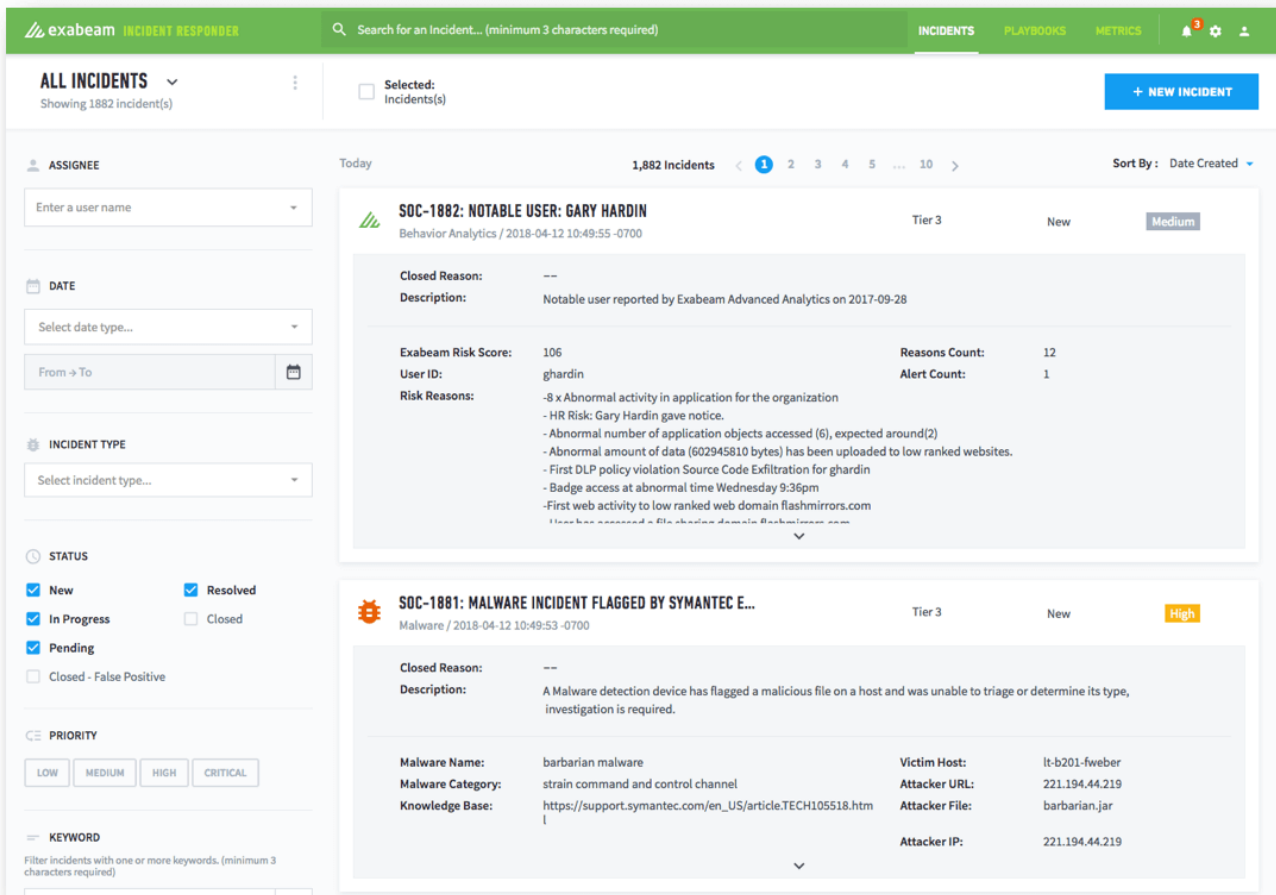


Exabeam Incident Responder

Add automation and orchestration to your SOC to make your cyber security incident response team more productive

