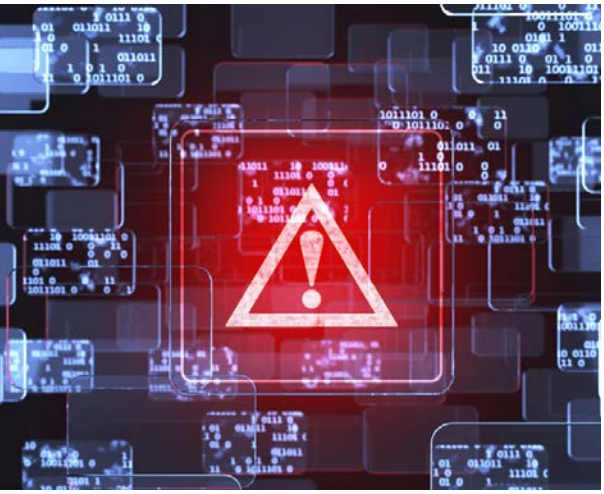
DATA SHEET

ALERT VALIDATION

Validate Security Alerts with Infocyte HUNT™



FALSE ALARM OR REAL THREAT?

Despite the rich data provided by SIEMS many organizations find themselves drowning in false positives, making it difficult to sift through and gain visibility into high priority and relevant events.

Infocyte HUNT provides ground truth with an automated solution to help validate alerts from your SIEM, network or endpoint product by performing a scan of the endpoint in question to determine if the threat is real so you can take swift action.

- Triages alerts to weed out false positives and quickly identify which to escalate.
- Reduces the time and resources needed to manually comb through volumes of false and low priority alerts.
- Allows your security team to focus on remediating real threats.
- Leverages your existing security investments.

Suffering from Alert Fatigue?

Many enterprises rely on security information and event management (SIEM) solutions to help detect suspicious activity on their networks. However, despite SIEM's attempts to dedup, contextualize, and correlate thousands to millions of alerts on a daily basis, many organizations find themselves drowning in irrelevant and/or false positive data, increasing the likelihood that a real threat will be missed – wreaking havoc on your systems and reputation.

One of the relatively recent and high profile cases of 'alert fatigue' was the Target breach in 2013, which resulted in 40 million stolen payment card records, and the loss of a CEO's job. The malware was detected, thousands of alerts fired, were reportedly seen by SIEM monitoring personnel, but ignored due to millions of other alerts being received in the same timeframe. This visibility to, and fast focus on, what is actually a real threat is a challenge for all security teams – whether a small team with no SOC, a large enterprise with a SOC, or an MSSP that oversees many customers with a SOC.

SIEMs and other security systems collect and aggregate data from a variety of sources including: Firewalls and Web Proxies, Intrusion Detection / Prevention Systems, IP/DNS Traffic Logs and PCAPs. SIEMs aggregate, dedup, correlate, and with more advanced systems, attempt to find the "needle in the haystack".

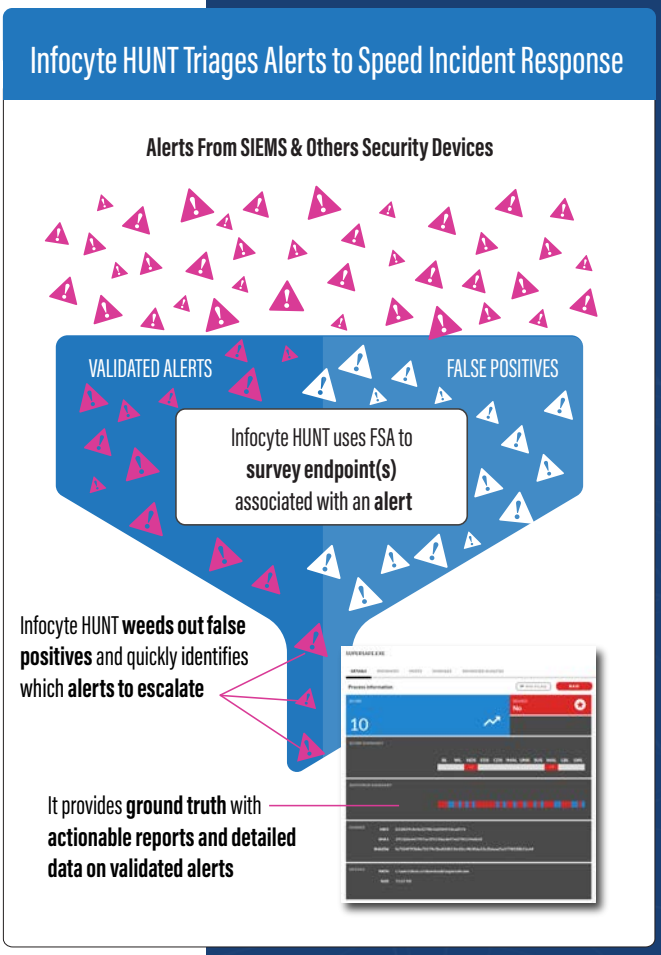
However, sophisticated attacks easily game defense systems, and false positives continue to waste the time of limited personnel. Average enterprise class organizations can receive 17,000 malware alerts per week. Of that, fewer than 20 percent are worthy of examination, and only 4 percent of valid threats are actually investigated.[1] Why? Alerts often requires human oversight and validation to confirm legitimacy. Most organizations simply don't have the resources to recognize legitimate alerts, let alone examine them to determine root cause and infected machines quickly and cost-effectively.

