THE BEST WAY TO CATCH A THIEF

Patrick Bedwell, Vice President, Product Marketing

AlienVault Vision

- **Accelerating and simplifying threat detection and incident response for IT teams with limited resources, on day one**

- **Enable organizations of all sizes to benefit from the power of crowd-sourced threat intelligence & unified security**

Understanding Thieves

Data thieves, resource thieves & customer thieves

- Botnets
- DDoS
- Spam-marketing
- Collecting sensitive data (financial, personal, corporate)
- Identity theft
- Fraud
- The dark side

Detection: Initial signs and symptoms

- Performance degradation
- Endpoint detection
- Network detection
- Honeypot

Detecting on the endpoint

- Antivirus
- Rootkit installations
- Unexpected popups
- Changes to Windows Hosts file
- Modified DNS servers

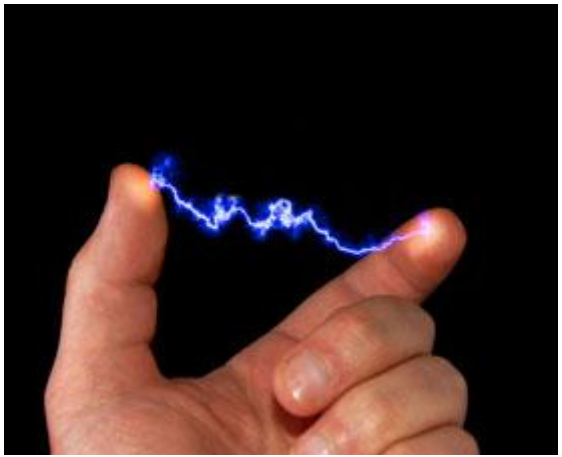
Detecting on the network

- Linking to established C&C servers for instructions
- Generating IRC traffic via a specific range of ports
- Generating SMTP traffic / emails
- Generating simultaneous identical DNS requests
- Deviation from ‘normal’

Best Practices: Host vs. Network Detection

#	Best practice
1	Deploy both host- and network-based detection tools, neither will find every instance every time by themselves.
2	Ensure your host-based IDS or an anti-malware solution that is capable of detecting the common endpoint signs of botnet infection and is frequently updated with the last known C&C server information. Not catching the easy, obvious infections can be used as a sign of negligence.
3	Implement a honeypot (or several) if you are protecting reasonably valuable information, have a lot of brand equity in your company's name, or make for a particularly juicy target for a lawsuit by a victim of a botnet-based attack originating from your network.

Static vs. Behavioral Detection



Best Practices: Static vs. Behavioral Analysis Detection

#	Best practice
1	Use static analysis at a minimum, but organizations should focus botnet detection on behavioral analysis if at all possible, as it is much more effective.
2	Talk to in-house and external experts about newer techniques such as P2P botnet detection techniques.
3	Ensure the rules for your behavioral, network-based botnet detection systems take into account less common systems.

The future of threat detection

- Attackers are evolving, but so are tools
- Know your assets and what normal looks like
- Analyze the nature and impact of new threats
- Directly quarantine, limit or eradicate local bots

AlienVault Approach: Unified Security Management

Unified Security Management Platform

- Accelerates and simplifies threat detection and incident response for IT teams with limited resources, on day one

AlienVault Labs Threat Intelligence

- Identifies the most significant threats targeting your network and provides context-specific remediation guidance

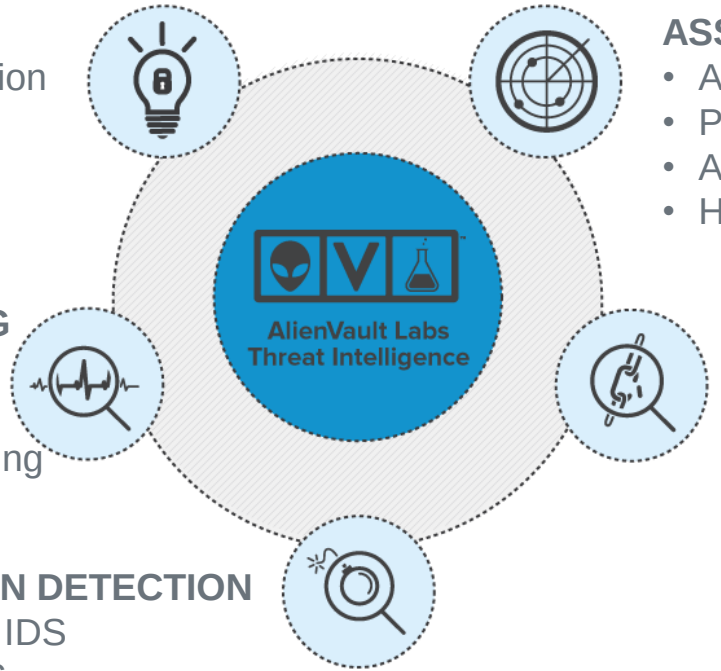
Open Threat Exchange

- The world's largest repository of crowd-sourced threat data, provides a continuous view of real-time threats

