



## Why Graphs Are Great For Security

*Speed. Intuition. Learning.*

Investigating a security risk can involve wrangling dozens of data sources. To uncover a successful phishing attack, you might have to integrate email records, process executions, user behavior, file access, netflow, antivirus alerts, etc. Gathering and correlating those logs is slow and cumbersome, making it difficult to follow the attack chain.

Sift Security's product extracts the most important information from disparate data sources into one straightforward, scalable system: a relational graph. Using the graph makes investigations *faster, easier, and more intuitive*. The graph also provides context to our machine learning platform, enabling it to discover and prioritize relevant anomalous activity.

### Sift Security's relational graph is a data structure with two parts:

- **Vertices** representing entities (like the user account Robert or host ws02.siftsec.com)
- **Edges** representing relationships (like my successful logon attempt)

The graph represents real relationships extracted from logs. At the same time we ingest a log into the index, we extract the relationships between the entities contained within.

For example, consider the following log entry:

Microsoft Windows audit log entry:

```
{ "EventTime": "2016-02-15 20:18:49", "Hostname": "ws02.siftsec.com", "Keywords": "-9214364837600035000",
  "EventType": "AUDIT_SUCCESS", "SeverityValue": 2, "Severity": "INFO", "EventID": 4624, "SourceName": "Microsoft-
  Windows-Security-Auditing", "ProviderGuid": "{54849625-5478-4994-A5BA-3E3B0328C30D}", "Version": 2, "Task":
  12544, "OpcodeValue": 0, "RecordNumber": 494242, "ActivityID": "{B0DAF283-66D6-0003-8EF2-DAB0D666D101}",
  "ProcessID": 744, "ThreadID": 1824, "Channel": "Security", "Category": "Logon", "Opcode": "Info", "SubjectUserSid":
  "S-1-5-18", "SubjectUserName": "WS02$, "SubjectDomainName": "WORKGROUP", "SubjectLogonId":
  "0x3e7", "TargetUserSid": "S-1-5-21-2257405197-1984329406-3649188883-1001", "TargetUserName": "robert",
  "TargetDomainName": "siftsec.com", "TargetLogonId": "0x185ed31", "LogonType": "2", "LogonProcessName":
  "User32 ", "AuthenticationPackageName": "Negotiate", "WorkstationName": "WS02", "LogonGuid": "{00000000-0000-
  0000-0000-000000000000}", "TransmittedServices": "-", "LmPackageName": "-", "KeyLength": "0", "ProcessName":
  "C:\\Windows\\System32\\svchost.exe", "IpAddress": "127.0.0.1", "IpPort": "0", "ImpersonationLevel": "%1833",
  "RestrictedAdminMode": "-", "TargetOutboundUserName": "-", "TargetOutboundDomainName": "-", "VirtualAccount":
  "%1843", "TargetLinkedLogonId": "0x185ed4f", "ElevatedToken": "%1842", "EventReceivedTime": "2016-02-26
  12:03:02", "SourceModuleName": "windows", "SourceModuleType": "im_msvistalog" }
```



The graph representation simplifies this process and speeds it up. To see the hosts authenticated to by the user joshb, you select the vertex joshb and then the edge type authentication. To see the processes that ran on one of the returned hosts, you select its vertex and the edge type process execution. The graph data structure is optimized to make taking each of these steps almost instantaneous. The revenue and reputation of a company may depend on quick discovery and remediation of a security breach. By paying the compute cost when the data is ingested, you save time when it really matters: during an actual investigation.

## ■ Graph Investigations Are More Intuitive

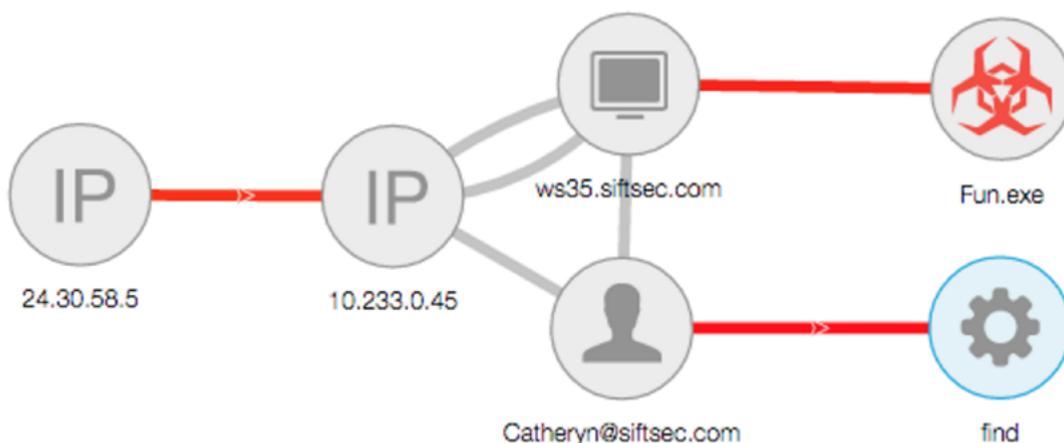
When you perform an investigation, a cast of characters emerges: users, IPs, geolocations, processes, servers, etc. The user interface for the graph puts those characters front and center, letting you see the story emerge. Instead of copying and pasting an IP into a text document with your notes about what it is related to, you can place it on the screen, visibly in context.

This graphical canvas helps you work at a higher level, making it easy to ask the right questions. Of course, the graph is linked to the underlying indexed data, so you can always drill down to the details of the logs whenever you like. Pivoting between the low-level log data and the higher-level graph representation helps you keep track of even a complex narrative.

## ■ Graphs Power Prioritization And Machine Learning

A typical enterprise network has a lot of alerting products, so finding the highest priority alerts is a critical challenge. Using the context provided by the graph, Sift Security clusters alerts involving related entities. For example, a spike in network traffic from an IP, malware detected on a related host, and erratic behavior from a user on that host can be correlated and brought to the fore. The graph enables intelligent prioritization, powering machine learning algorithms that cut down on alert fatigue.

The graph also surfaces alerts in context. If you start with an entity of interest, say an employee who unexpectedly resigned, you can surface alerts or unusual activity that, while not featuring their name exactly, are still indirectly related through connections in the graph.



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

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