

Sift Security helps SecOps teams analyze and visualize patterns of threats and speed up investigations

By Linda Musthaler, Principal Analyst with Essential Solutions Corp.

There's a powerful new generation of security tools coming to market designed to help security operations (SecOps) teams find and react to threats much quicker than before. The best of these tools also enable security analysts to proactively hunt for threats that might be present in their enterprise environment.

These tools bring data together from disparate sources and begin to connect the dots so analysts can dive right into the investigation without having to search for relevant data points. The products tend to eliminate the manual work of sifting through logs, finding all the relevant data, and trying to find correlations among the events.

Why are these tools so desperately needed? Consider some of the statistics that illustrate the pain points of the enterprise security operations team:

- According to Mandiant, the average number of days it takes to detect a data breach is 205.
- Verizon says the detection deficit is getting worse, and approximately 80% of compromises are detected by law enforcement or third parties.

Gartner says that detection is only a small part of managing an incident, with the majority of the work coming after the discovery and requiring more resources.

Ponemon Institute reports that, on average, organizations receive almost 17,000 alerts a week just on malware alone. Of these, only 3,218 are deemed reliable and 705 are actually investigated. What's more, organizations waste an average of 395 hours per week detecting and containing malware because of false positives and/or false negatives, costing approximately \$1.27 million annually.

Symantec reports there will be a projected shortfall of 1.5 million cybersecurity professionals by the year 2019, meaning the people who currently do this job are stretched thin.

Clearly, SecOps teams need a better way to work.

[Sift Security](#) is a new player that is out to make it easier, faster and less frustrating for SecOps teams to get their jobs done. Sift Security's Threat Hunting & Investigation Platform has a visual user interface that helps the security analyst see complex threat patterns at a glance. The UI shows which anomalous activities and entities are related and helps to prioritize the alerts that deserve further investigation.

The Sift Security platform has four elements: Graph Mapper, Sifter, Investigator and Terminator. Here's how they work together.

As soon as a customer installs the Sift Security software (on premises or on AWS using commodity hardware), the platform begins to ingest data from whatever sources are pointed to it. These can be existing logs or custom or proprietary logs. Since Sift Security's software isn't priced according to data volumes like some security products are, the customer can feed the Sift Security platform as much data as desired. Graph Mapper then creates a graph data structure and index from the raw logs. This is where meaningful relationships among entities such as workstations, hosts, networks and applications start to emerge.

In the next stage, Sifter identifies known threats, clusters of risk and anomalous behavior. Sifter uses third party and custom rules to identify known bad IP addresses, malware and so on. Using unique algorithms and novel data science techniques

developed at MIT and Stanford universities, Sifter is able to find previously unknown threats.

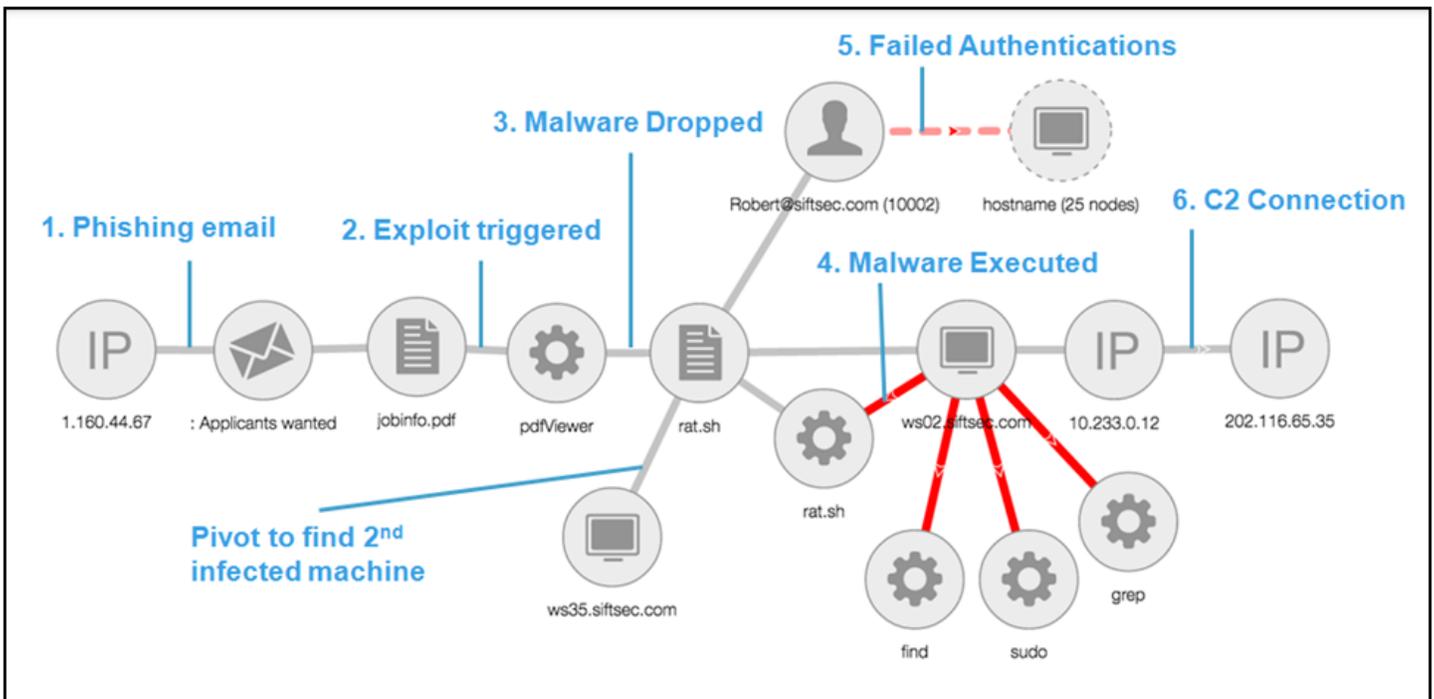
The next element, Investigator, is the UI that combines graph, search and dashboards. The graph UI makes it easy to see patterns and pivot across entities to trace an incident across the environment. Customizable dashboards allow a customer to build views of what they prefer to see.

And finally, Terminator is a workflow and API integration that is said to enable seamless collaboration among team members and the actions to address threats. The workflow enables the incident response team to work easier and faster. For example, say a junior analyst starts the investigation and takes it as far as they can. Then they share it with a senior

analyst to continue with the investigation and take it to its conclusion. Actions can include things like opening a ticket or adding an IP address to a block list.

Now let's take a more detailed look at how an analyst can conduct an investigation using the graph data structure. The investigators would use a graph similar to the one below to see what triggered an alert. Minus the chart labels, the graph is part of the actual user interface, which is interactive to allow for pivoting and drill-downs.

In terms of how an attack that triggered an alert happened, it goes in the numerical order seen in the graphic below.



1. A user receives a phishing email and clicks on the malicious attachment
2. The exploit, embedded in a PDF file, is triggered.
3. Malware (rat.sh) is dropped on the user's workstation (ws02.siftsec.com). The malware is also on a second host (ws35.siftsec.com).
4. The malware is executed and it performs reconnaissance activities.
5. A user's account (Robert@siftsec.com) is used to attempt logins to other hosts.
6. An infected workstation reaches out to a blacklisted C2 server to receive further instructions.

Numerous activities in this graph could trigger an alert: failed logins, anomalous behaviors, communication with a blacklisted IP, etc. This would escalate the priority of the investigation.

