# Threat Intelligence Management Practical Exercise

Moderator, Darnell Washington
Reena Vaswani, E.K. Associates
Ken  Ardiel, Threat-Zero
Mohan Reddy, The Pinnacle Group
Paul Forney, The Pinnacle Group

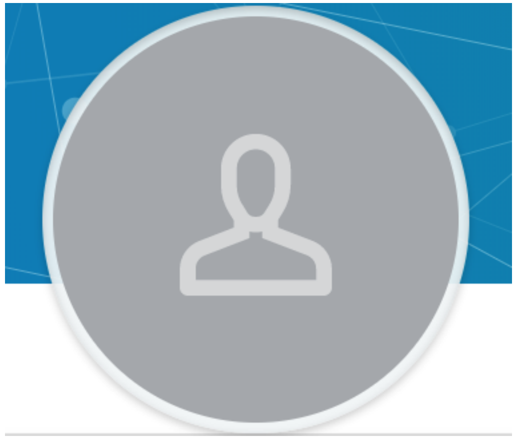
PORTCON 2019 LA Long Beach - Annual Update Conference of the Certified Port Executive Program

Paul Forney

Mohan Reddy

Darnell Washington

Reena Vaswani



Ken Ardiel, Threat-Zero

# Threat Intelligence

“If we know which vulnerabilities an adversary is exploiting, we can choose the technologies and activities that will best mitigate exposure to those vulnerabilities”.

# New attack vectors

## Cyber as the new warfare domain

Due to increasing cyber threats around the world, U.S. Cyber Command officially became a unified combatant command in May.

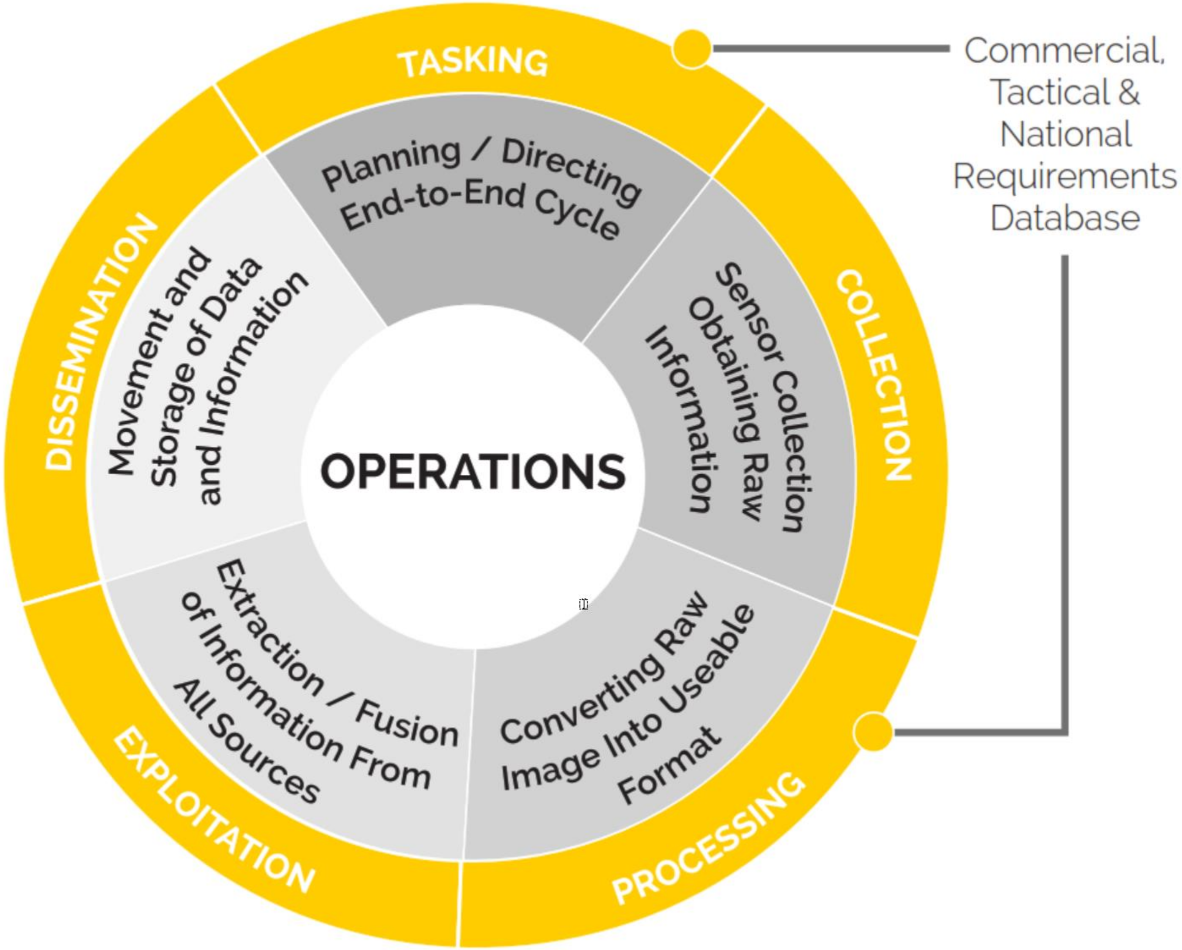
**Stuxnet- Date:** 2010.
**Target:** Iranian nuclear program.
**Attributed to:** NSA assistance from Israel.
Impact: Destruction of centrifuges
**Wiper attack Date:** 2012.
**Target:** Saudi Aramco
**Attributed to:** Iran hacking group.
Impact: Shamoon destroyed 30,000 Saudi Aramco office computers
**China Supply Chain Backdoors - Date:** 2013.
**Target:** US Companies and organizations around the world.
**Attributed to:** China's APT1 hacking group.
Impact: Global supply chain disruption
**Sony Pictures-** 2014.
**Target:** Sony Pictures.
**Attributed to:** North Korean hacking group "Guardians of Peace".
Impact: Corporate espionage, ransomware, disclosure of Intellectual Property
**Office of Personnel Management - 2015.**
**Target:** The US Office of Personnel Management.
**Attributed to:** The Chinese government.
**Ukraine power distribution disrupted- Date:** December 2015.
Impact: Power network distribution shut down

