Investigations With Sift Security

Faster response to incidents

We provide security operations teams an easier and faster way to discover, investigate and act on risks. This paper identifies 5 key challenges associated with security investigations and identifies how Sift Security's novel approach relieves alert fatigue and highlights the activity that results from complex attacks.

Investigations Challenges	Sift Security Solutions
Alert Overload	Provides better prioritization, confirmation and incident scoping
Unavailable Data	Lowers cost and complexity of implementing a security data lake
Manual Investigations	Presents an intuitive interface that accelerates common workflows
Inadequate Staffing	Simplifies investigations and response, enabling junior analysts and an extended team
Unknown Threats	Enabled proactive threat hunting, aided by advanced algorithms

Top 5 Challenges With Security Investigations

1. Alert Overload

Any investigation requires following a chain of entities and events. This user authenticated to that host, which ran this process, which touched this file, which was copied to that server, etc. If you only have a search index, then you have to write a bespoke query to take each intermediate step. This requires intimate knowledge of the formats and fields of the different kinds of records in the index, and the ins and outs of the query language. Crafting a query takes valuable time, and the query itself may take a while to execute if data from records of multiple types have to be joined. Then you have to parse the results, extract new entities of interest from the relevant fields, and start the process over again.

2. Unreliable Data

When it is time to investigate incidents, frequently the required data are not readily available. Oftentimes this is a result of security operations systems that are not scalable due to technical and / or economic limitations. The result is that analysts need to find and process the data. Only then can they start their investigations.

3. Manual Investigations

Once the investigation starts, all the pressure is on the analyst, who typically needs to comb through messy logs, manually correlate the data, and iteratively run queries. Assuming they are successful with their investigation, they typically need to use a separate tool to compile their reports and yet more tools to initiate the required actions.

4. Inadequate Staffing

We frequently hear from executives how hard it is to hire and retain security talent. Tier 1 analysts are often new in their roles, have limited security experience, and do not remain in that role for long. Many senior investigators complain that they get too many unvalidated incidents which take time away from diving deeper on more important incidents and proactively hunting threats.

5. Unknown Threats

Despite their best efforts, most organizations are unaware of important threats they have either missed entirely or lost in a sea of false positives. This leads to attackers having clandestine access to their systems for days, weeks, or months before their presence is discovered. Traditional security tools provide great defense against known threats, but fall short against new threats, even ones that are only incrementally different from those previously seen.

Sift Security Addresses these Investigation Challenges

Sift Security provides security operations teams an easier and faster way to discover, investigate and act on risks. Our product was built by and for security operators, with the goal of making these challenging roles easier and more enjoyable. Our technology was built from the ground up to take advantage of a relational graph data structure, which forms the foundation for our intuitive visualization and cutting edge analytics. This enables Sift Security to relieve alert fatigue and highlights the activity which might result from complex attacks.

> Sift Security reduces the time to investigate from weeks to hours, or even minutes
>
> *Colin Estep*
> *Incident Responder with experience at Netflix, Apple, FBI*

Specifically, Sift Security addresses the five investigation challenges as follows:

1. Alert Overload

Sift Security has a number of novel ways to address alert overload. First, we roll risks up to entities (e.g., users, hosts), identifying clusters of alerts and their commonalities. Second, we integrate a natural feedback loop into the investigation workflow. Sift Security learns from this feedback to prioritize only those alerts that are most important to the organization. Third, our product enables investigators to quickly drill down and evaluate an individual alert.

2. Unreliable Data

Sift Security leverages open big data technology and does not price our software on data volume like Splunk. As a result, enterprises can scale cost effectively enabling them to affordably create a data lake that includes all the data of interest to the security team. Since the data lake is built on open software, users can access the same data using third-party tools and technologies. Sift Security can be used to create a new data lake installation or analyze data in an existing data lake.

3. Manual Investigations

Sift Security's relational graph data structure provides a natural correlation across multiple data sources. This graph structure forms the foundation for our intuitive user interface and advanced algorithms. The graph structure enables analysts to make common queries without manually sifting through log data, and our algorithms help accelerate common workflows by automatically highlighting areas of interest in the graph.

