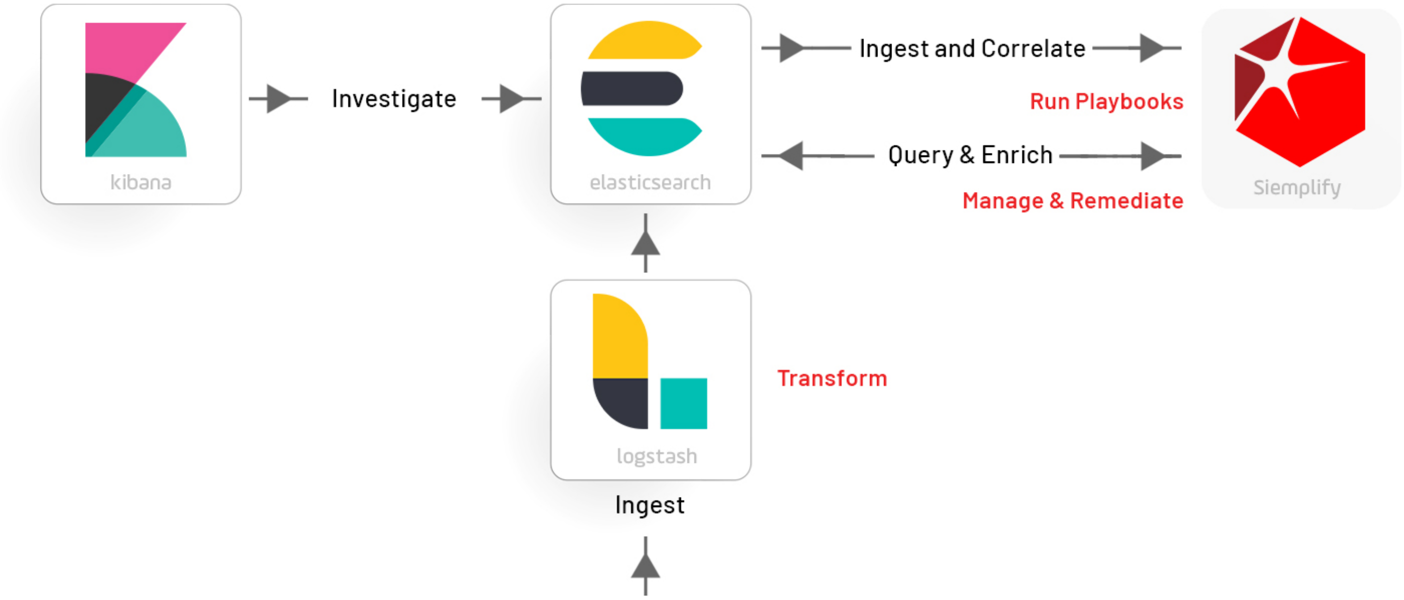
Siemplify x elastic

Elastic and Siemplify: Versatile SIEM. Powerful SOAR. Unparalleled Security.

Elastic, a leading provider of open-source enterprise analysis and search software, helps companies unlock critical insights hidden in their troves of data. Siemplify, the leading independent security orchestration, automation, and response (SOAR) provider, enables security operations teams to work more efficiently and effectively. Combining the Elastic Stack with the Siemplify Security Operations Platform enables security teams to detect, investigate and respond to threats faster than ever before.



Combining Elastic and Siemplify

The Elastic Stack, comprised of Elasticsearch, Kibana, Beats, and Logstash, enables organizations to collect, monitor, analyze, and identify any anomalies in their data. Powerful queries and Elasticsearch (ES) machine learning algorithms surface potential malicious activity, but this is only the beginning - the next logical step is to triage, investigate and eradicate the problem.

The Siemplify Security Operations Platform automatically ingests events from the Elastic Stack, and using a patented analysis engine, identifies and groups related alerts into threat-centric cases providing security analysts with a holistic view of the threat. Siemplify then triggers customizable response playbooks (aka runbooks) that automate repetitive tasks from enrichment to response. The combination of Elastic and Siemplify enables security teams to be up to 10x more productive and drive 80% faster response times.

Siemplify Capabilities

Intelligent Case Management

Reduce caseload by as much as 80% by working prioritized threat-centric cases that automatically group related alerts from across your detection tools.

Playbook Lifecycle Management

Build and automate response playbooks that orchestrate over 200 tools with simple drag and drop. Reusable playbook blocks and versioning simplify playbook lifecycle management as implementations scale and mature.

Context-Driven Investigation

Instantly understand and visualize the who/what/when of a security incident leveraging a patented contextual engine. Visualize the full threat storyline, then drill down and pivot on related entities to make faster, better decisions.

Machine Learning Recommendations

Machine learning-based recommendations leverage historical data to better prioritize and investigate alerts more effectively as well as assign the best analyst to a case.

Instant Collaboration

Harness the full power of your team and collaborate with internal and external stakeholders for faster more efficient incident response. All interaction is captured in a central, easily searchable and readily auditable repository.

Real-time Metrics and KPIs

Demonstrate the value of security operations to senior management and drive continuous improvement by tracking and analyzing a wide range of SOC key performance indicators across people, processes and technology.

Crisis Management

Enables organizations to streamline both tactical and strategic responses to a successful cyberattack in a virtual "War Room," ensuring all stakeholders inside and outside the SOC are working as a team.

Common Use Cases

The combined Elastic Stack/ Siemplify solution helps SOCs quickly and effectively address these common use cases

MALWARE INVESTIGATIONS WITH AUTOMATED THREAT HUNTING

PHISHING INVESTIGATION AND REMEDIATION

INSIDER THREAT IDENTIFICATION AND ERADICATION

BRUTE FORCE ATTACK IDENTIFICATION AND RESOLUTION

A real-world example from a SOC using Elastic with Siemplify:

An Elastic event has a host.IP field that is mapped to SourceAddress in Siemplify. When ingested Siemplify automatically creates a case and executes a playbook that initiates an ES query, using the source address placeholder as the search term.

Now a search will execute for any other events in ES containing this IP. Refer back to Kibana to investigate further with the Timeline feature of the SIEM App.

With Elastic and Siemplfy SOC teams can:

- Manage cases in Siemplify and refer back to Kibana and the Elastic SIEM App for active threat hunting.
- Investigate related alerts from multiple Elasticsearch indexes as part of a single threat-centric case
- Maintain a single source of truth for case archival
- Automatically run Elasticsearch queries from any playbook