**Bangladesh Central Bank Heist-Date:** February 2016
**Target:** Bangladesh Central Bank.
**Attributed to:** North Korea’s Lazarus group.
Impact: Threat to steal 1 Billion – Actual Loss 81 Million
**Cloud Hopper Date:** April 2017
**Target:** Managed Service Providers (MSPs) across the world.
**Attributed to:** APT10 and The Chinese Ministry of State Security.
The so-called Operation Cloud Hopper campaign involved supply-chain attacks of MS. Managed service providers (MSPs) The process is in direct accordance with China's attempts to steal intellectual property from western nations. The motivation is China's economic plan to close the gap between it and the West.
**Wanna Cry-** May 2017
Attributed to: North Korea
Impact: Global Malware campaign using NSA Leaked tools
**Not Petya - Date:** 2017- **The most costly attack in history (MAERSK)**
**Target:** Global cyber-attack, but initially targeting Ukraine.
**Attributed to:** Russia.
**Attributed by:** The UK and US governments.
Used the NSA-developed EternalBlue backdoor exploit using Ransomware.
Impact: Crippled and destroyed 49,000 computing and information systems… could not be wiped or reinstalled

# Nation State Attacks

- Government state funded cyber network exploitation
- Backdoors and malicious injection of code in web sites and cloud hosted applications
- Supply Chain infection of network connected devices and IoT and IoT
- Trade and Technology impacting world economic markets
- New Currency Trends and Technologies (Blockchain, Bitcoin)

# Threat Intelligence Overview



OPERATIONS

TASKING

Planning / Directing End-to-End Cycle

COLLECTION

Sensor Collection Obtaining Raw Information

PROCESSING

Converting Raw Image Into Useable Format

EXPLOITATION

Extraction / Fusion of Information From All Sources

DISSEMINATION

Movement and Storage of Data and Information

Commercial, Tactical & National Requirements Database

# Cyber Security and Threat Intelligence Management

The Pinnacle Group
Securiosity

# Cyber Security and Threat Intelligence Management

Threat-Zero™

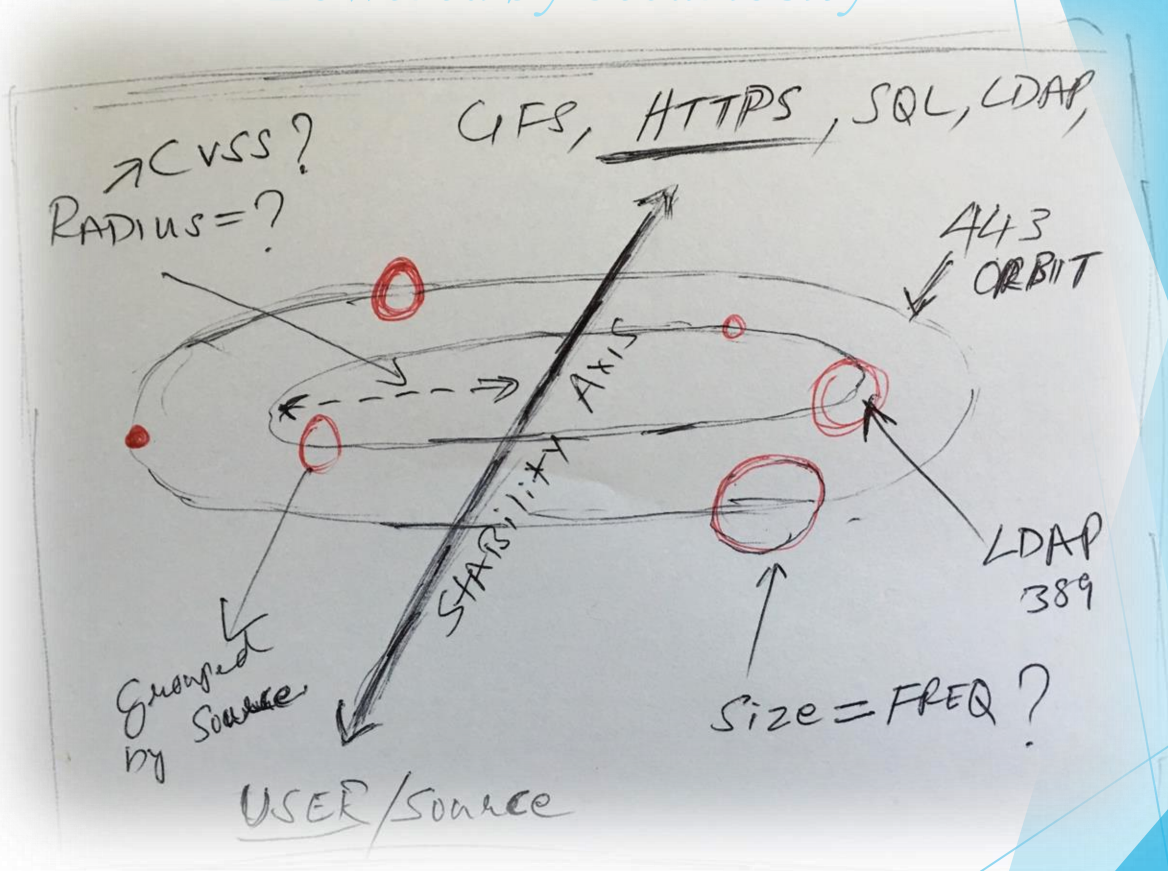
*Powered by Securiosity®*

Cognitive cybersecurity powered by deep-learning with AI

# Terms and Definitions

Threat-Zero™
*Powered by Securiosity®*

- ❑ Cognitive Learning
- ❑ Tensors
- ❑ Deep Learning
- ❑ Unsupervised Learning
- ❑ API Integration
- ❑ Complex Event Processing
- ❑ Predictive Analytics