Infocyte HUNT Provides Relief

What's needed is a triage process to investigate alerts and determine which alerts can truly be ignored and which are actionable threats that need escalation. Infocyte HUNT provides ground truth – enabling security staff to vet alerts captured by your SIEM and prevent wasted time on innocuous alerts and/or false positives. Unlike SIEM alerts that are often correlated from two or more secondary or tertiary security product alerts that often lead to erroneous conclusions, Infocyte HUNT surveys endpoint using Forensic State Analysis (FSA) techniques to look for irrefutable evidence of malware that has successfully bypassed traditional defenses.

[1] https://swimlane.com/cybersecurity-statistics-2017/

Infocyte HUNT provides an integrated endpoint interrogation solution to validate alerts by looking at the compromise state of endpoints. The Infocyte platform uses dissolvable agents to independently collect, identify and evaluate a variety of data (active processes, in-memory executable codes, auto-runs, execution artifacts, OS subversion, API hooks, abnormal configurations, disabled controls and more), then analyzes the data using forensic analytics and file intelligence services. This Forensics State Analysis (FSA) based approach, also analyzes OS and application persistence mechanisms – which can trigger the execution of code or executables. This provides a far deeper, and more conclusive, examination of an endpoint's state to let you know if the alert is in fact real.



How it Works

There are two "alert triage" use cases for Infocyte HUNT:

The first approach is to use your existing analytics system and investigative procedures to whittle down existing SIEM alerts to a short list that warrant deeper investigation. Short-listed SIEM alerts can then be set to automatically trigger an API-driven Infocyte HUNT survey of the affected endpoint. Ground truth evidence of a compromise that has bypassed defenses - and relevant forensics - are returned to the SIEM. If a compromised host is identified with Infocyte HUNT, the analyst can pivot on key attributes of the finding to create a timeline of events (i.e. on all events with the same IP Address).

As teams become more comfortable with the power of Infocyte HUNT, it makes sense to start the triage process with an Infocyte HUNT survey; of some or all of an organization's endpoints, and at some meaningful frequency. Infocyte's endpoint surveys return information gathered along with analysis. The platform uses dynamic threat scoring to flag the severity of found issues, enabling analysts to focus their efforts and drill down into the survey findings. Then, additional SIEM-captured and stored data becomes far more relevant and useful to the investigative process.

Benefits

- Speed of assessment – triages alerts in minutes to weed out false positives and identify real threats, so you can escalate quickly.
- Reduces the time and resources needed to manually comb through volumes of false alarms and low priority alerts.
- Provides collected intelligence and allows analysts to drill down into identified issues to aid in swift remediation and incident response.
- Advanced detection combines forensic automation and memory analysis techniques tailored to detect malware and suspicious code on compromised systems.
- Agentless scans gather system information and scan volatile memory with no pre-installation of software for seamless deployment and minimal impact on your systems.
- Infocyte HUNT does not rely on the operating system or existing security tools, so results are untainted by any existing compromise.
- API-driven solution works with any platform, and a Partner Integration for Splunk Enterprise Users is available.

GET STARTED

Infocyte HUNT offers organizations a fast and cost-effective solution to triage alerts and combat threats, ensuring the security of your networks. Contact us to learn more.

Infocyte®

CORPORATE HEADQUARTERS
110 E. Houston St. Floor 6
San Antonio, TX 78205
+ 1.844.INFOCYTE (844.463.6298)
sales@infocyte.com

www.infocyte.com
@InfocyteInc