USM Platform

SIEM
- SIEM Event Correlation
- Incident Response

ASSET DISCOVERY
- Active Network Scanning
- Passive Network Scanning
- Asset Inventory
- Host-based Software Inventory



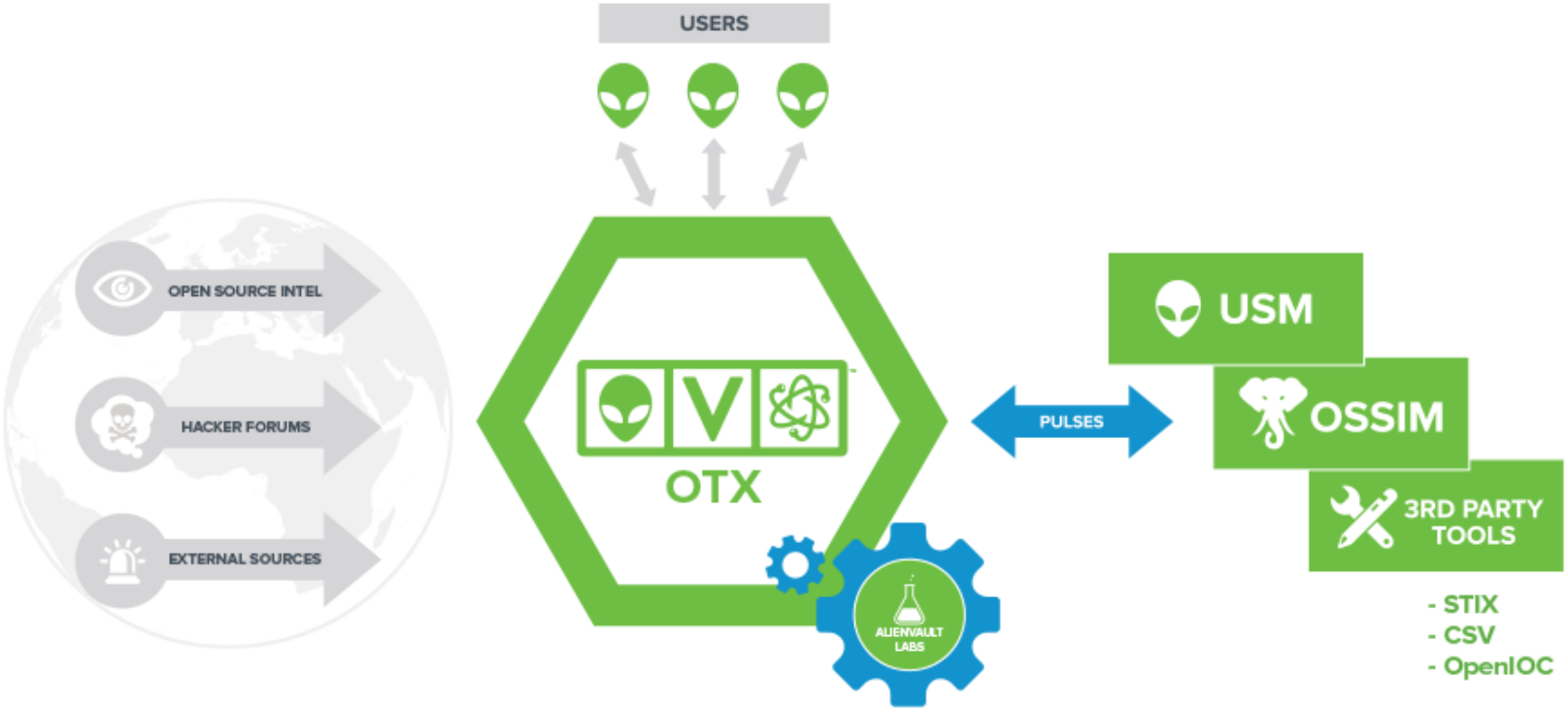
BEHAVIORAL MONITORING
- Log Collection
- Netflow Analysis
- Service Availability Monitoring

VULNERABILITY ASSESSMENT
- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning

INTRUSION DETECTION
- Network IDS
- Host IDS
- File Integrity Monitoring

Built-In, Essential Security Capabilities

Open Threat Exchange



Now for some Questions..

Next steps…

Test Drive AlienVault USM
https://www.alienvault.com/products/try-usm

Join the Open Threat Exchange (OTX)
https://www.alienvault.com/open-threat-exchange

CONTACT US


888.613.6023


ALIENVAULT.COM


HELLO@ALIENVAULT.COM