# What is Threat-Zero™

Threat-Zero™
*Powered by Securiosity®*

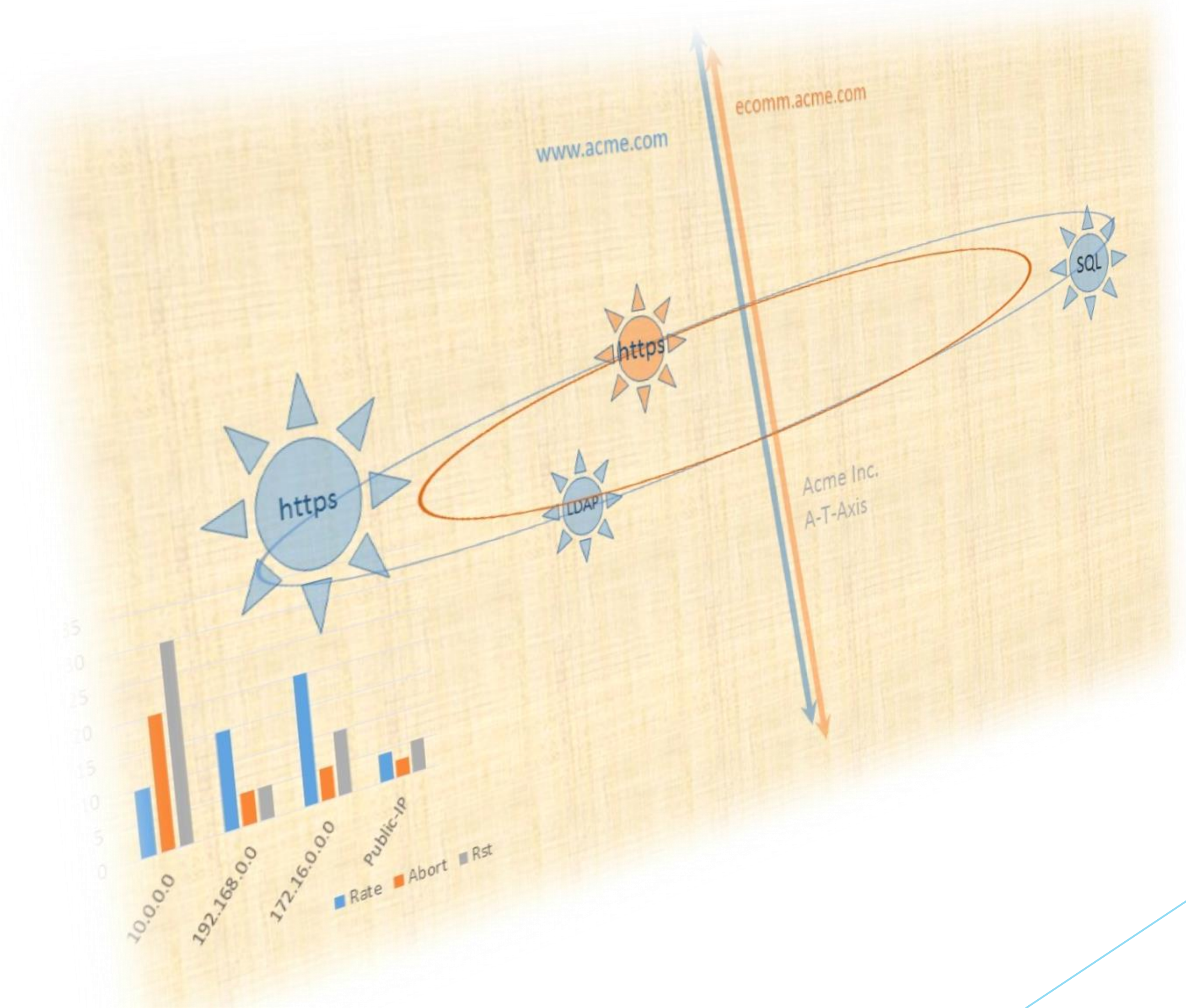
Cognitive cybersecurity powered by neural networks For unsupervised learning, complex event processing for early mitigation of previously unseen threats to your data. We utilize deep learning with AI techniques that borrow from astrophysics research, to search for patterns beyond the byte-signature methods.

