ALIEN VAULT™

Security Operations Center (SOC) Essentials for the SME

INTRODUCTIONS

Meet today’s presenters

Javvad Malik
Senior Analyst, 451 Research
451 Research

Patrick Bedwell
VP, Product Marketing
AlienVault

Tom D’Aquino
Director, Technical Sales
AlienVault

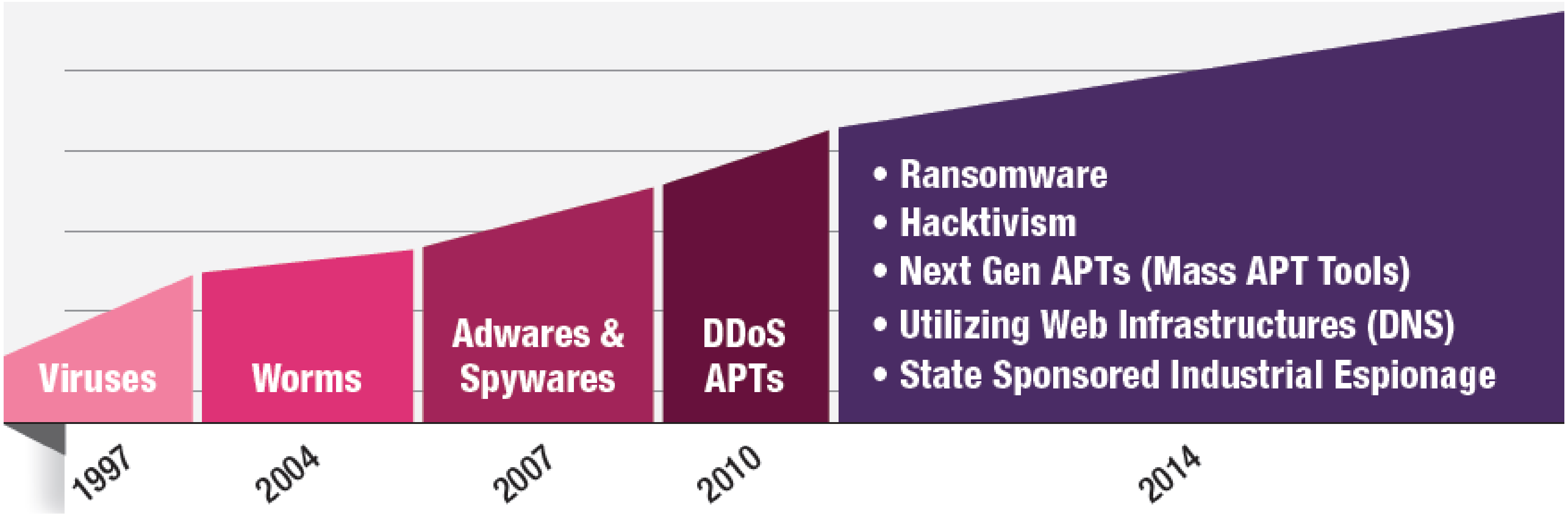
@AlienVault

AGENDA

- Developments in the threat landscape are driving a shift from preventative to detective controls
- Essential security controls needed to defend against modern threats
- Fundamentals for evaluating a security approach that will work for you
- How a unified approach to security visibility can help
- Demo of AlienVault Unified Security Management
- Q&A

Developments in the Threat Landscape Are Driving a Shift from Preventative to Detective Controls

