SOLUTION BRIEF

Splunk> +WootCloud: Supercharge your SIEM

You want to arm your Security team with the best information possible

The threats inside the network are just as real as the ones that come from the outside. Compromised, lost, or stolen devices and credentials make insider threats some of the most dangerous for an organization — and buildings are often full of unmanaged and unseen smart devices that are not registered in most configuration management databases (CMDB).

Enriching your SIEM with constantly updating information about every smart device provides unparalleled insight into the full scope of possible network threats — including those devices that may be already compromised.

WootCloud's API connections with Splunk creates a bi-directional data stream harnessing the power of the HyperContext Artificial Intelligence engine to quickly provide your analysts with actionable insight, thus enabling automated security response from the network perimeter to a specific device.

ADD WOOTCLOUD DEVICE CONTEXTUAL INFORMATION FOR SMARTER EVENT ALERTS

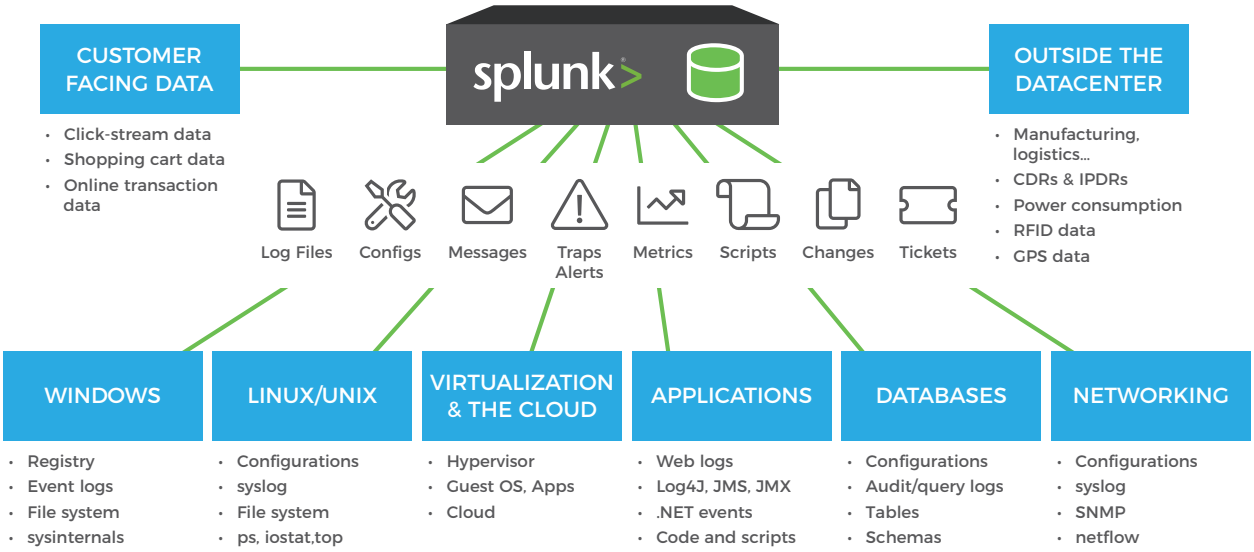
Combining your Splunk SIEM with WootCloud's HyperContext TrueID™ device fingerprinting technology enriches your event alerts with device and site-specific location information.

What's in a SIEM?

Splunk is one of the best SIEM (Security Information and Event Management) products on the market today. A SIEM is a big-data platform that receives information from many sources, enabling you to aggregate, de-duplicate, and correlate the information to identify important streams or facts. Every security operations center (SOC) uses some type of SIEM, such as Splunk. The popularity of Splunk in SOC environments is attributed to the SIEMs flexibility in customization.

Splunk's security operation suite does more than just injest security events from a multitude of network sources via forwarders. The suite also provides advanced threat detection, forensics, and incident management. SOC analysts use Splunk around the clock to view a stream of security events from networks throughout the organization and analyzing data from diverse information sources spanning from within the network perimeter out to roaming endpoints.

