数据驱动安全

2015 中国互联网安全大会
China Internet Security Conference

Security Innovation & Startup

OPEN THREAT EXCHANGE (OTX): THE HISTORY AND FUTURE OF OPEN THREAT INTELLIGENCE COMMUNITY

PRESENTATION OVERVIEW

- A very quick overview of AlienVault
- Our Open approach to crowd sourced threat intelligence
- The OTX Platform and Data

ABOUT ALIENVAULT

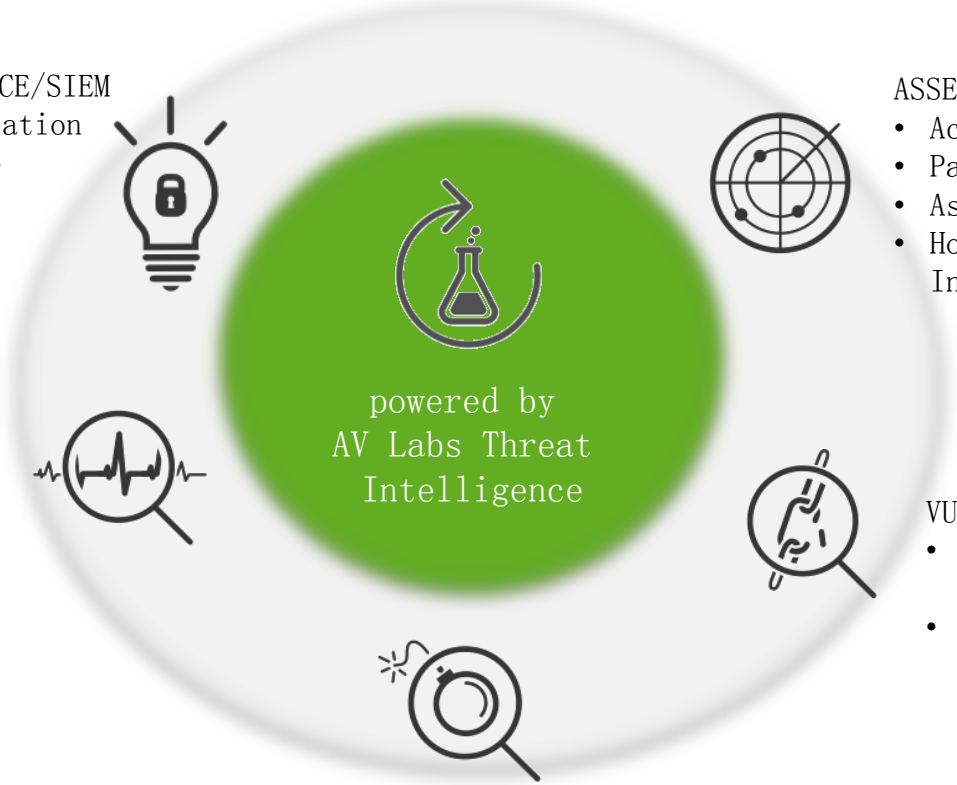
AlienVault is the leading provider of Unified Security Management (USM) and crowd-sourced threat intelligence technology required to detect and act on today's advanced cyber threats

USM PLATFORM

5 CRITICAL CAPABILITIES

SECURITY INTELLIGENCE/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

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

THE ATTACKER'S ADVANTAGE

- They only need to be successful once
- Determined, skilled and often funded adversaries
- Custom malware, 0days, multiple attack vectors, social engineering
- Persistent