EXAMPLE OF TRENDS

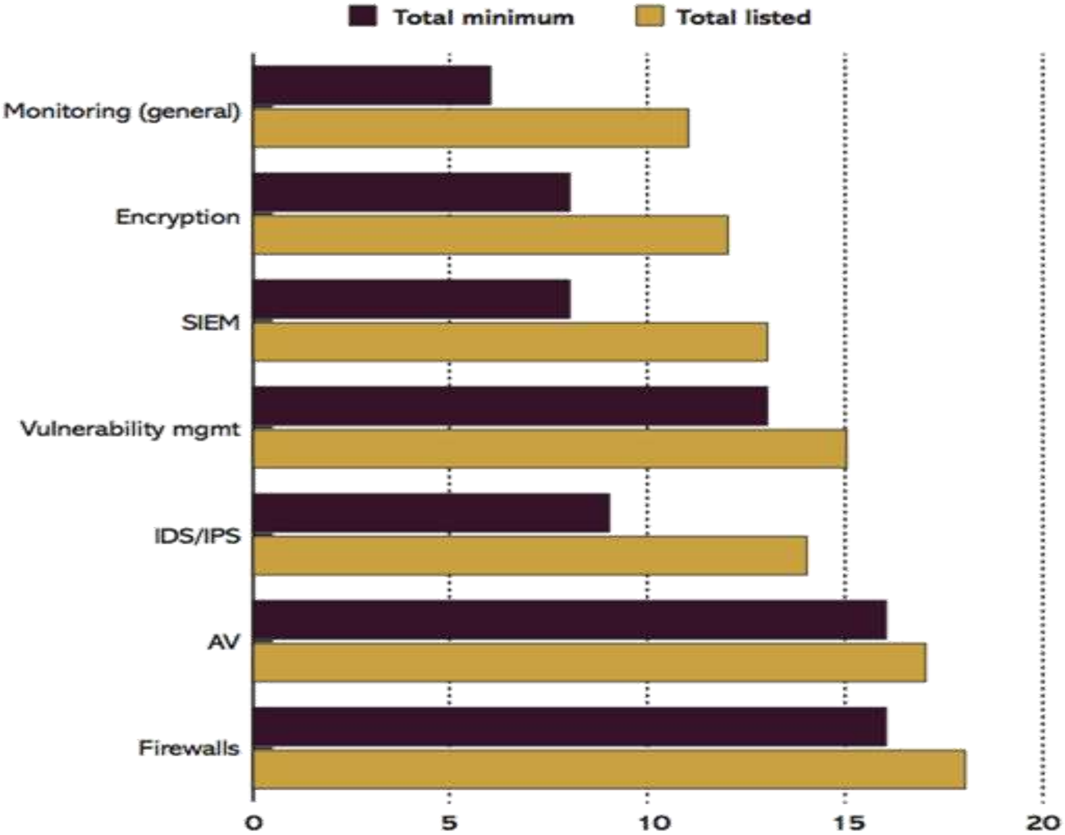


Source: Check Point Security Report - 2014

@AlienVault

Essential Security Controls Needed to Defend Against Modern Threats

MOST RECOMMENDED SECURITY TECHNOLOGIES