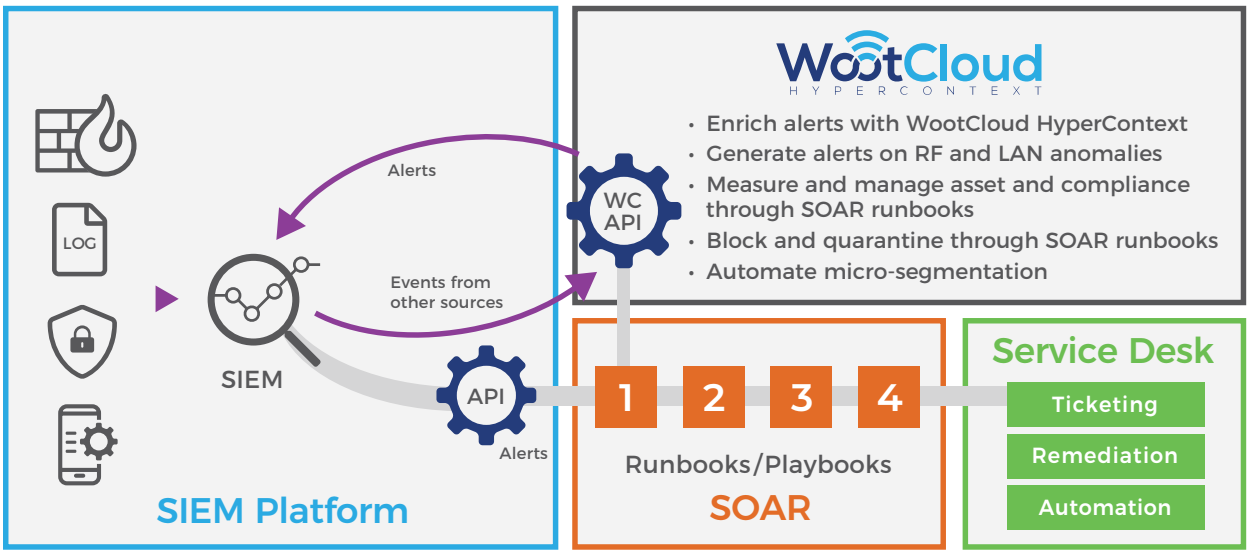
The following local network diagram is a simplified depiction of what can be a complex production network.



Source: **BestITCourseBlog**

The SIEM ingests data from disparate sources and reports all the high-impact events, which results in a veritable flood of information. Where does the SOC analyst start? How do they get from an alert such as "a Cisco ASA reported malware from Source IP xxx.xxx.xxx.xxx attempting to enter Destination IP yyy.yyy.yyy.yyy, action stopped" and identify if any follow-on action or investigation is appropriate? An alert fatigued analyst might be moved to consider the case closed and dismiss it, but is there more? Where did that IP come from, and who does it belong to? Can we see if someone is physically where they do not belong?

With the myriad of network tools reporting security events, the SOC analyst needs additional context to tie events together to make them actionable, and to inform them of an appropriate response, both in the moment and in follow on investigation from a centralized source.



Enter WootCloud's HyperContext™ Information

With event data pouring into your SOC and being sorted by your analysts, you need contextual information that correlates events of interest like the Cisco ASA malware scenario above with NAC and device data to answer the Who, What, and Where contextual information of any smart device event.

HyperContext adds an enriched information stream into your Network Access Control (NAC) solution, checking not only whether a device's MAC or IP address is on the whitelist for network access, but adding new information about the device's physical location, communication interfaces, and other potential vulnerabilities. Further checks can include which operating system is running on the devices, which are the actively communicating applications, or whether the anti-virus software is up to date. All this data is critical for a high-security organization with active asset management lists, a continuous, dynamic, network traffic analysis methodology is the only way to ensure that all devices are known, fingerprinted, and accounted for in standard behavior.

Let's look at what additional information HyperContext could offer the SOC Analyst from the original scenario. "Cisco ASA reported malware from Source IP xxx.xxx.xxx.xxx attempting to enter Destination IP yyy.yyy.yyy.yyy, action stopped." HyperContext can find the MAC address and identification for Source IP, report on the owner, and offer whether the device is patched versus infected with something new. If the device was in the wrong place at the wrong time, or was moved then infected, HyperContext information can pinpoint the owner.

If a device does not comply with the organization's security policies, HyperContext can trigger a Splunk alert on the anomaly, and instruct the NAC to redirect the device to a quarantine zone with limited server access (e.g. only enabling software updates). Solutions like these cannot be manipulated or avoided by malicious actors. WootCloud's asset management and compliance run books track all assets and a noncompliant device's access is denied as security policies are enforced. You can set policies by risk rating, where dangerous devices can be quickly identified and disconnected from vital network resources and data.

All these policies and alerts are sensitive not just to device compliance, but also device physical location and behavior. HyperContext is an important addition to your micro-segmentation strategy,

allowing you to use your SIEM to see events they couldn't sense before. In a security scenario that forbids outside smart devices inside a SOC or datacenter by policy or federal contract, HyperContext can allow Splunk to see that a hidden phone was carried in — and immediately isolate that phone's connections to the rest of the network, even if plugged in via USB.

