Security teams face unique challenges in today’s data-heavy landscape with sophisticated attackers and vast threat surfaces. Separating insights from the noise of incoming alerts and coordinating between multiple security products often involve repetitive tasks that waste valuable analyst time which could be put to more productive use.

Coordinating between different systems to capture/collaborate on application, website and enterprise systems data and logs is a repetitive task that sucks up valuable analyst time which could be spent threat hunting or responding to critical incidents.

The Demisto and Elasticsearch integration equips security teams with rich, correlated application and log data that can be leveraged during incident investigations or by playbooks for automated data enrichment and incident response.

### Benefits
- Leverage Elasticsearch alerts to automate triage and response.
- Automate extraction and enrichment to identify and auto-close false positives.
- Easily query Elasticsearch data within Demisto to shorten the incident investigation cycle.
- Enrich investigation data with rich context, analytics and correlations across products.

### Compatibility
- Products: Demisto Enterprise, Elasticsearch

### Integration Features
- Query Elasticsearch data to investigate or enrich incidents in Demisto and trigger automated triage and response.
- Leverage hundreds of Demisto third-party product integrations to further enrich incident data for investigations or coordinate response across security functions.
- Run 100s of commands (including for Elasticsearch) interactively via a ChatOps interface while collaborating with other analysts and Demisto’s chatbot.
USE CASE #1  AUTOMATED DATA ENRICHMENT AND INCIDENT RESPONSE

**Challenge:** If SOCs use different solutions for data enrichment and incident response, it can be tough to track the lifecycle of an incident due to fragmented information distributed across multiple locations. As a result, analysts spend time chasing data and completing these low-level tasks.

**Solution:** Elasticsearch alerts can trigger Demisto playbooks that orchestrate response actions across the entire stack of products that a SOC uses in a single seamless workflow. For example, analysts can create tickets, quarantine endpoints and send emails as automated playbook tasks.

In addition, Demisto’s classification mapping enables users to easily segment Elasticsearch alerts so that separate incident types can be created to run different playbooks that map to existing incident response processes.

**Benefit:** Automation of repetitive, manual tasks streamline incident lifecycle processes to speed incident triage and resolution. For example, as Elasticsearch alerts trigger playbooks, these playbooks can also fetch additional incident data from endpoint products and threat intelligence sources to determine if the alert might be a false positive or a duplicate that can be auto-closed.
**USE CASE #2**

**INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS**

**Challenge:** While automated playbooks can ease analyst load, an attack investigation usually requires additional tasks such as pivoting from one suspicious indicator to another to gather critical evidence, draw relations between incidents, and finalizing resolution.

**Solution:** After running playbooks, analysts can then gain greater visibility and new actionable information about the attack by running Elasticsearch commands in the Demisto war room. Analysts can query and view data in real-time for search, logging, security, and analytics use cases via the work plan and war room windows. Analysts can also run commands from other security tools in real-time, ensuring a single-console view for end-to-end investigation. The war room auto-documents all analyst actions and suggests the most effective analysts and command-sets over time.

**Benefit:** All participating analysts will have full task-level visibility into the process and be able to run and document commands from the same window. Auto-documentation of all automation and analyst actions allow for reports to be generated quickly for executive review or post-investigation debriefs.

---

**About Elasticsearch**

Elastic is a search company. As the creators of the Elastic Stack (Elasticsearch, Kibana, Beats, and Logstash), Elastic builds self-managed and SaaS offerings that make data usable in real-time and at scale for use cases like application search, site search, enterprise search, logging, APM, metrics, security, business analytics, and many more. For more information, visit [www.elastic.co](http://www.elastic.co/).

**About Demisto**

Demisto, a Palo Alto Networks company, is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Demisto, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit [www.demisto.com](http://www.demisto.com).