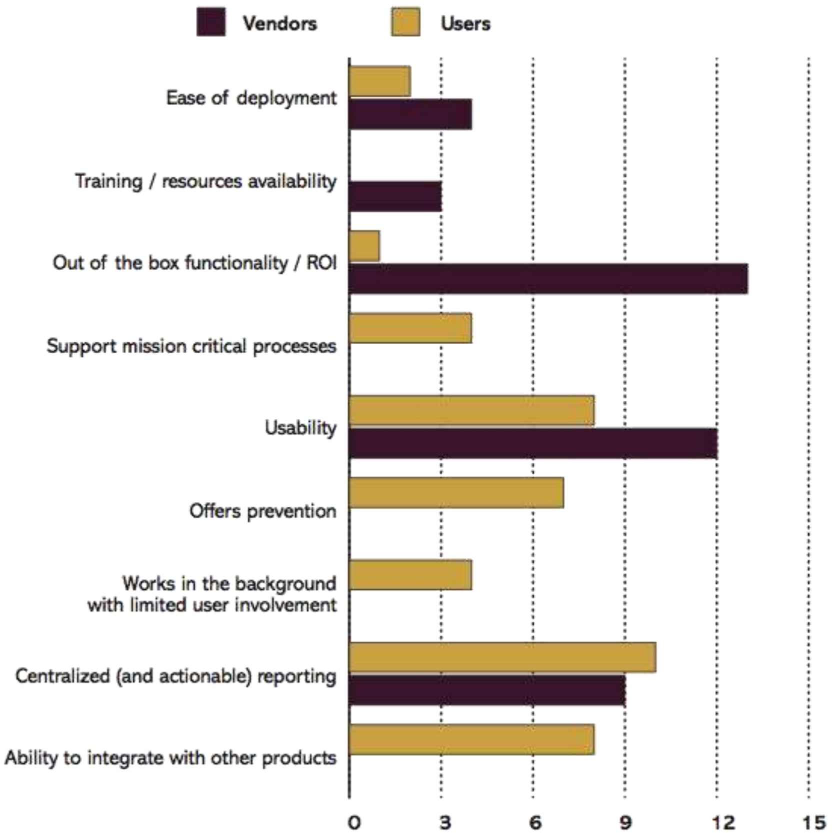


Source: 451 Research

@AlienVault

MOST IMPORTANT FEATURES OF SECURITY PRODUCTS

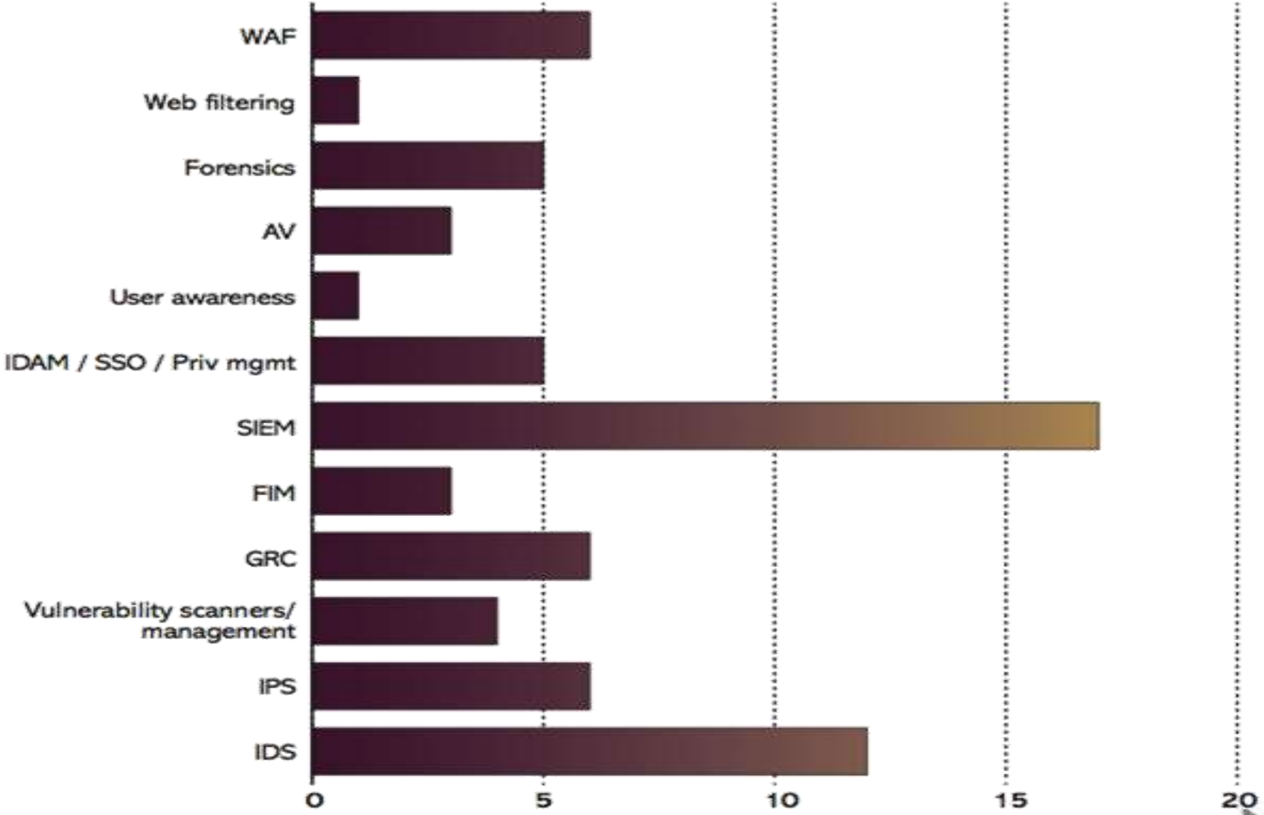
WHAT MAKES A GOOD SECURITY PRODUCT?



