Proactively Hunt for Threats Using Sift Security

Many mature security organizations have people or teams focused on proactively hunting for threats. One of Sift Security's co-founders, Ram Sripracha, spent a lot of time in his previous role on Amazon's security team hunting for threats using a leading enterprise search tool. This experience inspired him to create Sift Security to fill-in the gaps he found in existing security tools.

Requirements for Threat Hunting

Based on our experience and the conversations we have had with dozens of incident responders and threat hunters, there are 5 key requirements for effective threat hunting.

1. High Quality Starting Points

Hunters have limited time and need tools to help focus their attention on the areas most likely to contain risk.

2. Immediate Access To Data

Hunters need access to all data that contain evidence of risks to develop and test hypotheses.

3. Seamless Pivots

Complex threats leave evidence in many places, so Hunters need the ability to easily pivot across data sources and dive into the raw data.

4. Practical Visualization

Hunters need more than eye candy, they need practical visualization to help them more easily investigate the data.

5. Actionable Intelligence

Hunters benefit from intelligent algorithms that accelerate their investigations and point them towards the most interesting results.

How Sift Security Enables Threat Hunting

Sift Security was built from the ground up to be the best product available for threat hunting. This is how we address the requirements above.

1. High Quality Starting Points

Sift Security makes available many starting points for Threat Hunting: Alerts from third party detection tools, out of the box and custom rules, and risky entities flagged by our machine learning algorithms.

2. Immediate Access To Data

Sift Security is built on top of open big data technology that scales inexpensively on commodity hardware, and is not priced based on data volume like other search and SIEM tools.

3. Seamless Pivots

Our graph canvas user interface provides an aggregated view of the data, and makes it easy to follow an investigation no matter where it leads.

4. Practical Visualization

Sift Security offers the easiest to use graph investigation tool available, and includes a wide range of out of the box and custom visualization tools and dashboards.

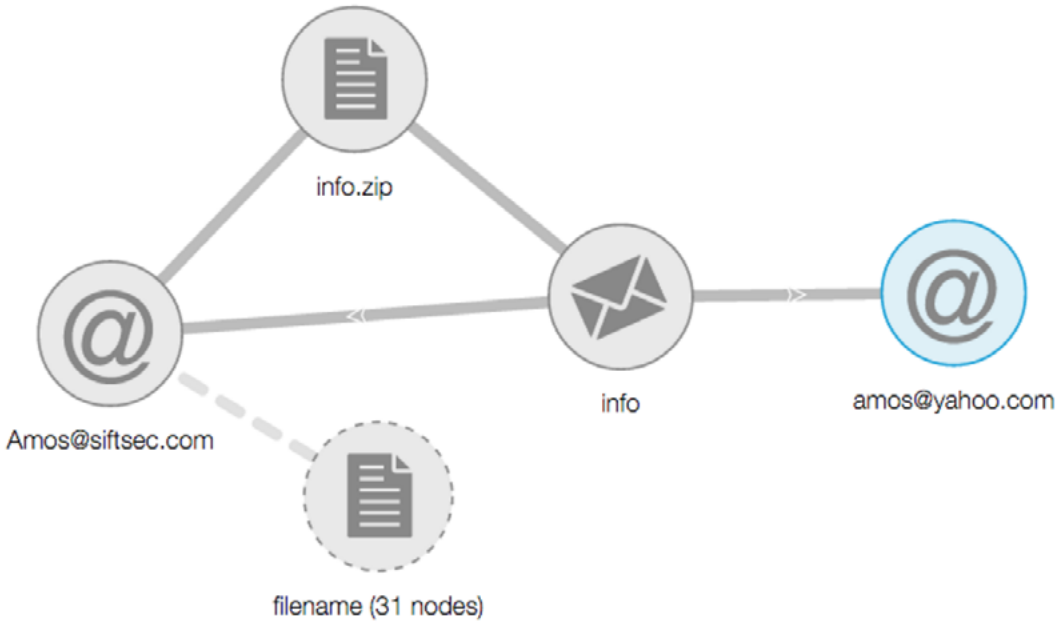
5. Actionable Intelligence

Sift Security's algorithms are constantly running in the background to identify known threats and risky behavior and are integrated into the hunting experience.

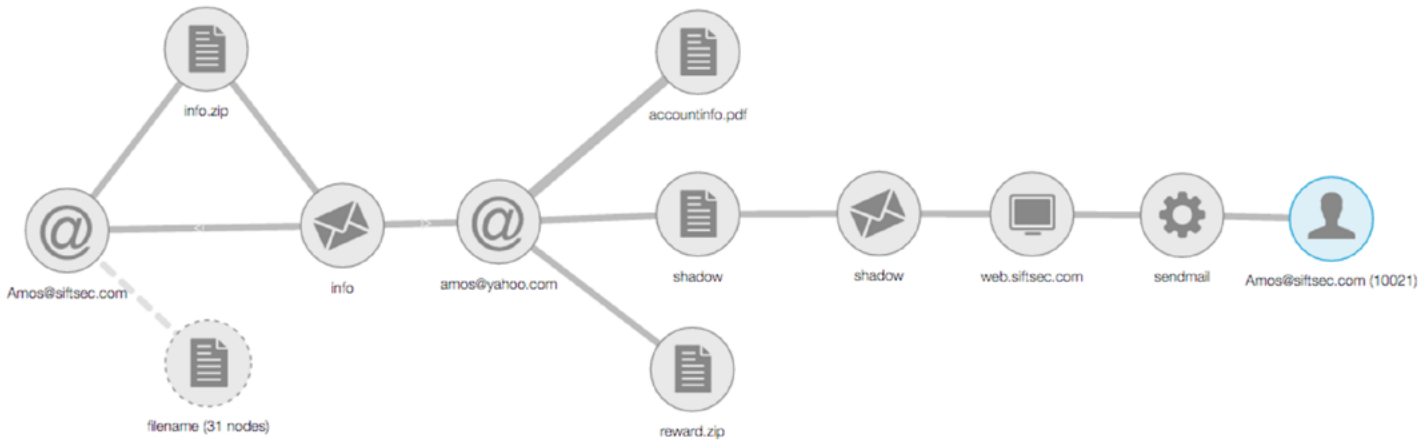
Sift Security in Action: An illustrative Threat Hunt