IMPORTANCE OF SHARING

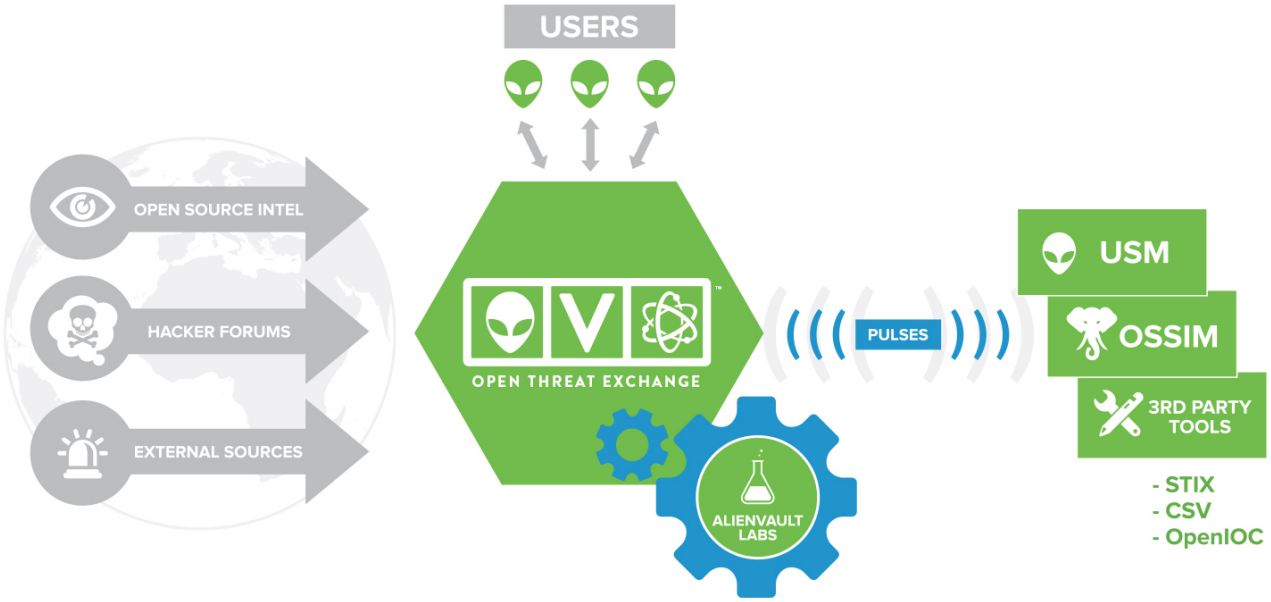
"In the case of threat-intelligence sharing, the adversary has only to mess up once – being detected – and all the defenders will know about it. It's in our best interest, as an industry, to keep the odds ever in our favor."

-- Wendy Nather, 451 Group, 2014 Threat Intelligence Report

- Helps you to achieve a preventative response to changes in the threat landscape by learning how attackers are targeting others
- Armed with real-time, detailed security event information, you can update your defenses to avoid becoming a victim
- The right solution will allow you to automatically share anonymized threat information

OPEN THREAT EXCHANGE OTX

- Launched in 2012 - The world's largest open threat sharing and analysis network
- Supports more than 26,000 participants in over 140 countries contributing more than 1 million threat indicators daily
- Provides access to real-time, detailed information about threats and incidents around the world