**Threat-Zero is uniquely positioned to disrupt the bad actors and secure your network.**

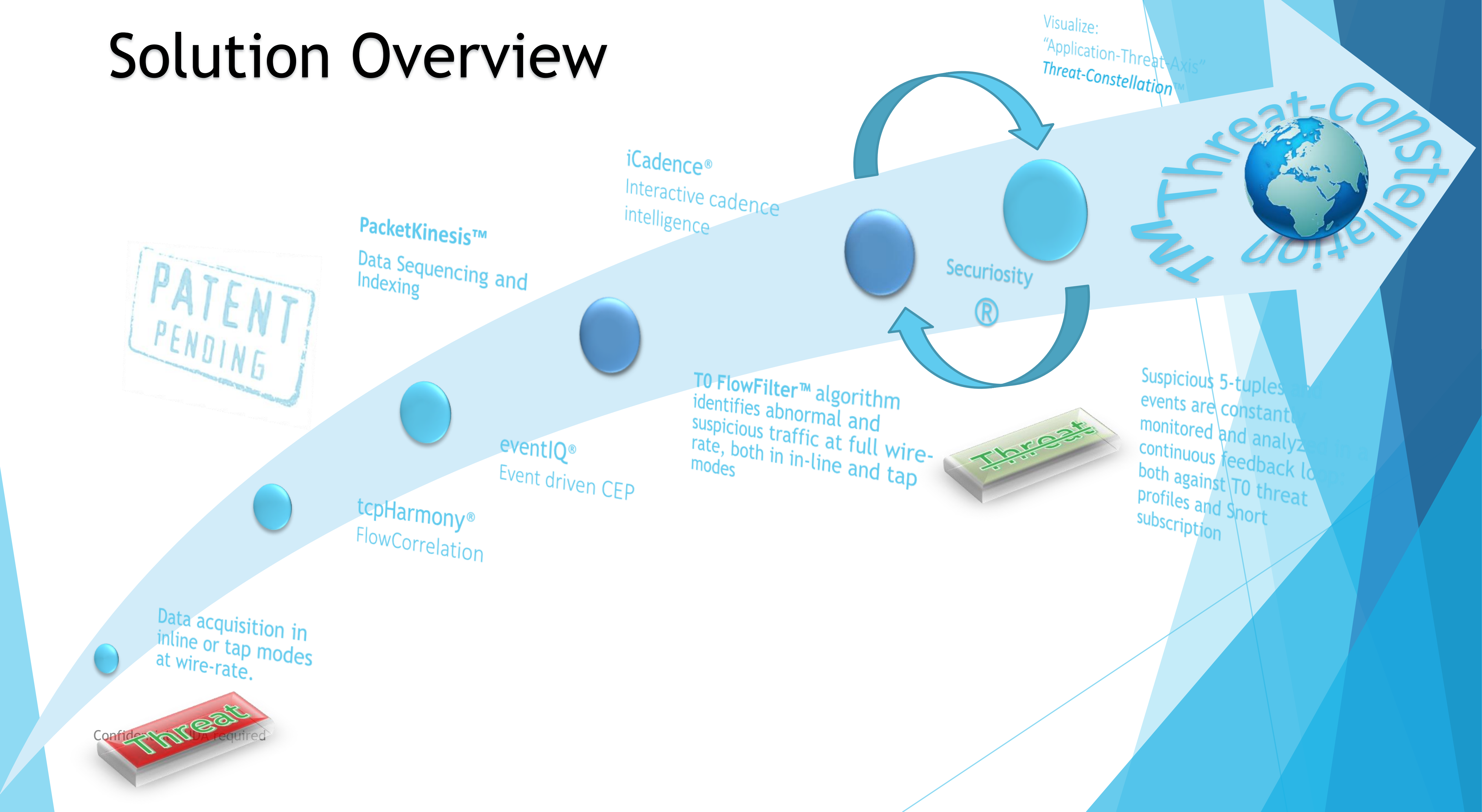
# Design Concept

Threat-Zero™

*Powered by Securiosity®*



# Solution Overview



PATENT PENDING

Data acquisition in inline or tap modes at wire-rate.

tcpHarmony®
FlowCorrelation

PacketKinesis™
Data Sequencing and Indexing

eventIQ®
Event driven CEP

iCadence®
Interactive cadence intelligence

T0 FlowFilter™ algorithm identifies abnormal and suspicious traffic at full wire-rate, both in in-line and tap modes

Securiosity ®

Suspicious 5-tuples and events are constantly monitored and analyzed in a continuous feedback loop: both against T0 threat profiles and Snort subscription

Visualize:
"Application-Threat-Axis"
*Threat-Constellation*™

# Highlights

Threat-Zero™

*Powered by Securiosity®*

- API first, mobile first, SAAS ready “container” system
- Byte signature AND cognitive pattern learning algorithms
- Lowest false positive rate in the industry
- Single appliance and simple licensing
- Uncluttered and intuitive UI: *ThreatScape*™
- Wire-rate threat detection for complex events (DDoS, APTs, Exfiltration)
- *ThreatConstellation*™ flow-monitoring
- E-Vision event correlation with cloud intel, syslog
- AI-Polymorphic Threat Defense