Consider an employee, Amos, who is leaving the company under unusual circumstances. We have reason to suspect that Amos might be stealing confidential information. Here is how Sift Security could be used to determine whether Amos poses an insider threat.

In our deployment of Sift Security, we are monitoring email metadata, network activity, and host audit logs. Since one of the most common channels over which data are expropriated is email, we begin the investigation at Amos's email account. We narrow our investigation to the past few days, and look at all of the files Amos attached in email messages. We find 32 such attachments and begin investigating the largest one. We identify the message to which it was attached and the recipients to which it was sent. We find a target email address that appears to be a personal account belonging to Amos.

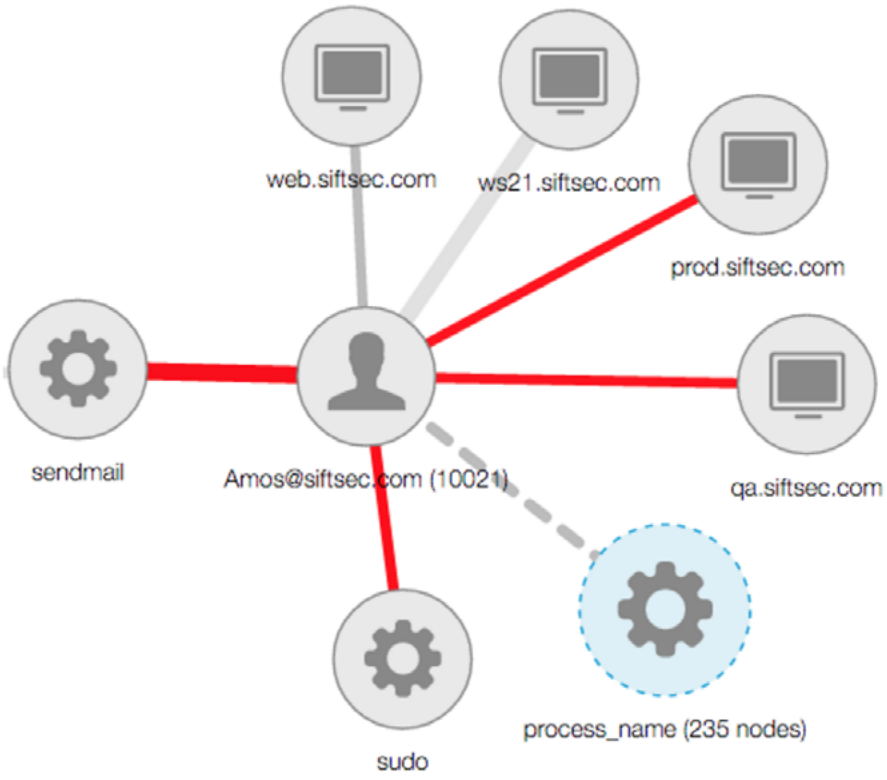


Next, we focus on Amos's personal email address. First, we identify what other files have been sent to this personal address. We find a few more files, among which is shadow. Because this might be a password file for a Unix system, we continue our investigation here. We identify the message to which it was attached and the host from which it was sent. We find that it was sent by Amos from our webserver.



At this point, we know that Amos has been expropriating data by sending files, including our web server password file, to his personal email address. At this stage, we revoke Amos's access and continue the investigation. With Sift Security, we can investigate each of the files Amos sent to himself and determine what other systems and information he accessed ahead of his departure.

Sift Security facilitates this investigation in a number of ways. It seamlessly enables pivots between multiple log sources, like email and host audit logs. Its graph queries provide rapid results to common queries that would otherwise require multiple search queries and intimate knowledge of log formats. Its built-in machine learning and intelligence also automatically highlights abnormal behavior during an investigation, for example by showing the abnormal process execution and authentication events surrounding the user Amos. These features help threat hunters quickly find, investigate, and verify potential threats.



Why not just use Search for Threat Hunting?

Sift Security's co-founder and many security analysts with whom we have spoken have shared many common challenges with regards to using Search to hunt for threats.

1. Cost

The pay-by-the-byte business model results in critical data not being ingested to save money, rendering the data unavailable for analysis and investigation.

2. Complexity

Indexing log data is easy, but investigating a complex threat that leaves evidence across multiple data sources is difficult. Pivoting between data sources requires performing manual queries and correlations. This requires intimate knowledge of the tooling.

3. Lack Of Intelligence

All the pressure is on the analyst to ask the right question and dig through logs looking for answers.

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 can be collected directly.

Open And Scalable Architecture

Sift Security is deployed on clusters of commodity hardware and includes tight integrations with leading big data architecture such as Kafka, Spark, Elasticsearch, and Titan Graph database. These work together, but customers also have direct access to these technologies.

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