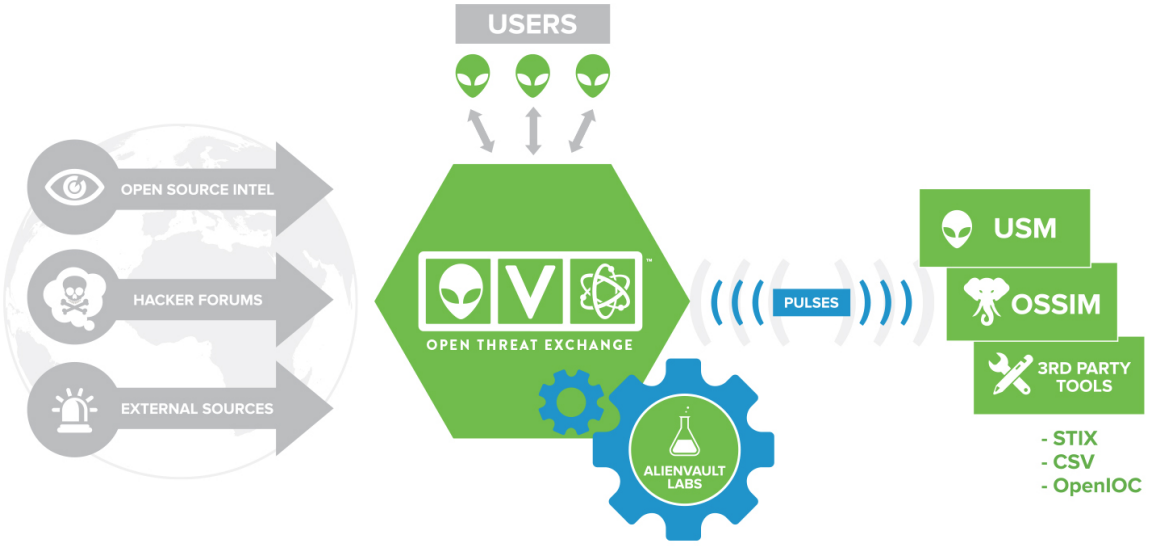


COLLABORATION
POWERING OTX

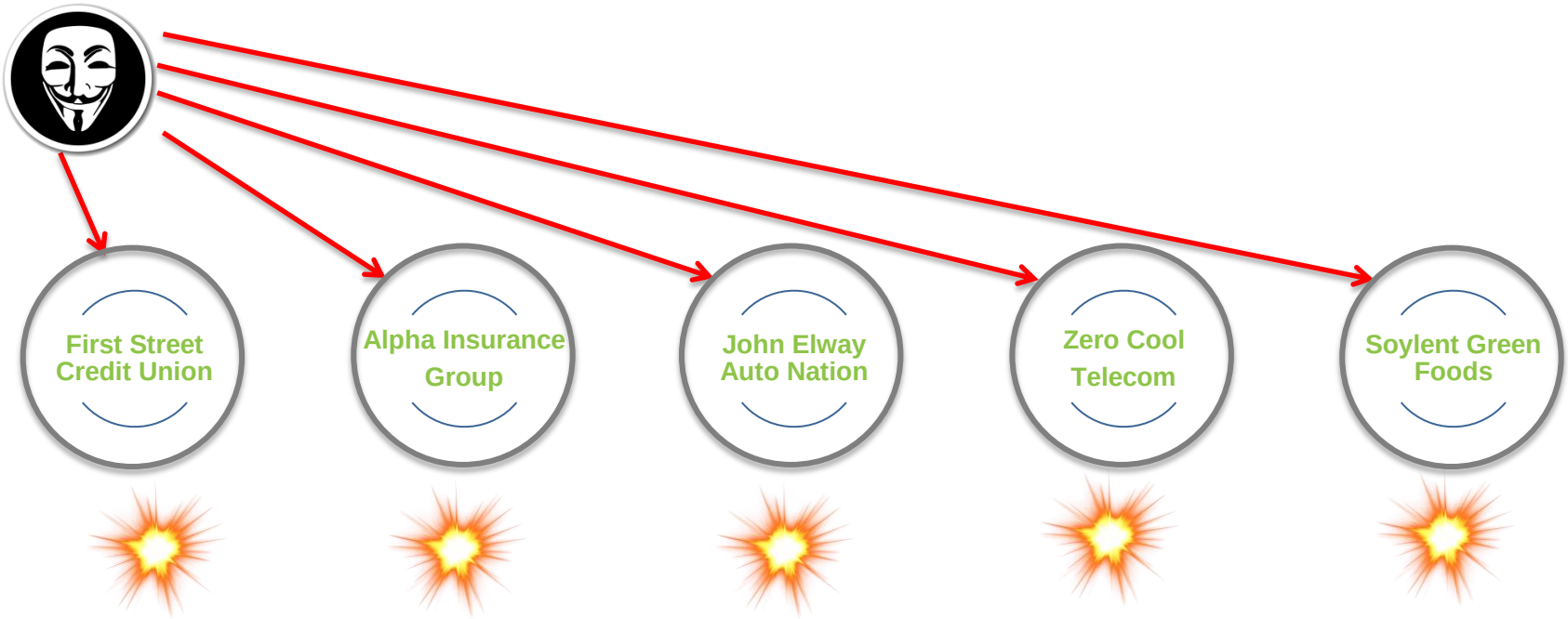
Collaborate
Openly research and collaborate on emerging threats.

Defend
Integrate with AlienVault USM or Export IoCs to any security produc

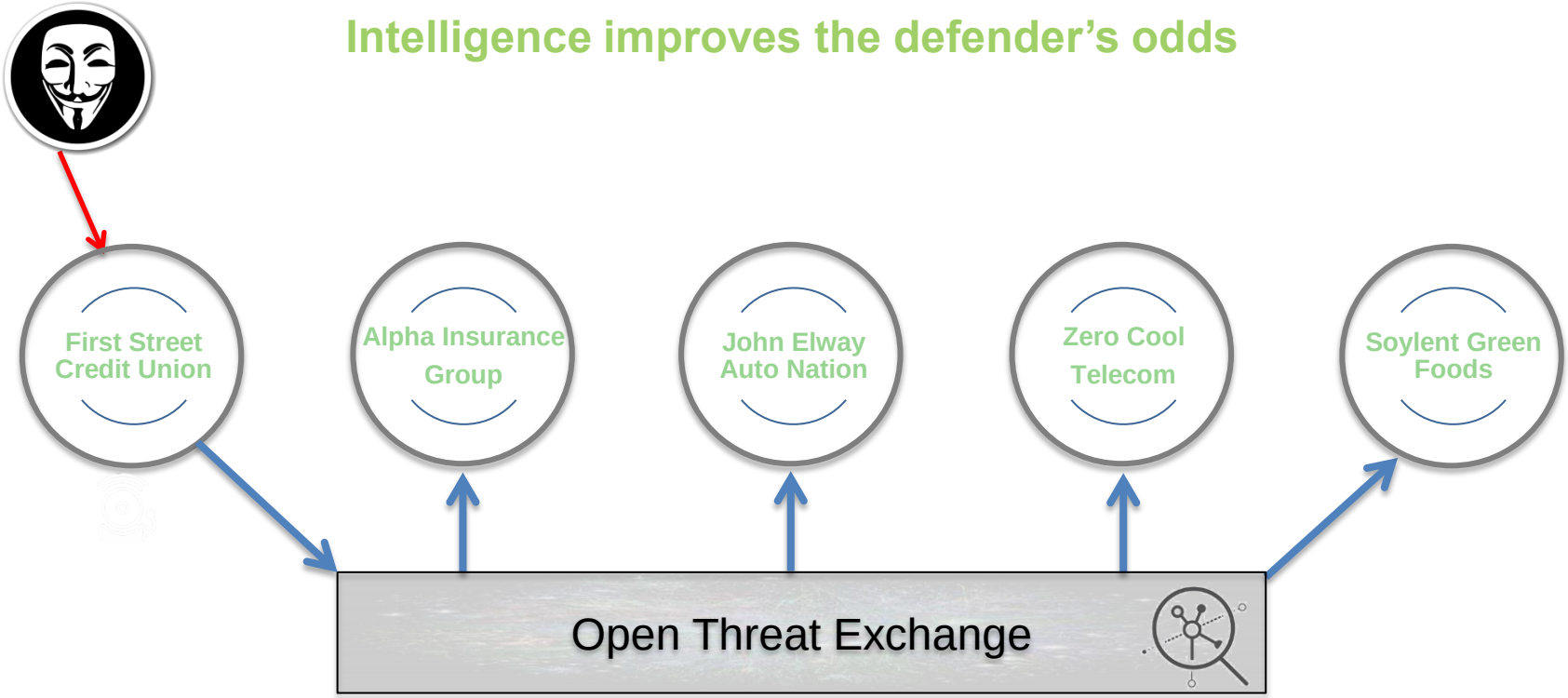
Learn
Extract, validate and investigate data from logs, blogs, articles an reports



