SIFT SECURITY

Detection Use Cases

Sift Security provides two distinct detection mechanisms: a custom rules engine and an advanced anomaly detection platform.[1] Both tools come with built-in support for common use cases and are extensible, enabling users to easily add detection features on the fly.

The Sift detection tools are advantageous because they leverage existing data are are lightweight, customizable, and extensible. Our detectors provide additional value on top of existing tools, such as firewalls and traditional AV and IDS, and are specifically tailored to detect common phases of cyber-attacks. Instead of providing individual alerts, Sift Security considers these alerts in context, prioritizing alerts that are components of a more serious attack.

This document describes some of the use cases supported out-of-the-box by our custom rules engine and advanced anomaly detection platform. Each detection is described in the context of the cyber kill chain, which can be partitioned into the following phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. For each detection described below, the types of data sources used to support it are listed.

Reconnaissance

Scanning

Scanning and reconnaissance can be performed from outside the network by someone looking for a way in, or someone inside the network looking to move laterally or gather information for future attacks. Such behavior is detectable because it often involves rare events occurring: network traffic between hosts that don't typically communicate, ports that aren't normally used, users or hosts who don't typically perform certain actions, or an abnormal volume of attempts to connect between machines. Sift Security monitors all of these features and more to identify the source of scanning and recon behaviors.

Data sources: netflow, firewall

Weaponization

The weaponization phase typically occurs on the attacker's end, leaving no detectable artifacts on the victim's network.

[1] For more details about our data science approach, request our Data Science Whitepaper - contact@siftsec.com

Delivery

DNS Fast Flux

DNS fast flux is a technique commonly used by botnets, especially for malware delivery and phishing. It involves rapidly changing the IP addresses associated with a hostname. Sift Security can detect fast flux and other suspicious DNS activity.

Data sources: DNS logs, network traffic analysis

Exploitation

Privilege Escalation

Privilege Escalation refers to an attacker gaining an unauthorized level of permission on a system. This usually happens through attacks on the account passwords (Windows hashes, weak passwords that replicate the username, e tc.) or attacking the vulnerabilities of a privileged process. Sift Security monitors activity from host logs to find abnormal connections and system level operations indicative of this type of attack.

Data sources: authentication, host audit logs

Compromised Credentials and Insider Threats

Sift Security monitors multiple behavioral features to identify possibly compromised credentials and insider threats. We look at normal behavior surrounding a user and alert on any outliers, such as access from abnormal IP addresses or geolocations. Another technique we use is process analysis. As with network ports, users and hosts typically execute a relatively predictable set of processes. By identifying users who violate these and other patterns, we can identify potential compromised credentials and insider threats.

Data sources: authentication, host audit logs

Installation

Compromised Hosts

Many of the features used to detect compromised user credentials and insider threats can also be used to identify compromised hosts, when collected at the host level. By monitoring processes, authentication events, and other behavioral features we can identify hosts that have been compromised.

Data sources: authentication, host audit logs

Command and control

Rogue Network Services

Workstations and servers typically contain known software, using a relatively predictable range of ports. Adversaries and certain types of malware may install new network services that alter this behavior, which is detected through Sift Security's machine learning techniques.

Data sources: netflow, host audit logs, firewall logs

Actions on Objectives

Lateral Movement

Lateral movement refers to the spreading of an attacker's footprint inside an organization after they have gained an initial foothold. Commonly used techniques in the Windows ecosystem include Pass-the-Ticket (PtT) and Pass-the-Hash attacks (PtH), wherein an attacker dumps credentials from memory and uses them to move internally within an organization.

Sift provides rules and anomaly detection techniques to identify unusual authentication patterns that are indicative of lateral movement. We have also developed advanced heuristics specifically for identifying PtT and PtH style attacks.

Data sources: authentication

Data Exfiltration

Data exfiltration refers to the unauthorized transfer of data, and can be performed by either an insider-threat or a malicious outsider. Sift Security includes rules and algorithms for detection of abnormal network traffic patterns indicative of data exfiltration, such as the use of DNS as a malicious channel.

Data sources: netflow, firewall, DNS logs

DHCP Attacks

DHCP DoS attacks can be achieved either by having malicious clients requesting all of the available IP addresses, or by having malicious servers providing incorrect IP addresses. Sift Security detects abnormal DHCP behavior to identify both types of malicious actors.

Data sources: network traffic analysis, DHCP server logs

DDoS

Distributed denial of service (DDoS) refers to a style of attack where a distributed adversary aims to disrupt normal activity by overwhelming a target. Sift Security's machine learning algorithms leverage aggregate statistics associated with possible targets to detect DDoS attacks that might be part of a larger cyberattack.

Data sources: netflow, firewall

Email contact@siftsecurity.com to learn more.

SIFT SECURITY

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

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