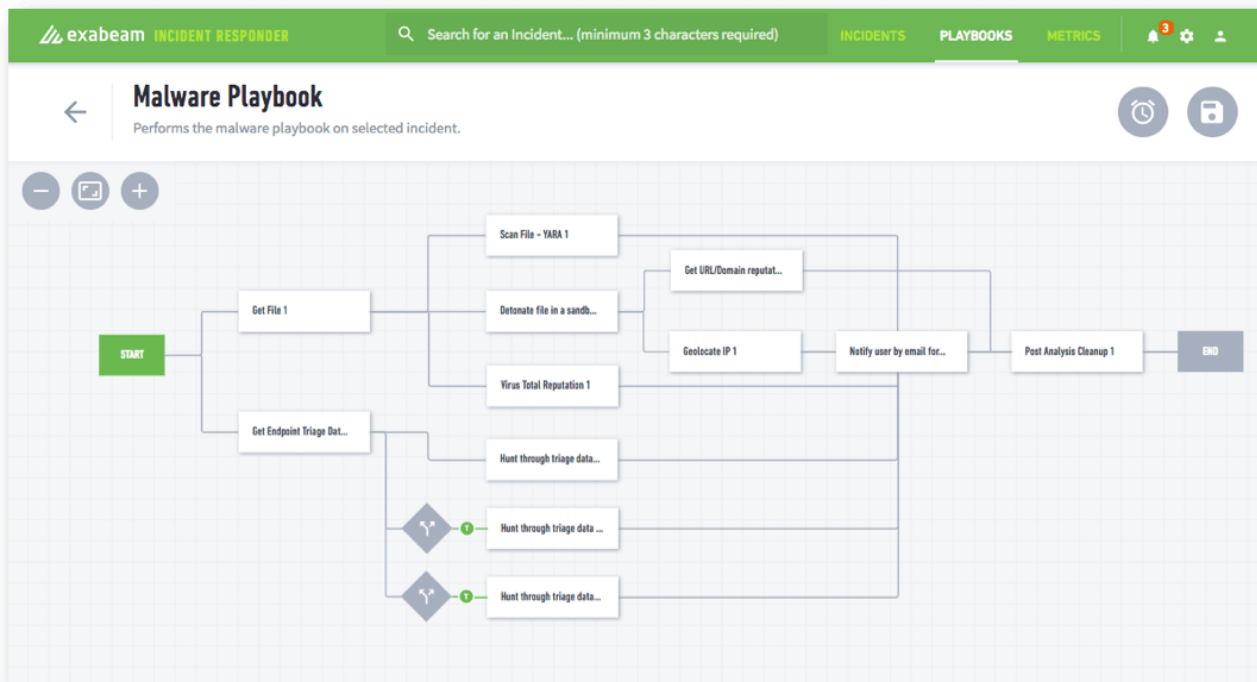


The screenshot displays the Exabeam Incident Responder dashboard. At the top, there is a search bar and navigation tabs for 'INCIDENTS', 'PLAYBOOKS', and 'METRICS'. The main area shows a list of incidents with filters for Assignee, Date, Incident Type, Status, Priority, and Keyword. Two incident cards are visible:

- SOC-1882: NOTABLE USER: GARY HARDIN** (Tier 3, New, Medium): Behavior Analytics / 2018-04-12 10:49:55 -0700. Description: Notable user reported by Exabeam Advanced Analytics on 2017-09-28. Risk Score: 106, User ID: ghardin, Reasons Count: 12, Alert Count: 1. Risk Reasons include abnormal activity, HR risk, application objects accessed, data upload, DLP violation, badge access, and web activity to low ranked domains.
- SOC-1881: MALWARE INCIDENT FLAGGED BY SYMANTEC E...** (Tier 3, New, High): Malware / 2018-04-12 10:49:53 -0700. Description: A Malware detection device has flagged a malicious file on a host and was unable to triage or determine its type, investigation is required. Malware Name: barbarian malware, Victim Host: lt-b201-fweber, Malware Category: strain command and control channel, Knowledge Base: https://support.symantec.com/en_US/article.TECH105518.htm, Attacker URL: 221.194.44.219, Attacker File: barbarian.jar, Attacker IP: 221.194.44.219.