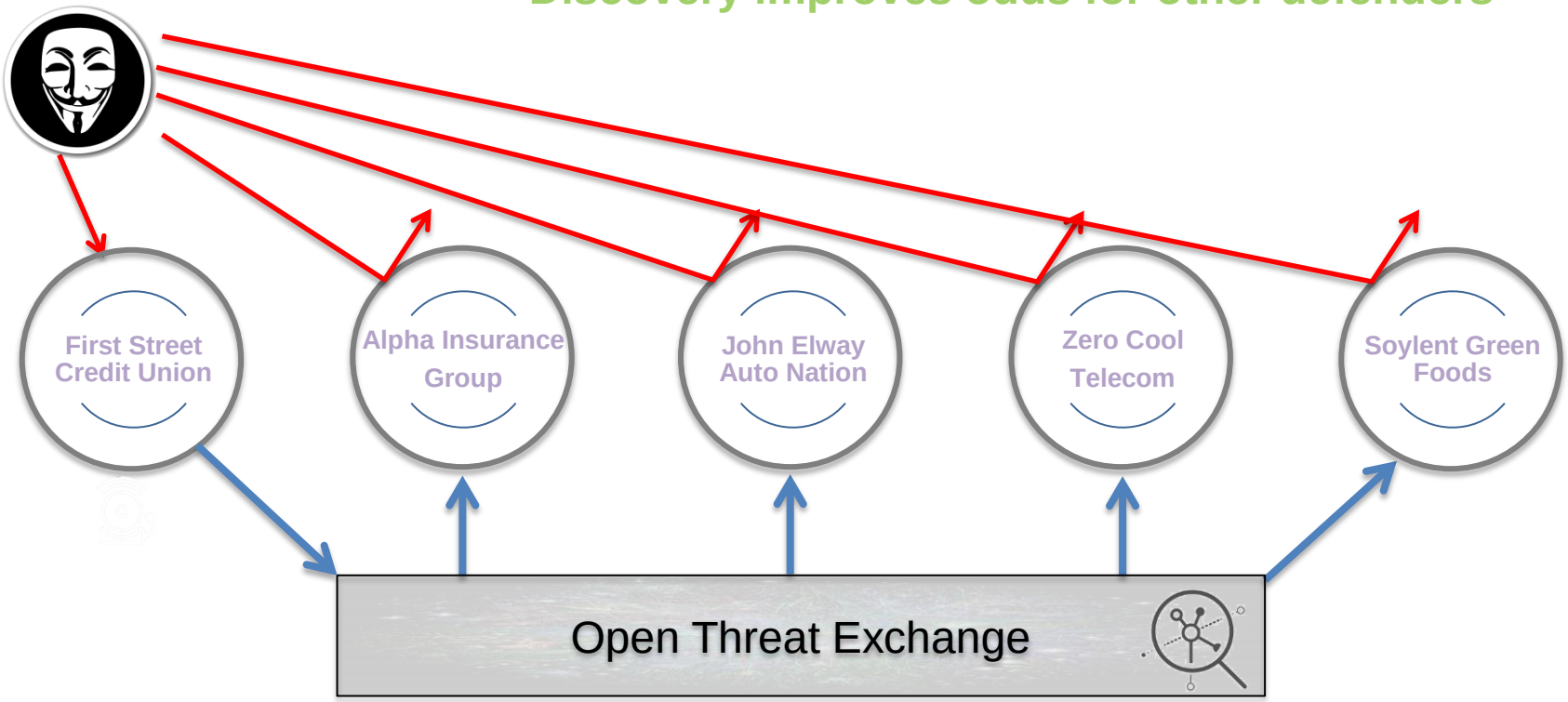
THE DEFENDER'S DILEMMA



THREAT INTELLIGENCE APPLIED



THREAT INTELLIGENCE APPLIED



OTX 1.0
IP REPUTATION DATA

- Updates provided every 30 minutes
- 200,000-350,000 validated malicious IP's at any point