Source: 451 Research

@AlienVault

SHELFWARE BY PRODUCT TYPE

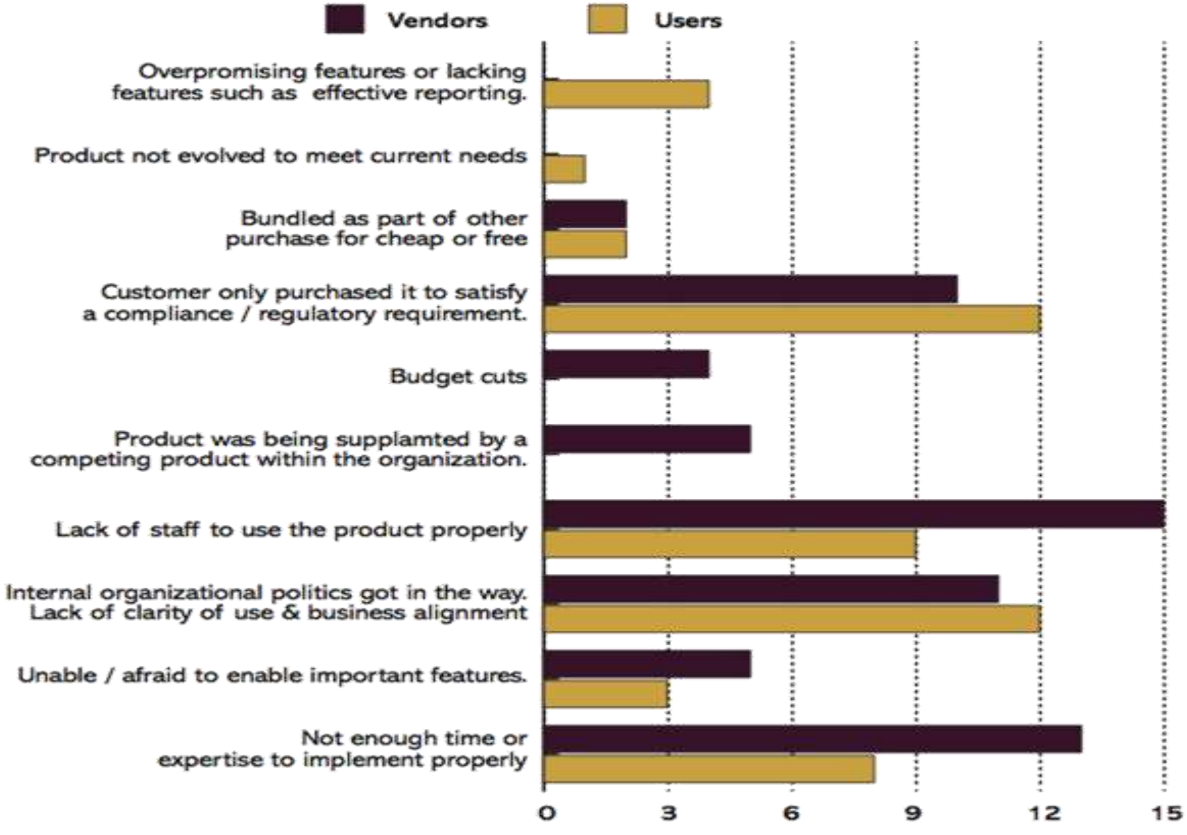


Source: 451 Research

@AlienVault

TOP REASONS WHY PRODUCTS BECOME SHELFWARE

WHY ARE PRODUCTS UNDERUTILIZED OR NOT USED AT ALL?



Source: 451 Research

@AlienVault

Fundamentals for Evaluating a Security Approach that Will Work for You

QUESTIONS TO ASK

- Why?
  - Being clear on the security objective this product will meet.
- Stakeholder support?
  - More relevant to larger companies, but lack of stakeholder support caused many projects to fail.
- Deployment plan?
  - Have a deployment plan taking into account resources needed to deploy, rollback plans & impact on production systems.
- Product capabilities?
  - Don’t just take someone’s word for what their product can do. Verify the product capabilities – get a trial version or POC.

QUESTIONS TO ASK - PART 2

- Decommissioning plan?
  - Don’t complicate your environment by adding technology on top of technology.
  - Decommission older security technology if you’re implementing new one.

- Negotiate?
  - On price, training, features etc. If you get stuck using a product will the vendor be there to help you?
- Do your homework?
  - Ask peers what their experiences have been in using certain technologies, ask analysts

SO MANY SECURITY TECHNOLOGIES TO CHOOSE FROM

Given the 10 most recommended technologies and the pricing range, an organization could expect to spend anywhere from $225,000 to $1.46m in its first year, including technology and staff.