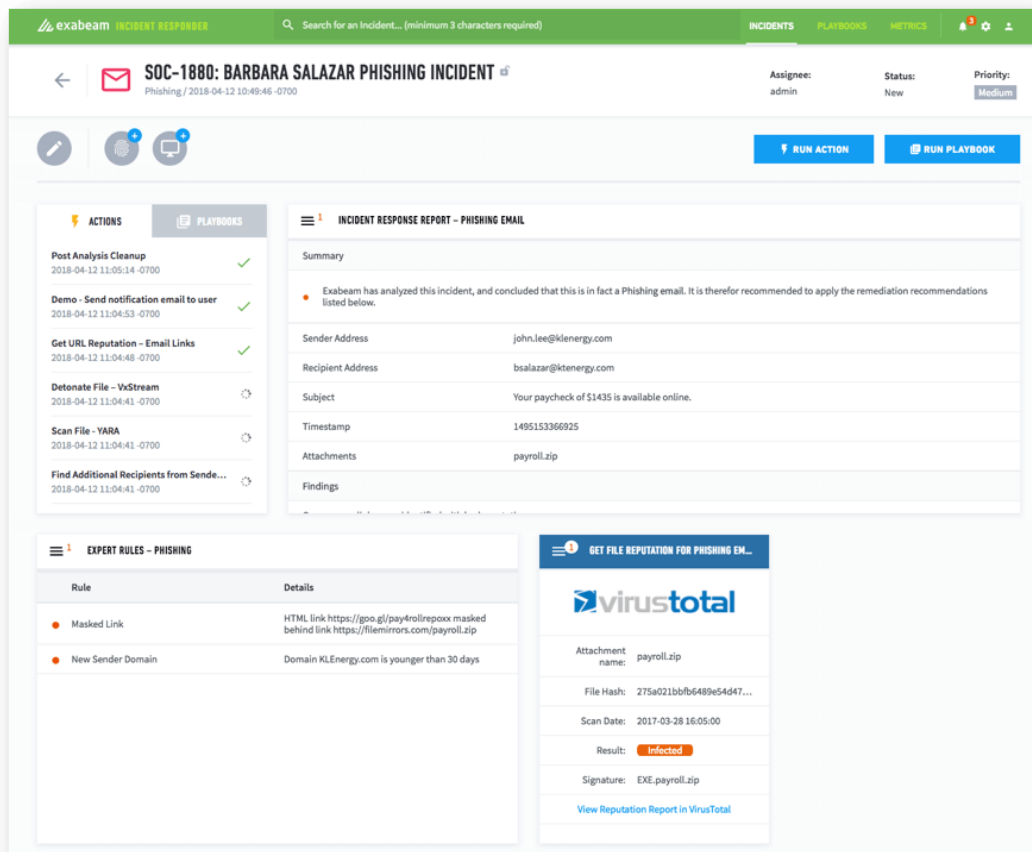
Customizable Case Management Designed for Security Teams

Incident tickets and alerts can pile up into the thousands, requiring a team for prioritization and response. Often security teams are using an outdated IT case management system not designed for security workflows. Scarcity of security talent spreads SOC teams too thin. With Exabeam, your SOC can use customizable tools designed for security incidents, ensuring that threats do not slip through the cracks.