# Third Party Integration

Threat-Zero™

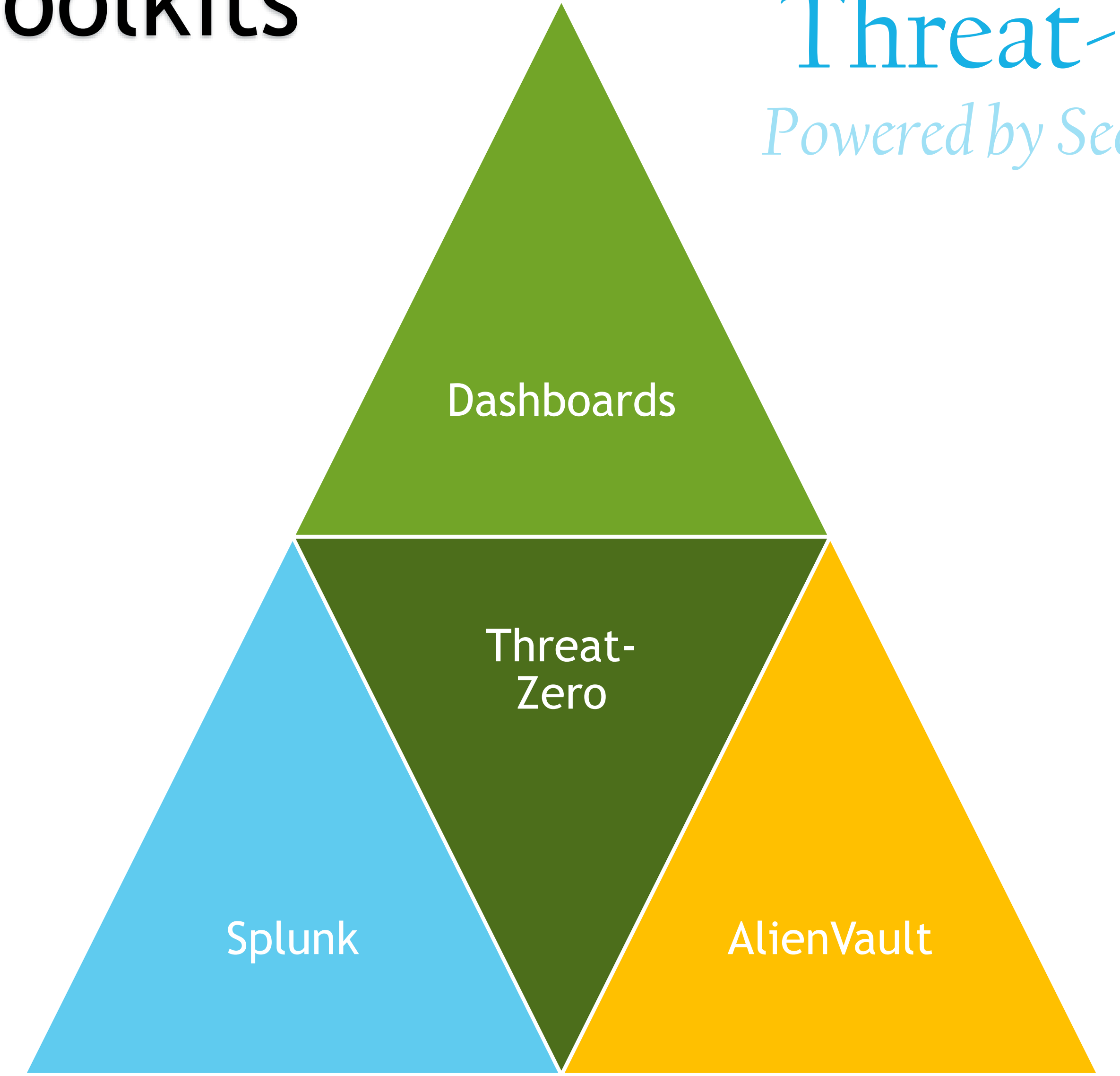
*Powered by Securiosity®*

- Threat-Zero Active Security: deep learning, polymorphic defense
- 1U, 20TB, Threat-Zero appliance: deploys in minutes
- SteelCentral™ Packet Analyzer: deep packet analysis riverbed STEELCENTRAL
- AlienVault™ USM: 360° view of your network
- Splunk™ Security for continuous machine data analysis splunk>
- SIEM capability integrated with your edge, core and DMZ
- Integrated enterprise dashboards for your command center
- Real-time, clutter-free, summarized views for operators and executives
- Leverages Existing tools already deployed