*Source: **The Real Cost of Security**, 451 Research, April 2013*

Factor in:

- ✓ Initial Licensing Costs
- ✓ Implementation / Optimization Costs
- ✓ Ongoing Management Costs
- ✓ Renewal Costs
- ✓ Integration of all the security technologies
- ✓ Training of personnel/incoming personnel

@AlienVault

UNIFIED SECURITY MANAGEMENT

CLOSING THE GAPS

- Deployment & Use
- Awareness
- Intelligence
- Action

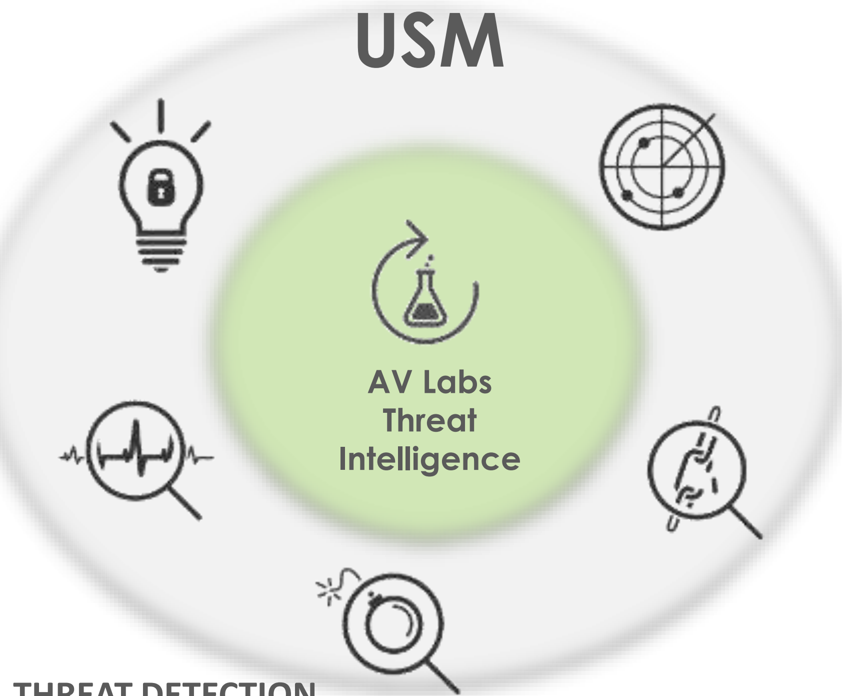
USM PRODUCT CAPABILITIES

SECURITY INTELLIGENCE

- SIEM Event Correlation
- Incident Response

BEHAVIORAL MONITORING

- Log Collection
- NetFlow Analysis
- Service Availability Monitoring



THREAT DETECTION

- Network IDS
- Host IDS
- Wireless IDS
- File Integrity Monitoring

ASSET DISCOVERY

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

VULNERABILITY ASSESSMENT

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning

@AlienVault

UNIFIED SECURITY MANAGEMENT

COMPLETE. SIMPLE. AFFORDABLE.

AlienVault USM provides the five essential security capabilities in one, pre-integrated platform

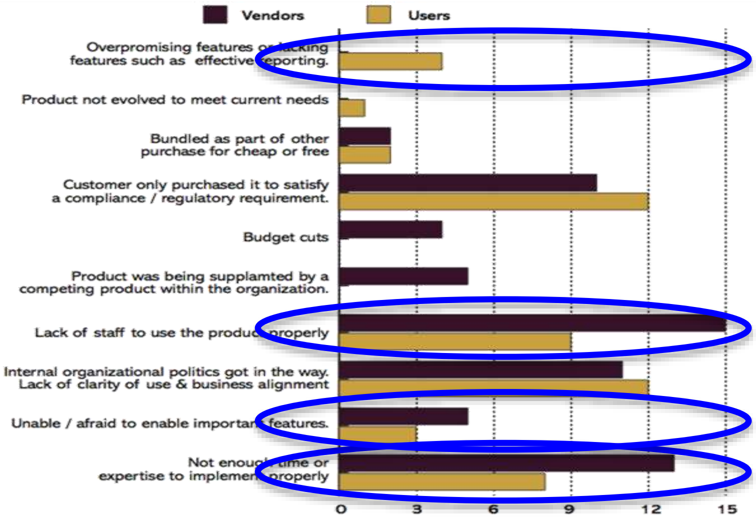
- Unified Security Management (USM) Platform
- AlienVault Labs Threat Intelligence
- AlienVault Open Threat Exchange