Malware Domain
Distributing malware or hosting exploit code

Malware IP
Instrumental in malware, including malicious redirection

Command and Control
Sending command and control instructions to malware or a botnet

Scanning Host
Observed repeatedly scanning or probing remote systems

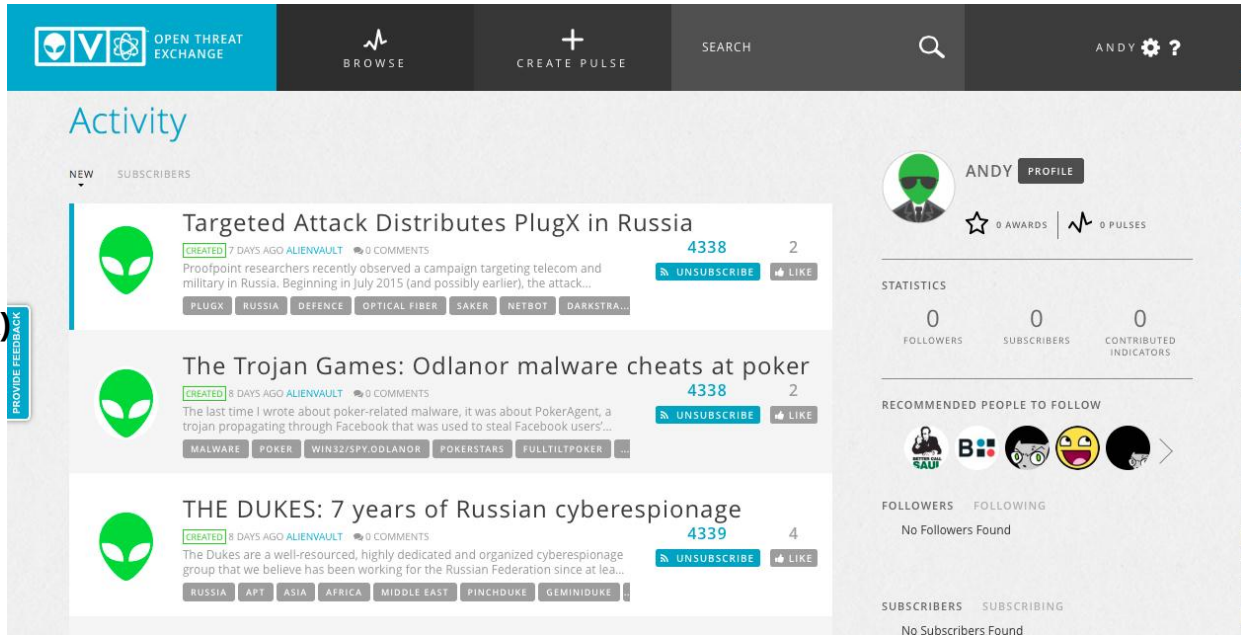
APT
Observed to be actively involved in an APT campaign