How HyperContext Connects with Splunk and SOAR

WootCloud's HyperContext has an API integration with Splunk that allows for bi-directional flow of information to and from the SIEM. WootCloud HyperContext imports logs written to the SIEM by other tools like MDM, EDR, Vulnerability assessment, Active Directory, and asset management tools. Since many of these tools write logs to Splunk, this integration with Splunk allows WootCloud HyperContext to collect rich data to correlate without having to directly integrate with any of these tools.

HyperContext can also enrich existing data within Splunk. This device data integrated into Splunk's Indexed security data offers unparalleled information about events and the associated devices, be it smartphone, Audio / Visual hardware, laptop, etc. If it has a MAC address and/or an IP address, WootCloud HyperContext can fingerprint it. HyperContext's API connects to Splunk's Search Head to add context to every Indexed event from any source in the network environment. WootCloud's AI engine generates a rich set of alerts and anomalies based on device behavior and provides zero-day threat detection information which can be routed into the SIEM. Further, HyperContext's unique device risk assessment data can also be fed into the SIEM.

HyperContext's policies are constructed in a cloud-based visual user interface and can be integrated into the runbooks and playbooks of a SOAR (Security Orchestration, Automation and Response) tool to supercharge the SOC and reduce the incident response time. WootCloud HyperContext supercharges SOC operations and helps you get more out of your SIEM and SOAR investments by:

- Enriching alerts with deep WootCloud HyperContext. This provides all the information on the device needed along with the incident which enables the operator to quickly handle threats, reducing incident response times
- Generating alerts on RF and Network Anomalies. WootCloud's HyperContext correlated anomalies surface true threats and thereby reducing alert fatigue
- Measuring and Managing Assets and Compliance — by automating them through SOAR Runbooks. This improves IT security hygiene and helps in incident prevention
- Block & Quarantine through SIEM policies or SOAR Runbooks
- Automating Micro-segmentation

The Benefits of your WootCloud + Splunk Integration

A Smarter Mobile NAC for Automated SIEM Responses

Using NAC in a mobile deployment where workers connect over various wireless networks involves challenges that are not present in a wired LAN. When a user is denied access because of a policy, productive use of the device is lost, which can impact the ability to complete a job or serve a customer. In addition, automated remediation that takes only seconds on a wired connection may take minutes over a slower wireless data connection, bogging down the device. HyperContext integrated with Splunk gives system administrators greater control over whether, when, and how

to remediate the security concern. A lower-grade concern such as out-of-date antivirus signatures or deprecated OS may result in a simple warning to the user but, doesn't enter the SOC, while more serious issues may result in quarantining the device, shutting down access, or escalating to a live Analyst or responder.

Added HyperContext to Every Event in Splunk

Most Network security devices provide the IP address involved in an incident. HyperContext's bi-directional IP query allows Splunk to send an API call to instantly identify a MAC and associated device fingerprint. This device data feeds into Splunk, offering unparalleled information about the offending device. If it has a MAC address and an IP address, WootCloud HyperContext can inform the SIEM with all the salient details, including user behavior. Sequence Detection becomes possible for wireless devices in a way not previously possible with traditional intrusion prevention systems (IPS) or next generation firewalls (NGFWs).

Customized Threat Feed

Unique IoT Device Fingerprint information from your own organization and work sites can be loaded into the SIEM, including information about the device sensing interfaces including Bluetooth and WiFi. With WootCloud HyperContext you can discover your complete Smart / IoT device attack surface, analyze it for potential "easy fixes" including clear-text and default passwords, then create and enforce policies.

Prevent Insider Incidents

WootCloud's HyperContext helps identify changes in user behavior, unexplained logins or movement, or even a change in the user on the device. Imagine a compromised device sending an instant alert to Splunk, which is monitored and responded to by your SOC or MSSP to improve and even automate your response in the event of a breach.

Don't settle for protecting the old IP perimeter. WootCloud and Splunk, when integrated, provide a software-defined perimeter that reaches outside traditional monitoring and controls to bring you true micro-segmentation of your network down to every smart device that enters or exits your environment.

If you'd like a **demo** please contact our team at **sales@wootcloud.com**. You can also enjoy a complimentary smart device assessment for your organization.

About WootCloud

WootCloud is the only smart device security platform that can uncover all types of unmanaged devices by scanning both the radio and network spectrum, and also provide critical context about each device by analyzing over 300 device parameters to generate a unique device identifier & risk rating which generates a device risk score rating. This device score helps organizations discover gaps in their device risk posture and the opportunity to close these gaps. A privately held company, WootCloud is headquartered in San Jose, California, with offices in India and Argentina.

WootCloud HYPERCONTEXT

3031 Tisch Way
Suite 308
San Jose, CA 95128
T: 408-564-4220
sales@wootcloud.com