Delivery Options:
Hardware, **Virtual**, or **Cloud**-based appliances
Open-Source version (OSSIM) also available

WHAT UNIFIED SECURITY MANAGEMENT OFFERS

- Out of the box functionality
  - Hours, not weeks or months
- Ease of deployment / Ease of use
  - Accessibility to features and information
- Actionable information
  - Proven, effective guidance
- Single pane of glass for consolidated view
  - One admin, not many

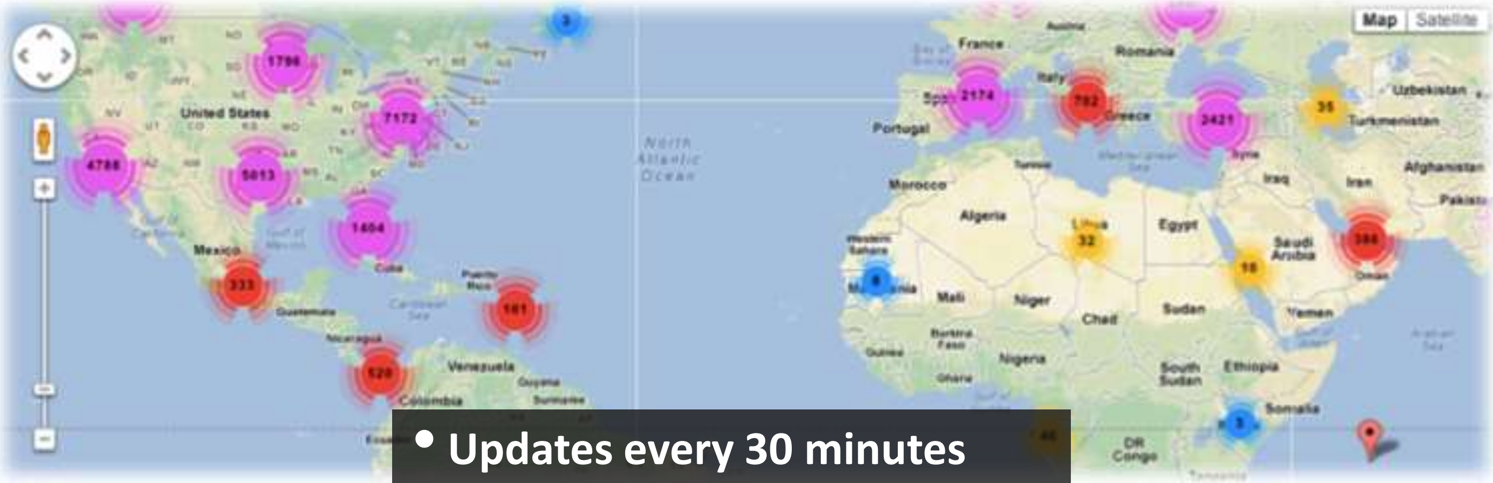
Top Reasons Why
Products Become Shelfware