Spamming Host
Actively propagating or instrumental in the distribution of spam

Malicious Host
Engaged in malicious but uncharacterized activity

OTX 2.0: “PULSES”
CROWD SOURCED THREAT RESEARCH

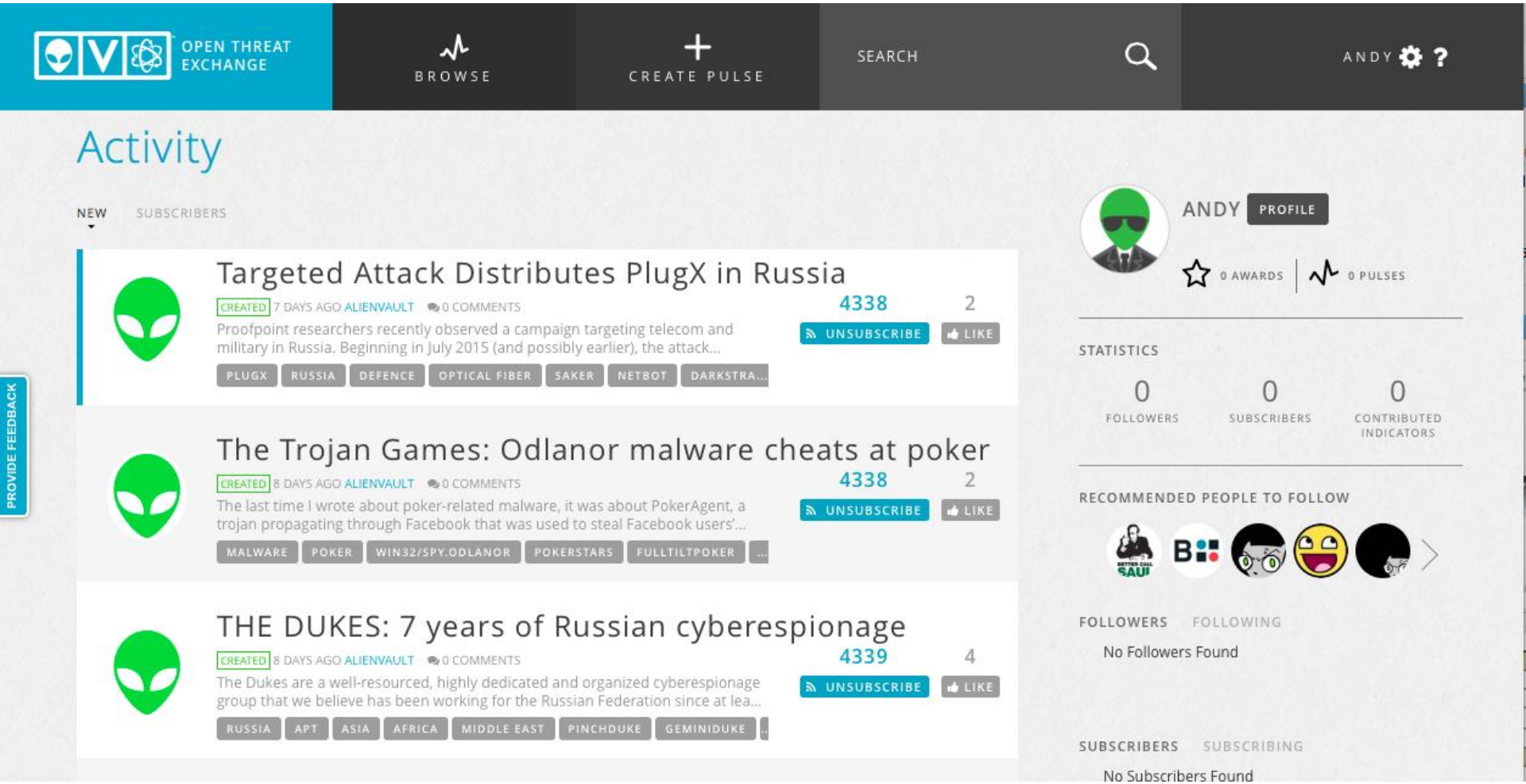
- **THE FACE OF OTX – SOCIAL INTERFACE TO COLLABORATIVELY DEVELOP & SHARE THREAT INTELLIGENCE IN REAL-TIME**
- **CREATE, ENHANCE OR CONSUME “PULSES” – SHORT MULTIVARIATE ANALYSIS OF THREAT INDICATORS**
- **EXPORT INDICATORS OF COMPROMISE INTO SECURITY TOOLS (OPENIOC, STIX) AND AUTOMATICALLY CONSUME IN ALIENVAULT PRODUCTS**
- INTEGRATE & EXPLORE THROUGH AN OPEN API
- **STRENGTHEN DEFENSES AND HELP OTHERS DO THE SAME**



INVESTIGATING THREATS

- Pulse: *ONE* data construct for ALL types of threats
  (Data breach, Botnet, APT Campaign, etc.)
- Defined by *Indicators of Compromise or IoCs*:
  (md5, IPv4s, URLs, hostnames, etc.)
- Explore attack vectors and threat geolocation information
- Share and comment on Pulses and IoCs

OTX HOME PAGE



DETAILED INTELLIGENCE

The Trojan Games: Odlanor malware cheats at poker

8 DAYS AGO ALIENVAULT DOWNLOAD

0	4	Green		4338	2
RELATED PULSES	INDICATORS	TLP CLASSIFICATION	PUBLIC	UNSUBSCRIBE	LIKE

TAGS: MALWARE POKER WIN32/SPY.ODLANOR POKERSTARS FULLTILTPOKER ESET

REFERENCE: http://www.welivesecurity.com/2015/09/17/the-trojan-games-odlanor-malware-cheats-at-poker/ COPY

The last time I wrote about poker-related malware, it was about PokerAgent, a trojan propagating through Facebook that was used to steal Facebook users' logon credentials, credit card information and the level of Zynga poker credit. Today, we're bringing you news about Win32/Spy.Odlanor, which is used by its malware operator to cheat in online poker by peeking at the cards of infected opponents. It specifically targets two of the largest online poker sites: PokerStars and Full Tilt Poker.