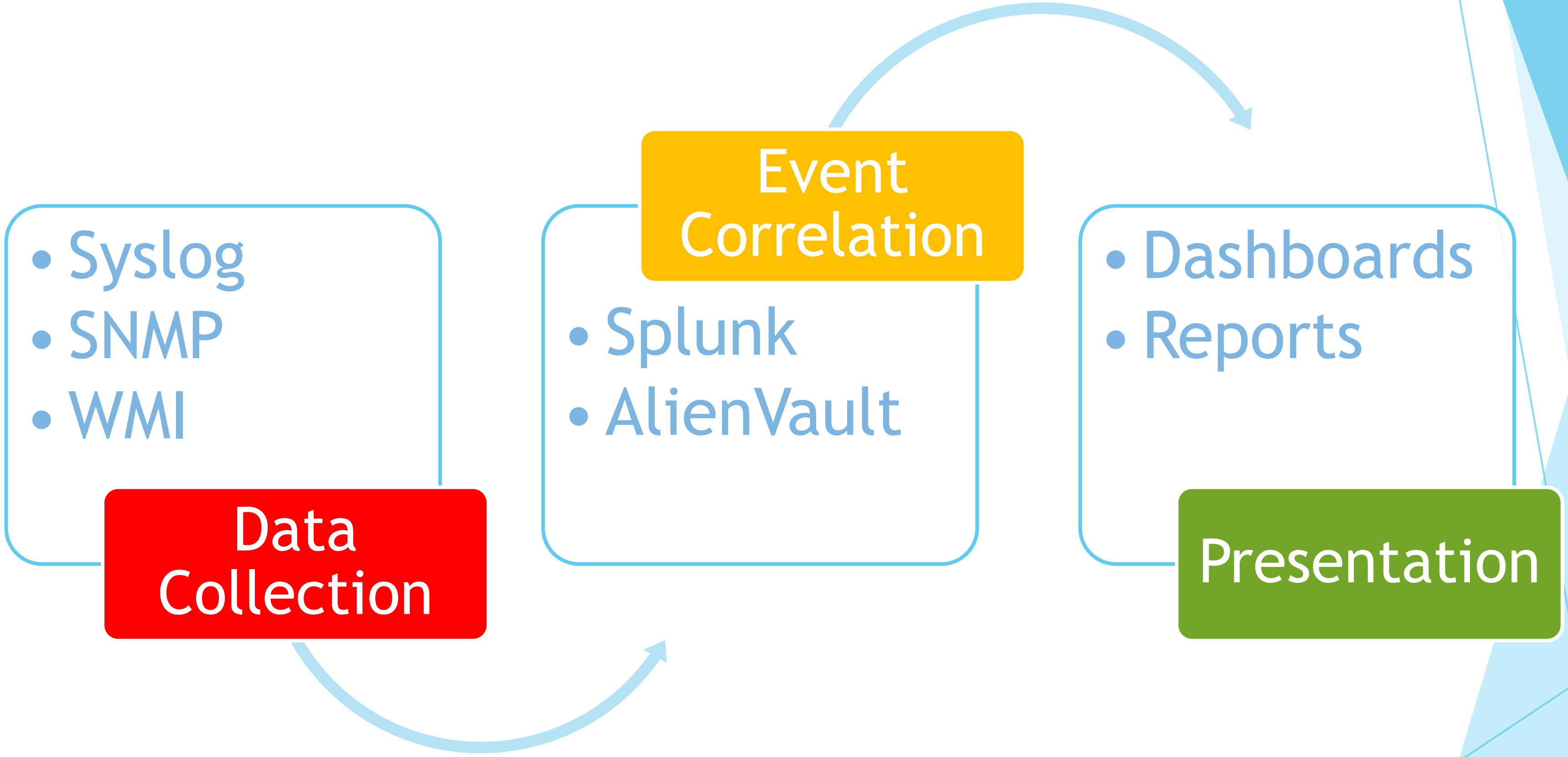
# Modular Toolkits

Threat-Zero™

*Powered by Securiosity®*



# Capture -> Correlate -> Captivate



- Syslog
- SNMP
- WMI

Data Collection

Event Correlation

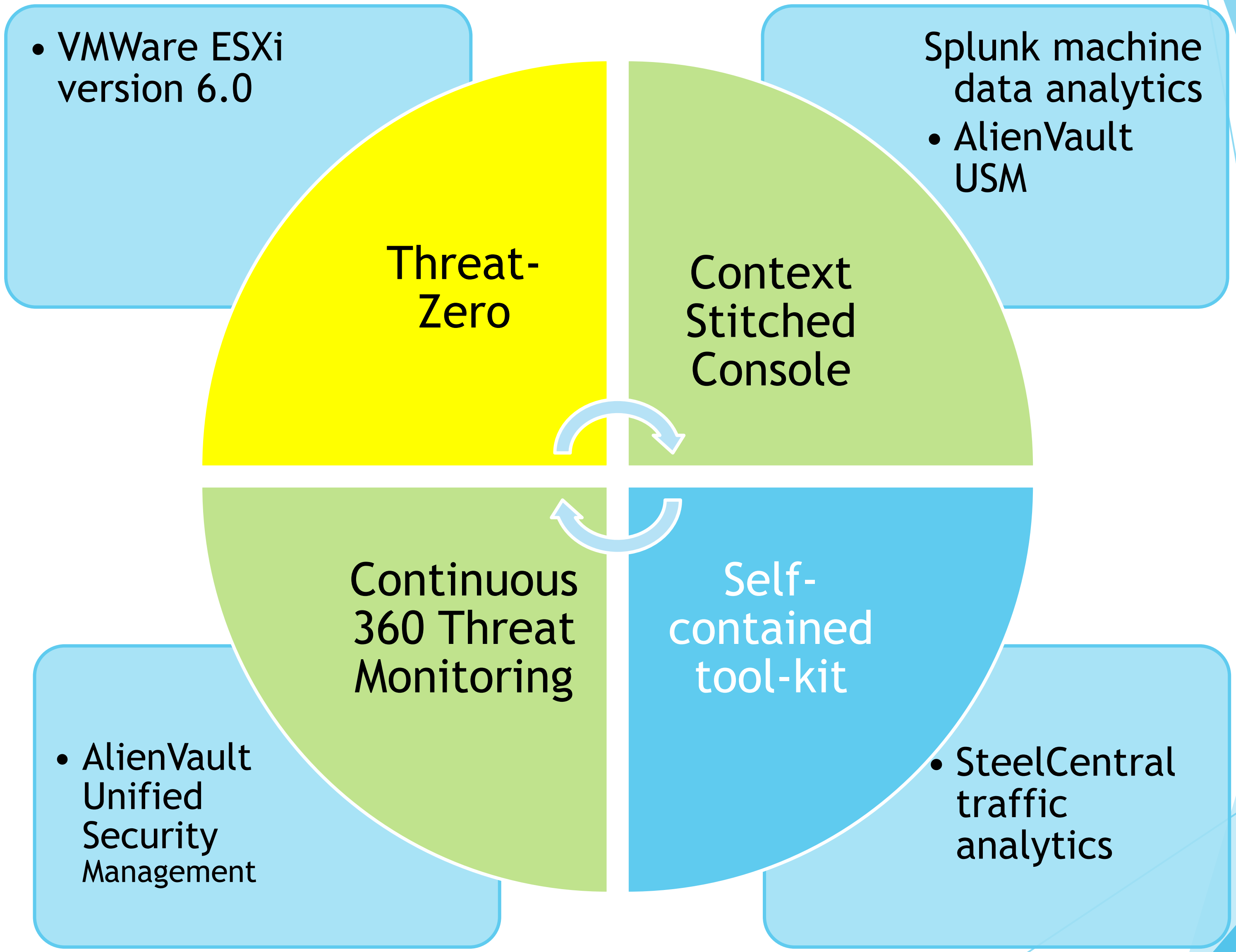
- Splunk
- AlienVault

- Dashboards
- Reports

Presentation

Threat-Zero™

*Powered by Securiosity®*



- VMWare ESXi version 6.0

Threat-Zero

Splunk machine data analytics

- AlienVault USM

Context Stitched Console