Source: 451 Research

ALIENVAULT LABS THREAT INTELLIGENCE

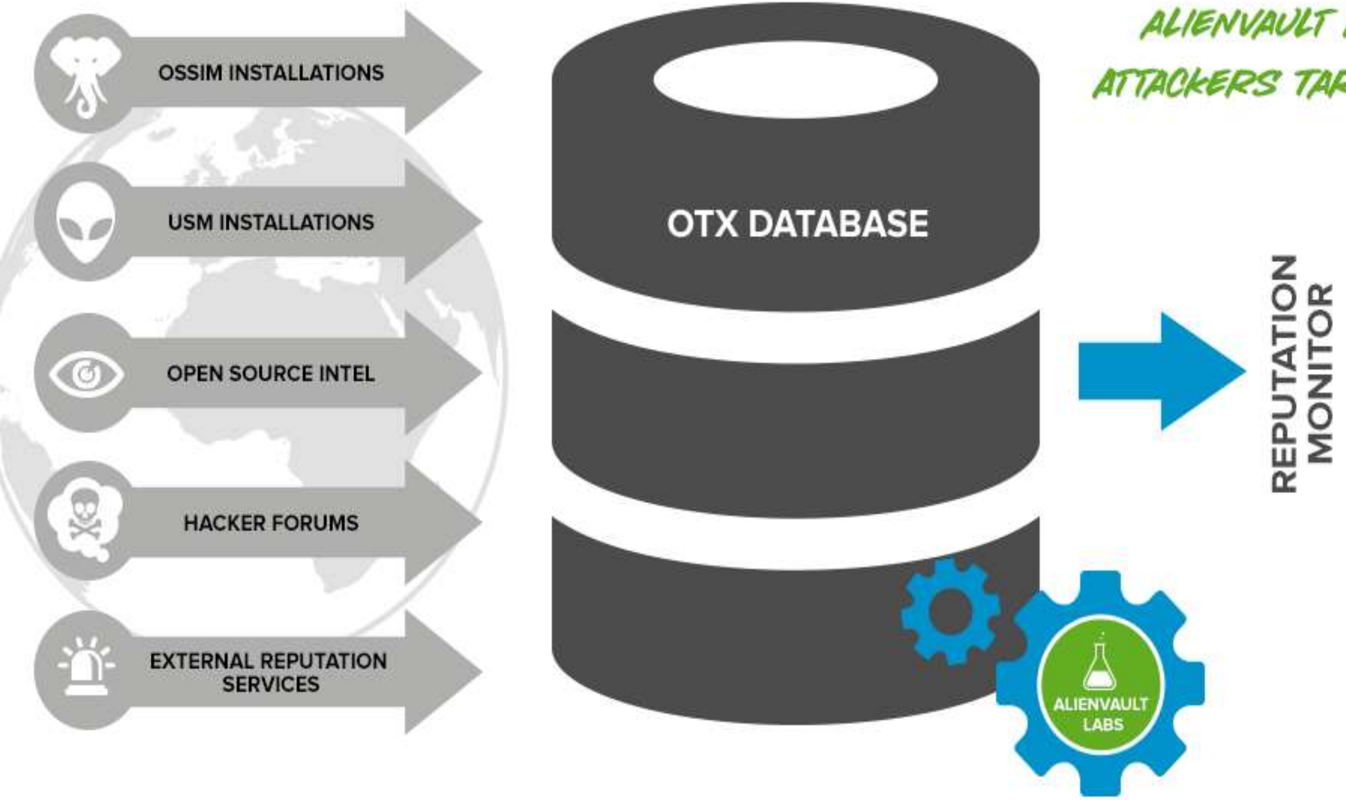
COORDINATED ANALYSIS, ACTIONABLE GUIDANCE



- Updates every 30 minutes
- 200-350,000 IP validated daily
- 8,000 Collection points
- 140 Countries

@AlienVault

THREAT INTELLIGENCE POWERED BY OPEN COLLABORATION



- Diverse set of data & devices
- 8,000 collection points
- 140+ countries
- 500,000 malware samples analyzed daily
- 1500+ Event Correlation Rules
- 5 Event Attack Types

@AlienVault

WE’VE GOT YOUR BACK

- Weekly updates that cover all your coordinated rule sets:
  - Network IDS signatures
  - Host IDS signatures
  - Asset discovery and inventory database updates
  - Vulnerability database updates
  - Event correlation rules
  - Report modules and templates
  - Incident response templates / “how to” guidance for each alarm
  - Plug-ins to accommodate new data sources
- Fueled by the collective power of the AlienVault’s Open Threat Exchange (OTX)

DEMO AND Q&A

Test Drive AlienVault USM

- Download a Free 30-Day Trial

  http://www.alienvault.com/free-trial

- Try our Interactive Demo Site

  http://www.alienvault.com/live-demo-site

Detecting Threats Has Never Been Easier (or Faster)

Introducing AlienVault USM v4.6

Within minutes, you'll be able to detect:

- ✓ Malware infections
- ✓ Command and control activity
- ✓ Known Vulnerability (CVE) Exploits
- ✓ Bruteforce Attacks
- ✓ SQL Injection & XSS Attacks

@AlienVault