SOLUTION BRIEF

A

PWN PULSE AND SPLUNK ENTERPRISE

DECREASE THE TIME TO RESOLUTION THROUGH CONTINUOUS DEVICE ASSESSMENT

THE PROBLEM

In an 8-hour shift, a typical analyst on a security team will review between 14 and 28 cases. During that time, the analyst is looks for patterns to find security gaps and indicators of attack. There's only one thing that all of these cases have in common: they start from a device. Increasingly, however, the device in question is transient, doesn't have a company-issued agent or certificate on it, or doesn't take into account the device's connection patterns which describe attack origin.

Like detectives, security analysts have a short amount of time to gain ground-truth on the state of their enterprise. They do this by collecting clues from a variety of sources to help them piece together the whole story during an incident, compromise or breach, but how can they be successful without having a complete picture of the crime scene? Having this context as a SIEM feed drives the time to resolution *down* while extending the value of this investment, helping to resolve the following challenges:

- Identification and classification of new devices across the distributed global enterprise *as they connect* and *when they leave*
- Gain a complete picture of the device & network landscape including shadow networks and rogue devices
- Real-time compliance monitoring through continuous change assessment of device and system posture
- Driving end-to-end incident response and containment

MINIMUM REQUIREMENTS

- Splunk Enterprise or Splunk Cloud
- Pwnie Express Pulse Cloud API
- Pwnie Express Pulse Sensors

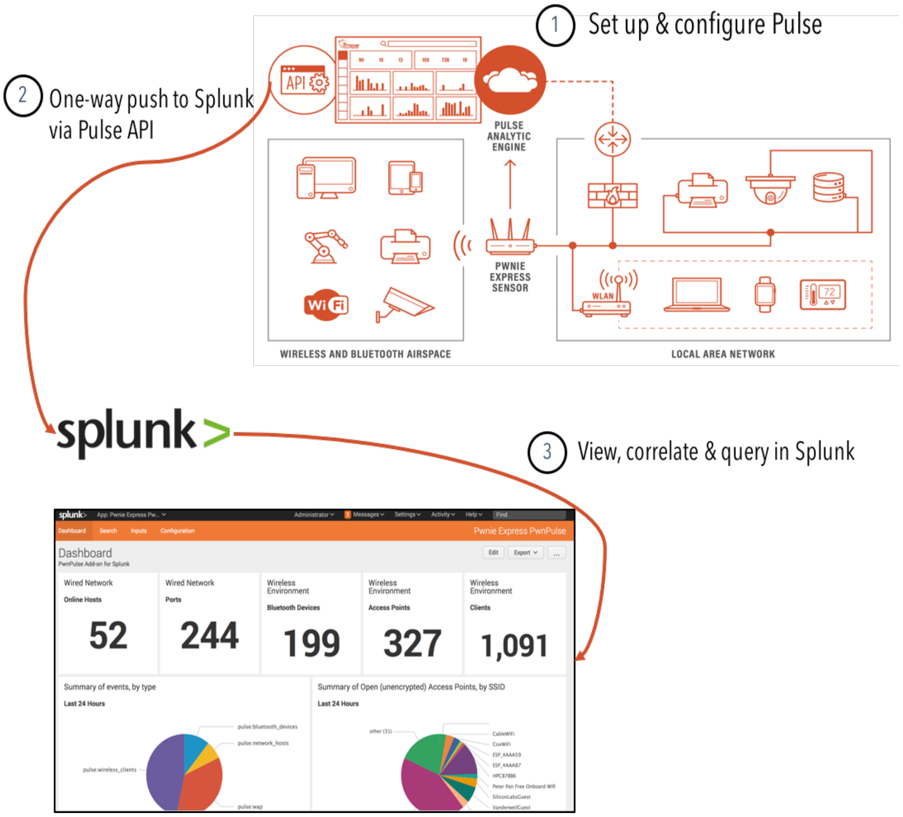
BENEFITS

- **Enables** 100% discovery of all corporate assets and their affiliated networks
- **Gain** full threat context of wired & wireless events impacting your organization
- **Identify** wireless attacks and/or malicious wireless devices impacting your corporate assets & critical systems

THE SOLUTION

The Pwnie Express™ Technology Add-on (TA) for Splunk leverages the device & network visibility provided by the Pulse Analytic Framework™ with Splunk's extensive investigation and visualization capabilities to deliver advanced security reporting and analysis. This TA enables security analysts, administrators, and architects to discover and correlate threats to business systems across all network and security infrastructures from a real-time and historical perspective. Complicated incident analysis that previously consumed days of manual and error-prone data mining can now be automated, saving not only manpower but also enabling key enterprise security resources to focus on critical, time-sensitive investigations.

Pulse provides Splunk users with continuous monitoring capabilities for complete device visibility, regardless of network, and their potential vulnerabilities, misconfigurations, rogue and malicious devices. The Pulse sensors deployed throughout your enterprise collects and classifies device data and system affiliations which is sent as seen to the Pulse Cloud to be analyzed for deviations that put your organization at risk of data breach, denial of service or compliance violation. This continuous monitoring capability delivers a complete and real-time picture of how devices interact with your corporate, guest and production networks. The Pulse Cloud API provides the results of this analysis to your Splunk Enterprise instance. This TA is available at no charge on Splunkbase. By leveraging Pwnie Express, Splunk Operational Intelligence users can slash the time to insight and take action on their findings.


1 Set up & configure Pulse
2 One-way push to Splunk via Pulse API
API
PULSE ANALYTIC ENGINE
PWNIE EXPRESS SENSOR
WLAN
72
WIRELESS AND BLUETOOTH AIRSPACE
LOCAL AREA NETWORK
splunk>
3 View, correlate & query in Splunk
Dashboard
Pwnie Express PwnPulse
Wired Network Online Hosts 52
Wired Network Ports 244
Wireless Environment Bluetooth Devices 199
Wireless Environment Access Points 327
Wireless Environment Clients 1,091
Summary of events, by type
Last 24 Hours
Summary of Open (unencrypted) Access Points, by SSID
Last 24 Hours

HOW IT WORKS

1. Splunk Enterprise utilizes the Pulse Cloud REST API to import historical Pulse data into Splunk.

2. As new devices (wireless clients/APs, network hosts, Bluetooth), threats, and alerts are identified, this information is pulled into Splunk at user-configurable time intervals

3. Splunk users can view & generate reports of this data from the out-of-the –box dashboard or build queries and correlations of the data against other Splunk inputs. secure and profitable. Visit splunk.com to learn more.

ABOUT SPLUNK

Splunk Inc. is the market-leading platform that powers Operational Intelligence. We pioneer innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government and education more efficient,

ABOUT PWNIE EXPRESS

Pwnie Express closes the IoT security gap exposed by the deployment of IoT in the enterprise. By continuously identifying and assessing all devices and IoT systems, our IoT security platform prevents IoT based threats from disrupting business operations. All without the need for agents, or changes to network infrastructure.

For more information visit: http://www.pwnieexpress.com/

Contact Us: Please email us at sales@pwnieexpress.com