Indicators of Compromise

Show 10 entries Search:

TYPE	INDICATOR
domain	bbsystems.info
FileHash-SHA1	510acecee856abc3e1804f63743ce4a9de4f632e

ADDITIONAL DETAIL

Indicator of Compromise: 510acecee856abc3e1804f63743ce4a9de4f632e

A file hash is an indicator of compromise commonly used in identifying malware such as viruses, trojans, ransomware, or other types of malicious software.

GENERAL DETAILS | 1 RELATED PULSES | ANALYSIS

PROVIDE FEEDBACK

Type

Sha1

File Type

FILE TYPE: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows

MIME-TYPE: application/octet-stream

SIZE: 520704

FILE CLASSIFICATION: PEXE

ANALYSIS DATE: May. 6, 2015, 5:48 am

Analyzed: File

MD5: ce19c30ffda76cd63a88eeb8af0340f0

SHA256: da6a2e97bbc433ae36714da1aa6eaa3b01970b50e65ccb5735dc32dca006ff8d

SHA1: 510acecee856abc3e1804f63743ce4a9de4f632e

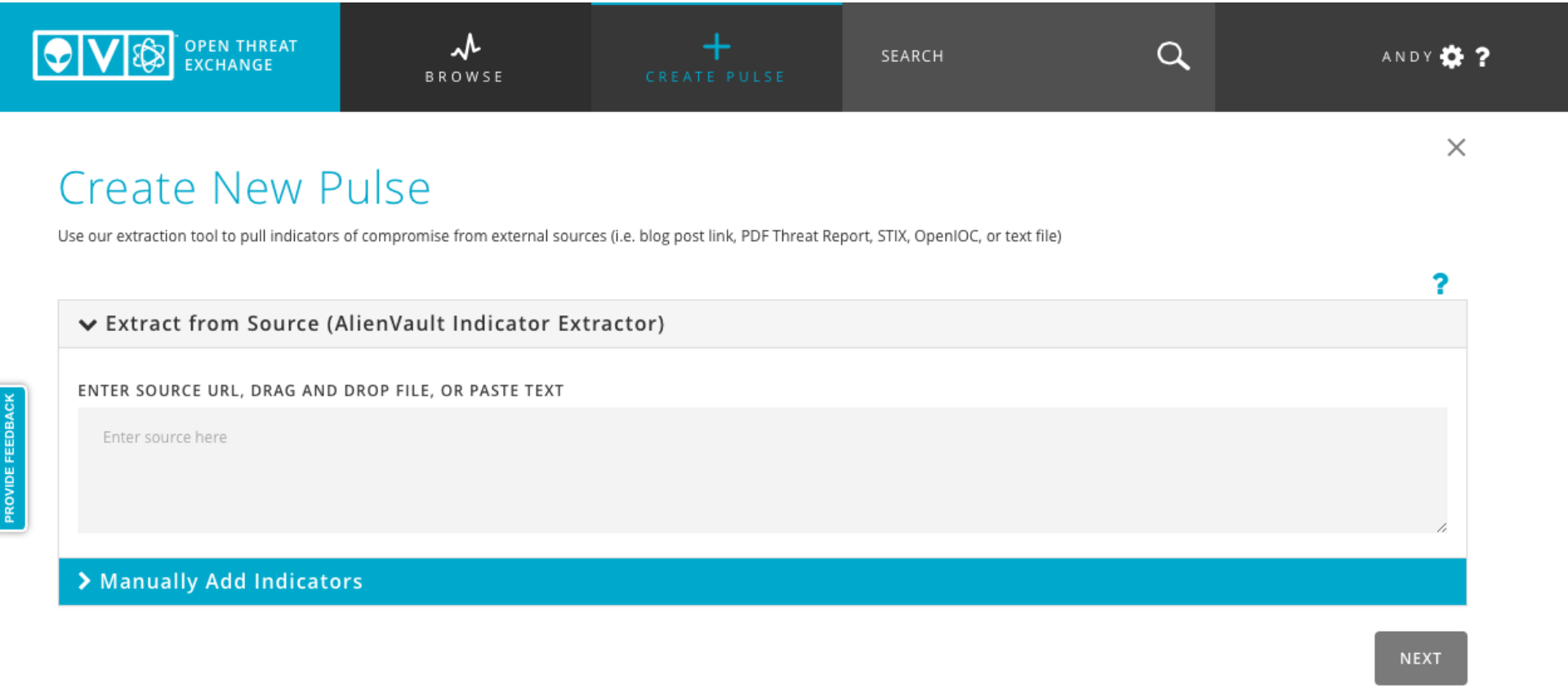
IMPHASH: 045e87923a29e07468a3e464d4fb1ffd