Continuous 360 Threat Monitoring

- AlienVault Unified Security Management

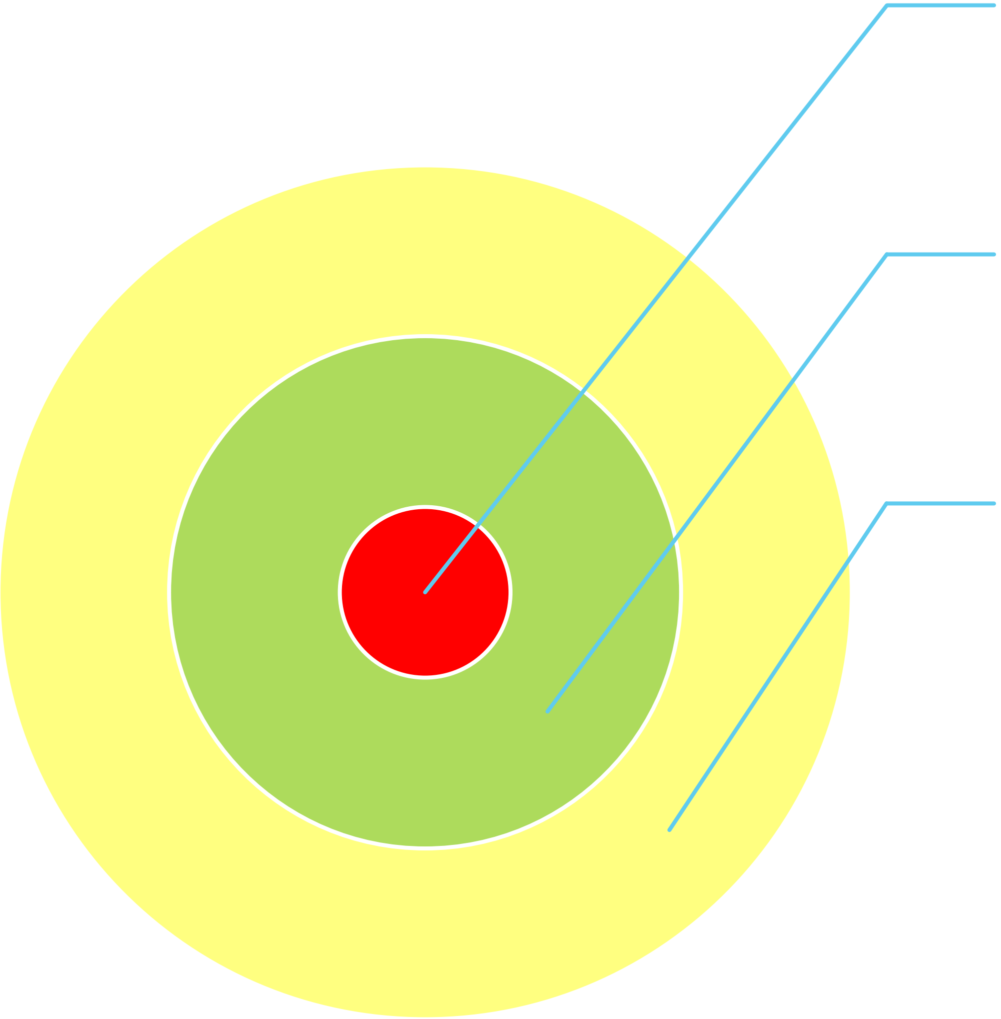
Self-contained tool-kit

- SteelCentral traffic analytics

# Smart Customization

Threat-Zero™

*Powered by Securiosity®*



Expert custom dashboards

Grafana

D3JS.org libraries

ThreatScape analytics

AI/Cognitive unsupervised learning

Log and event data collection

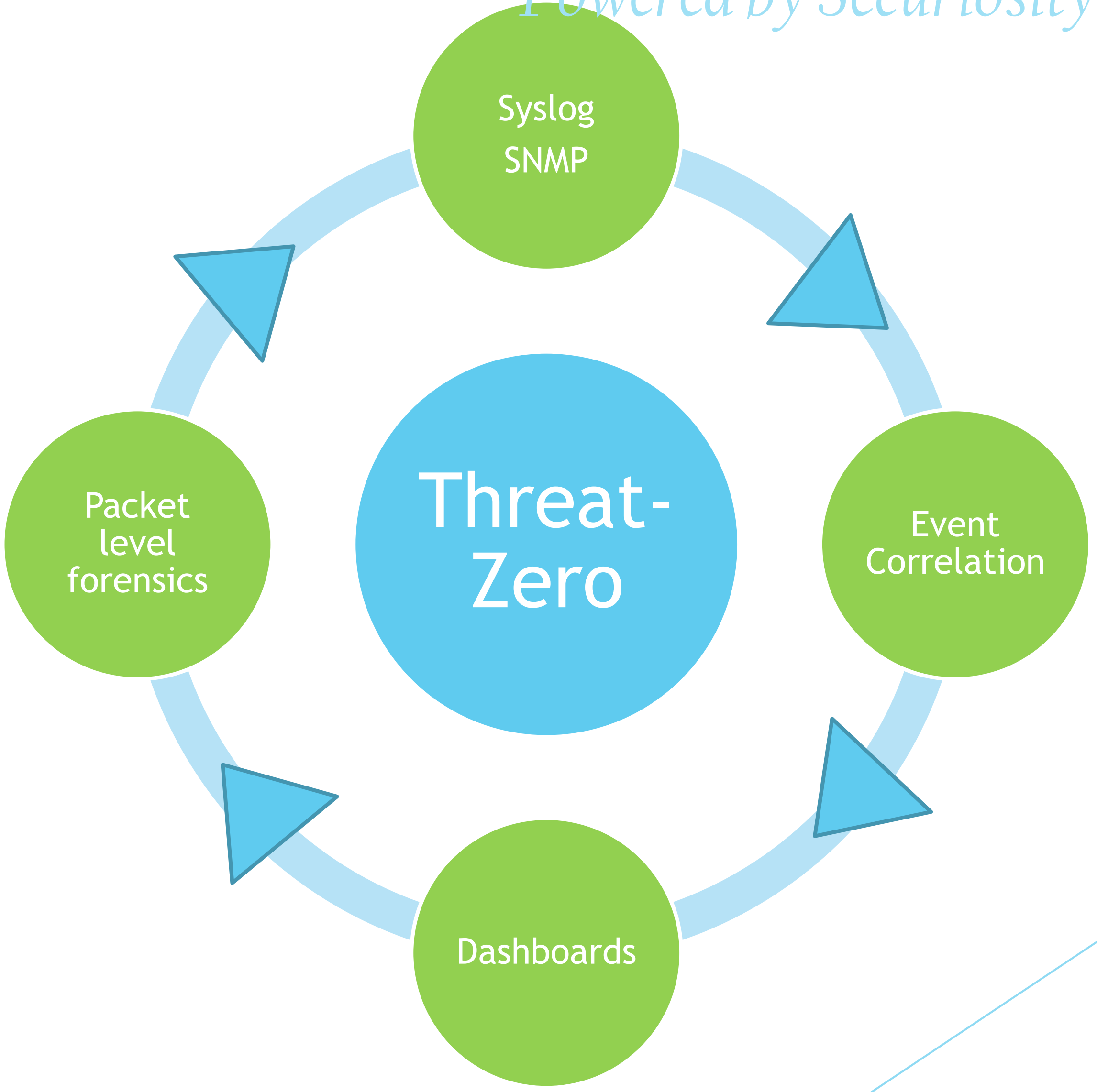
[SNMP, syslog, WMI]