4. Inadequate Staffing

Sift Security enables enterprises to get significantly more value out of inexperienced analysts by automating many of the task that are currently done manually, offering a simpler interface, highlighting anomalous behavior, and allowing seamless collaboration. This enables analysts to more quickly and effectively interpret alerts and conduct investigations.

5. Unknown Threats

Sift Security helps analysts identify unknown threats using behavioral anomaly detection. Through our graph investigation tool, users can investigate clusters and temporal spikes of behavior indicative of security risk. Sift Security also integrates well with other security tools and threat intelligence feeds, so you can find the hot-spots identified by multiple methods.

Sift Security in Action: An Example Investigation

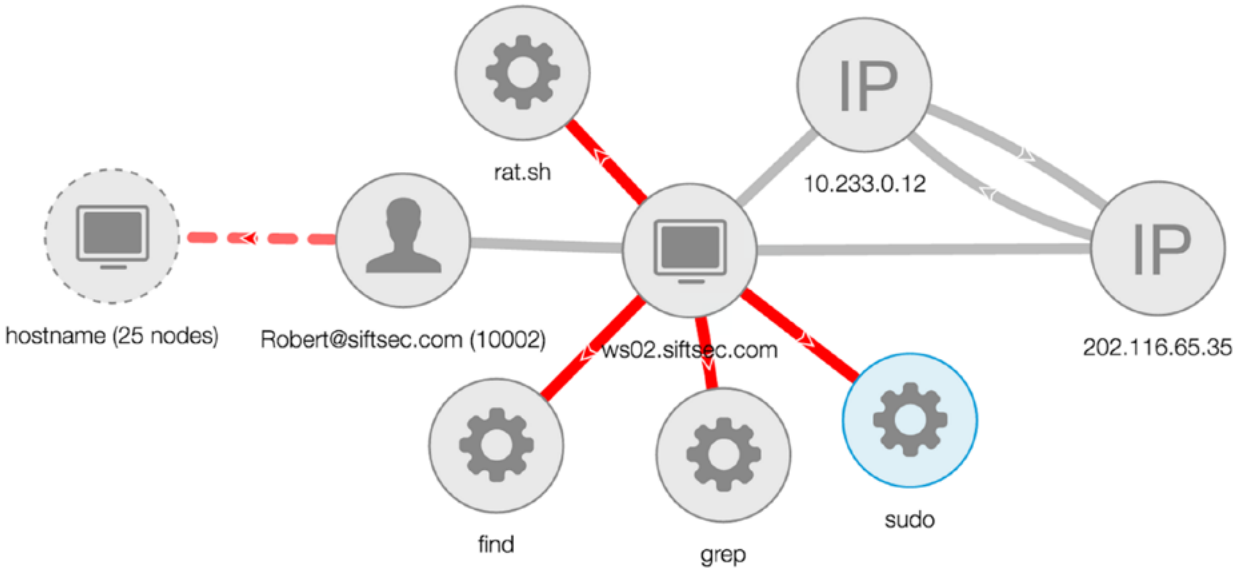
Consider a company targeted by a spear phishing attack, with an end goal of expropriating sensitive customer data. Here's how Sift Security could accelerate an investigation and stop the attacker from achieving their goals.

A junior security analyst, Lance, opens up Sift Security and sees a high-priority alert from its Netflow logs showing a connection to a blacklisted IP address. Lance pulls the alert into Sift Security and starts to investigate. He soon finds additional evidence of an attack in data drawn from host logs.