PEHASH: 2008dd5046a921ac23d6870149e59616d9d2b2c5

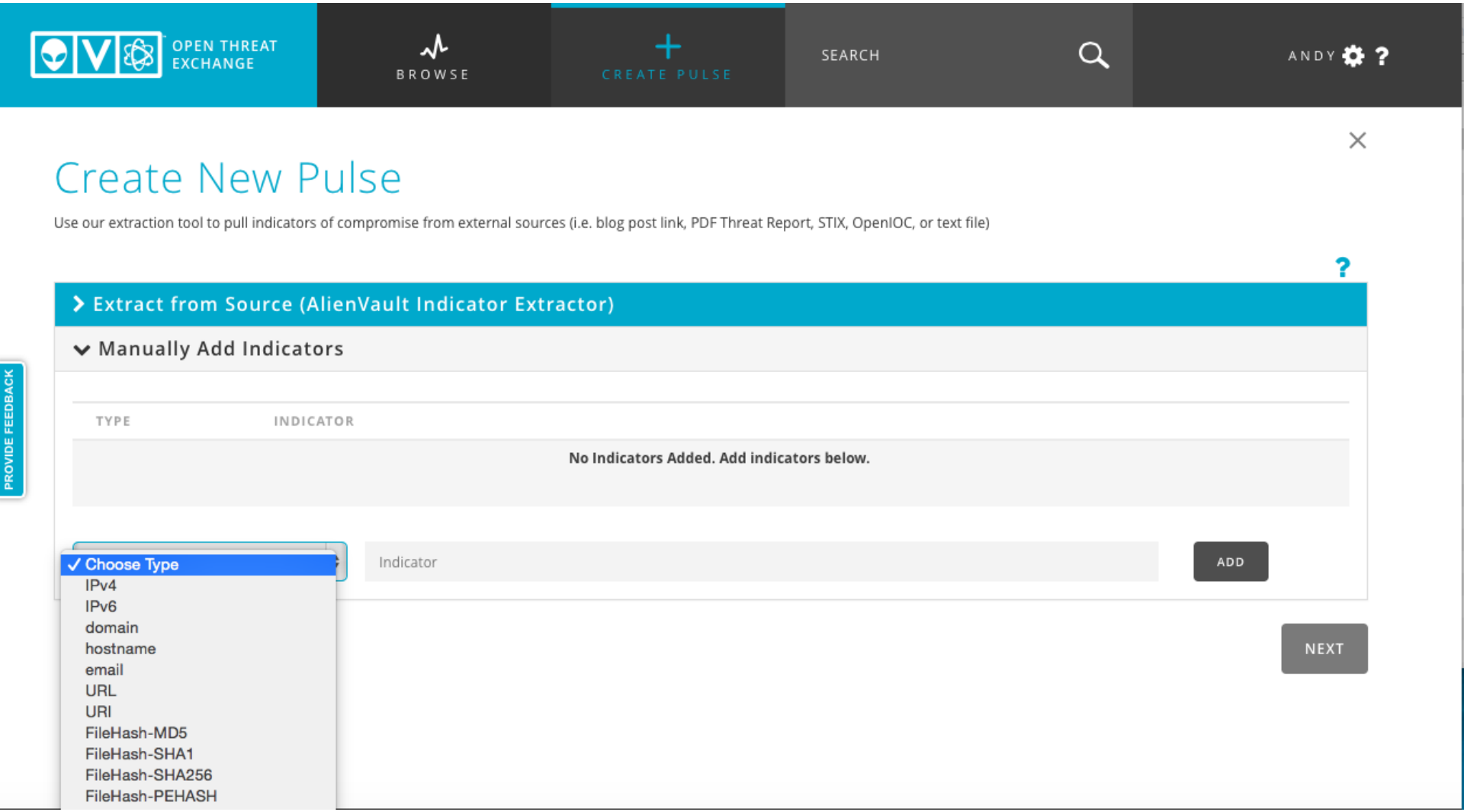
External Sources

VirusTotal

CREATING A PULSE FROM SOURCE FILE



CREATING PULSE MANUALLY



PULSE API:
OPEN ACCESS, OPEN STANDARDS

DirectConnect API

- Free access to Java and Python SDKs for pulse data
- DirectConnect Agents for popular open source software suites (e.g.: BroIDS)

Open Formats

- Export pulses to STIX, OpenIoC, CSV

STIX™

SUMMARY

EFFECTIVE THREAT SHARING

- Crowd-source threat data without attribution
- Provide valuable intelligence that can be acted on quickly
- Facilitate the collection, validation and dissemination of diverse, crowd sourced threat data
- Open, collaborative and affordable
- Enable organizations to share threat intelligence with each other in a trusted environment
- Should span industries, market categories and geographies


ISC
2015
中国互联网安全大会
360互联网安全中心