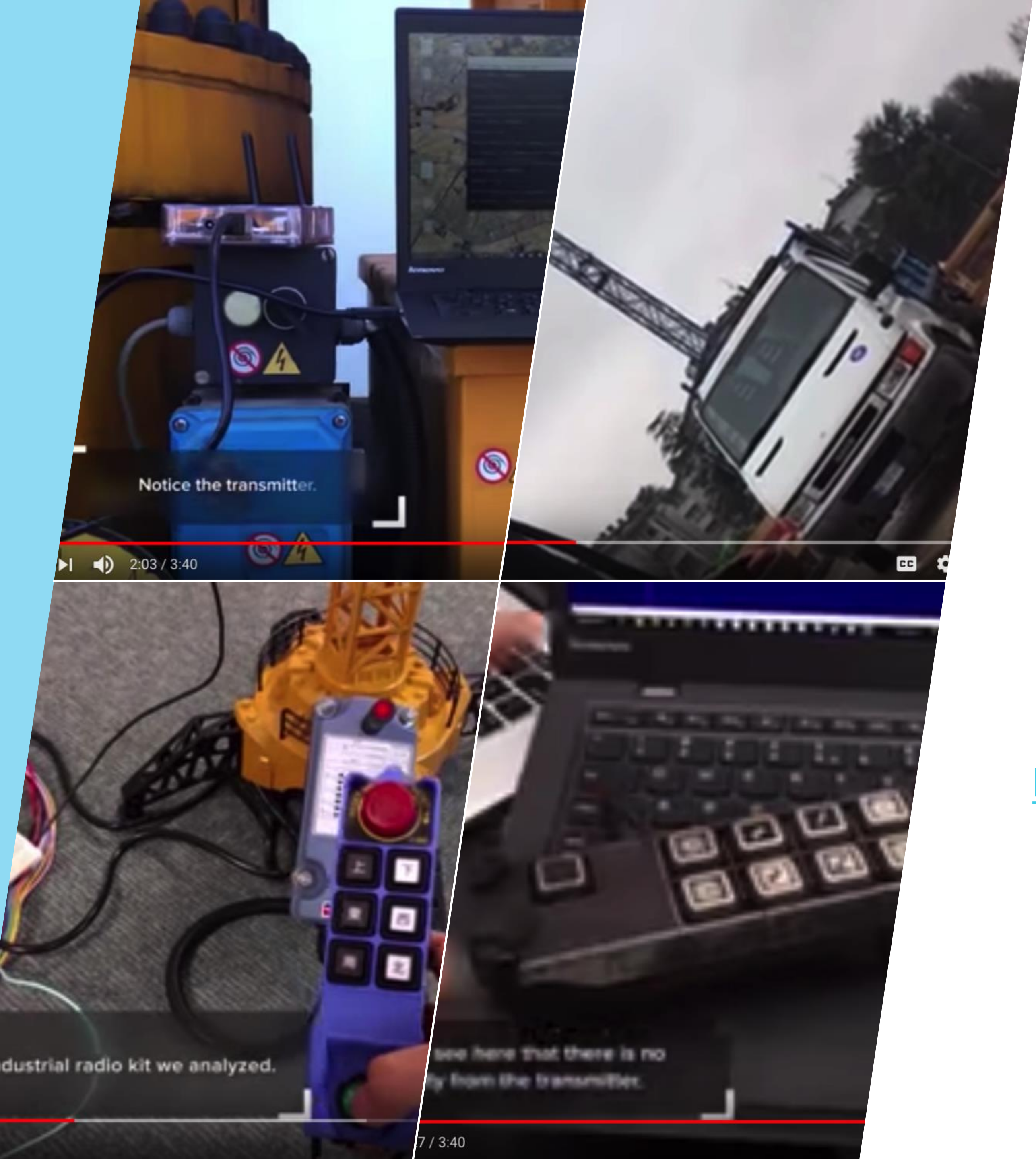
Logstash, Splunk

# 360º real-time views

Threat-Zero™

*Powered by Securiosity®*





Notice the transmitter.

dustrial radio kit we analyzed.

see here that there is no
y from the transmitter.

# Crane Hacking Practical Exercise

How we see it?

How we fix it?

How we share it?

https://www.youtube.com/watch?v=k8F7glmbCNg

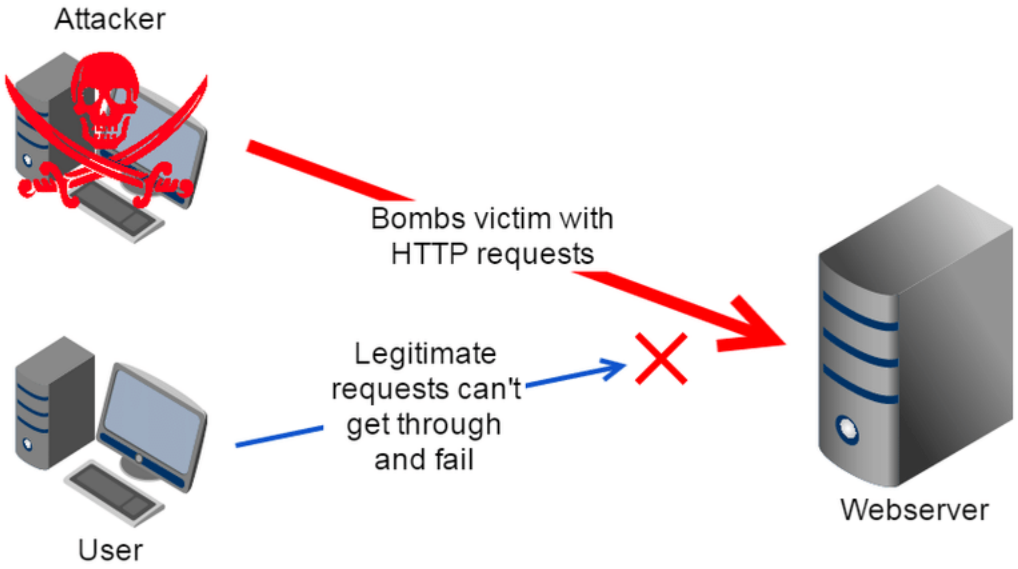
How we see it?

How we fix it?

How we share it?

# Malware Injection Practical Exercise

# Denial of Service Practical Exercise


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
Webserver
User

# Questions?