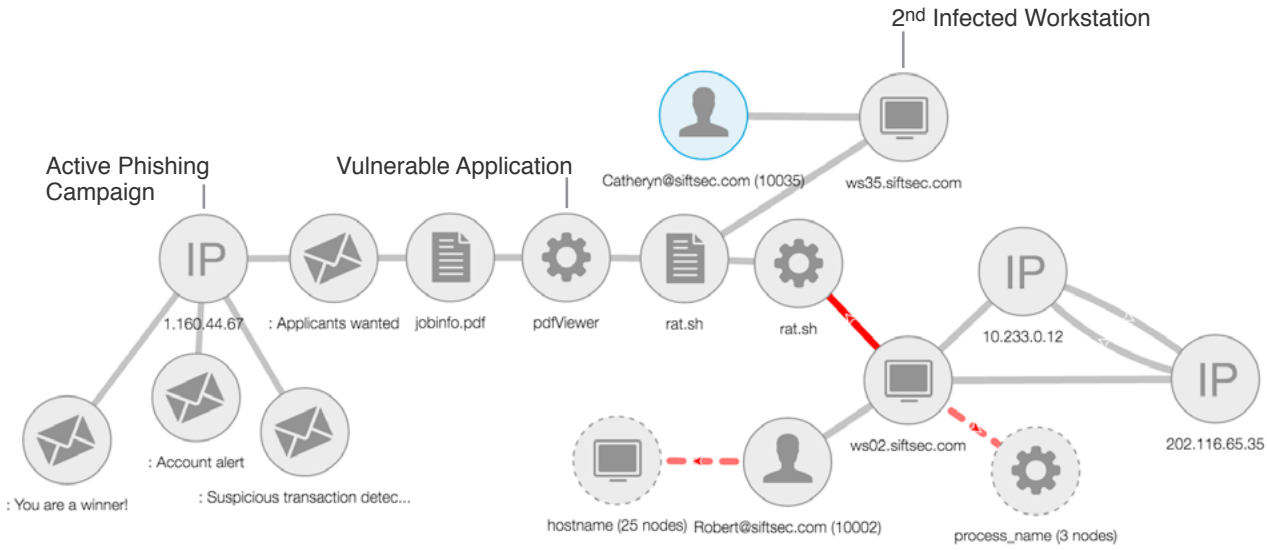
1. Connection to a blacklisted IP address, 202.116.66.35, which is identified as a command-and-control server. It turns out that a company host ws02 with IP address 10.0.0.2 had communicated with that IP yesterday.

2. Anomalous processes on Robert's workstation, ws02.sfitsec.com, such as processes typically associated with reconnaissance activity and possible malware.

3. Anomalous authentication attempts by a user Robert. He had a glut of failed authentication attempts, spread over nearly 40 hosts over the course of a day. Possible evidence of malware attempting lateral movement.



At this point, Lance turns the investigation over to Ted, a senior incident responder. Ted continues the investigation to find the root cause and better understand the full impact of the threat. He traces the investigation back to a phishing email that exploited a vulnerability in pdfViewer to drop a remote access terminal on Robert's workstation. He searches for other machines that contain this file and finds that ws35 is also infected. He investigates the source of the email message to find that the sender was also responsible for sending highly suspicious emails to other employees, each containing attachments.



Sift Security facilitated this investigation in a number of ways. First, it drew Ted's attention to the firewall alert, emphasized because it was related to anomalous user behavior and access to sensitive data. Second, it enabled Ted to easily pivot across netflow, host, and email data sources. Third, it enabled the junior analyst (Lance) to validate the initial alert and collaborate with the senior analyst (Ted). It also helped Ted to quickly complete the root cause and impact analyses. This allowed Ted to find previously unknown threats and to identify and initiate all the actions needed to protect the enterprise and stop the infiltration before any major damage was inflicted.

Key Sift Security Advantages

Flexible Data Support

Sift Security can easily ingest structured and semi structured data such as network, host, security alerts, email, applications and more. This data can be pushed from your existing SIEM or log management tool or collected directly.

Open And Scalable Architecture

Sift Security includes tight integrations with leading big data architecture such as Kafka, Spark, Elasticsearch, and Titan graph database.

Advanced Analytics

Sift Security includes innovative analytics out of the box, including a custom rules engine with a library of rules, machine learning with a feedback loop, and graph algorithms.

Intuitive Visualiztion

Sift Security offers the most intuitive user experience available, and includes seamless integration between alerts, search, graph, report, and collaboration capabilities.

About Sift Security

Sift Security provides security operations teams an easier and faster way to discover, investigate and act on risks. Sift Security was built from the ground up to take advantage of a relational graph data structure, which forms the foundation for our intuitive visualization and cutting edge analytics.

Email contact@siftsecurity.com to learn more.

We can provide a live demonstration of our product and answer your questions. Also, we have a few options to try our product for free, which can be as easy as getting a username and password to use our product on the same data set we use for our demonstrations.

SIFT SECURITY

1259 El Camino Real, Suite B
Menlo Park, CA 94025

Worldwide Sales:
Tel: +1.855.743.8732
Email: sales@siftsec.com