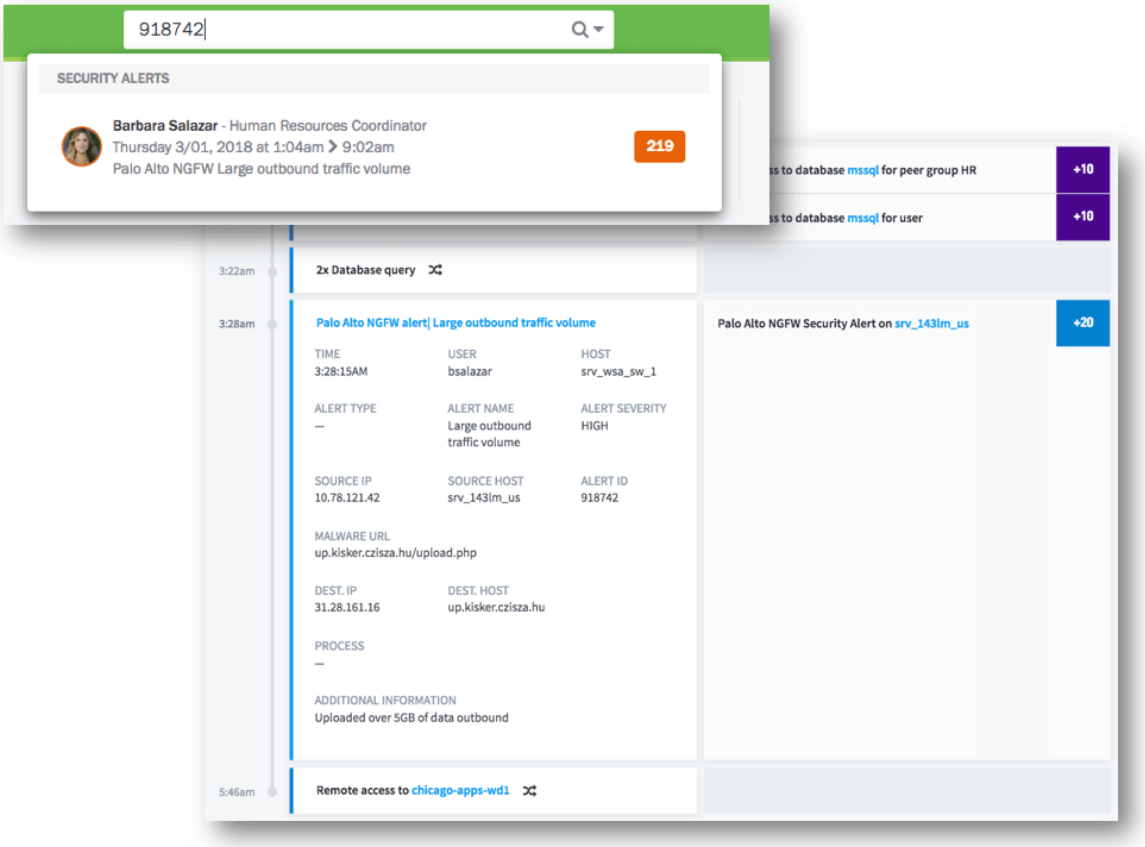
Easy-To-Use Point-And-Click Interface

The Threat Hunter point-and-click interface simplifies the process of creating complex search queries. Now anyone in the SOC can quickly and easily engage in threat hunting by developing searches that otherwise may have been extremely difficult or impossible using traditional querying.



Work With Completed Incident Timelines

Traditionally, threat queries use the syntax of the SIEM — requiring an analyst with the right skills. When a threat is uncovered, the analyst must then gather remaining evidence by pivoting and querying their SIEM. This involves manual steps that can take weeks, slowing threat hunting. By contrast, Threat Hunter is designed for to be used by everyone, providing automatic incident timelines instead of logs for rapid and proactive threat hunting.



Security Alert ID-Based Search

An alert ID such as from an anti-malware or DLP tools is the starting point for many security investigations. Often the result of such a search produces a complex sea of event logs. With Threat Hunter, entering an alert ID or IP address produces an automatic timeline of events showing how the security incident unfolded — for complete situational awareness of the threat.