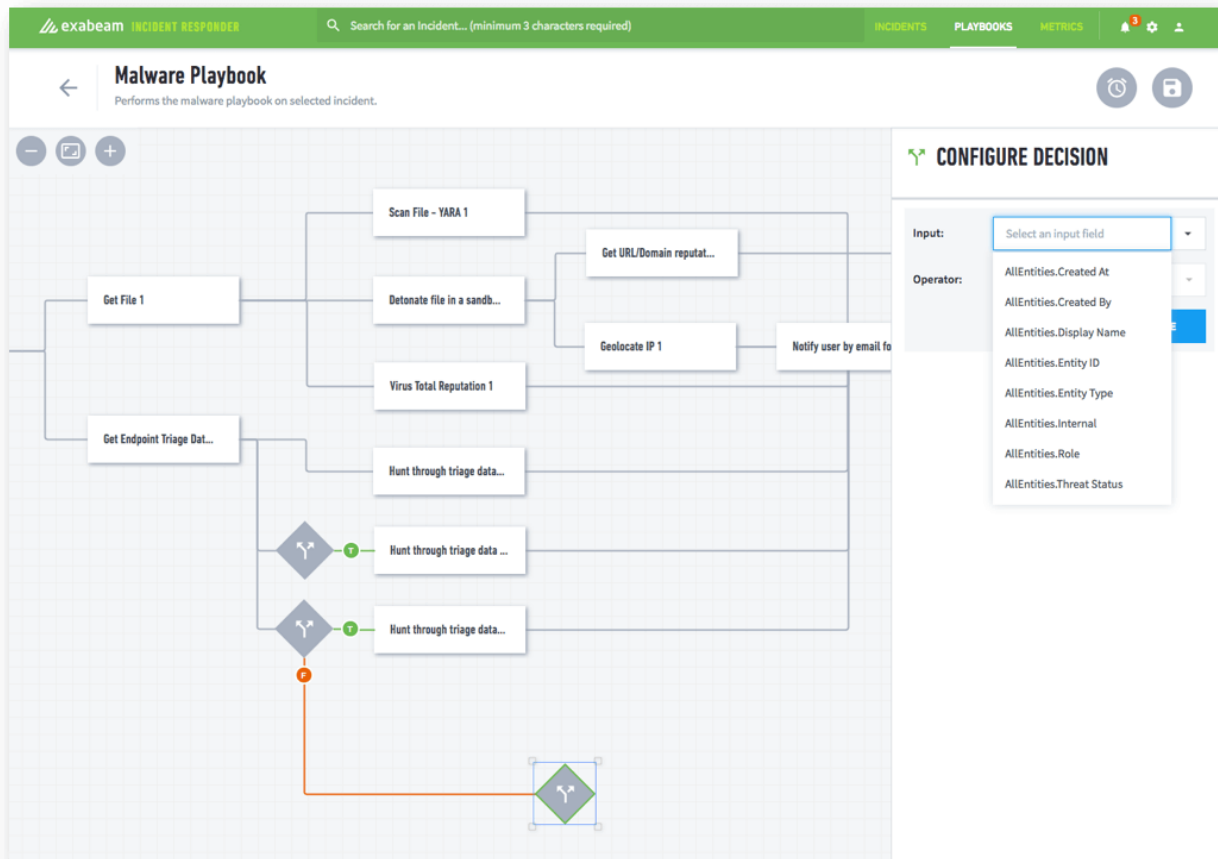
Centralized Security Orchestration Enables Rapid, Automated Responses

Security teams responding to an incident can use hundreds of tools, resulting in an inefficient “swivel-chair” response. A centralized approach and console are needed to pull in data and push actions to other systems. The Incident Responder prebuilt APIs connect and integrate all your systems, IT, and security tools, whether it’s email servers, active directory (AD), or your firewall, for a rapid automatic response.



Automated Incident Response Playbooks

Security threats happen repeatedly whether it's malware or an email phishing scheme. Some threats are predictable, while others are unique -- with responses requiring many steps. Incident Responder playbooks take programmatic actions that are semi or fully automated. Teams can automate investigations, gathering of evidence, containment, and mitigation to improve the success of their cyber security incident response processes.



Graphical Playbook Editor

With security automation and orchestration tools it can be very difficult to develop the needed playbooks that accurately take action with all the systems involved. The Incident Responder visual playbook editor dramatically simplifies security playbook development, using logic and flow charts that you can drag and drop to connect systems and create actions.