RISKSENSE

RiskSense

The industry's most comprehensive risk-based vulnerability management and prioritization platform

Arizona State Board for Charter Schools

Mark J. Fidel
CO-FOUNDER
STATE-LOCAL-EDUCATION SALES

19 Nov 2019

Milestones

- Computational Analysis of Cyber Terrorism against the U.S. (CACTUS)
- Behavior Risk Analysis of Vicious Executables (BRAVE)
- University Incubation CAaNES

CACTUS
BRAVE
CAaNES

2010

- Identified fragmented RFID as weaponized malware

RFID

2012

- RiskSense platform launched

RiskSense Platform

2015

- RiskSense, Inc. established

RiskSense, Inc.

2016

- **Series A Funding**
- Released KOADIC, command & control framework

Series A

2017

- RiskSense calls early warning of WannaCry

Early Warning of WannaCry

2018

- **Series B Funding**
- Improved EternalRomance, EternalSynergy, Eternal Champion pen testing tools

Series B

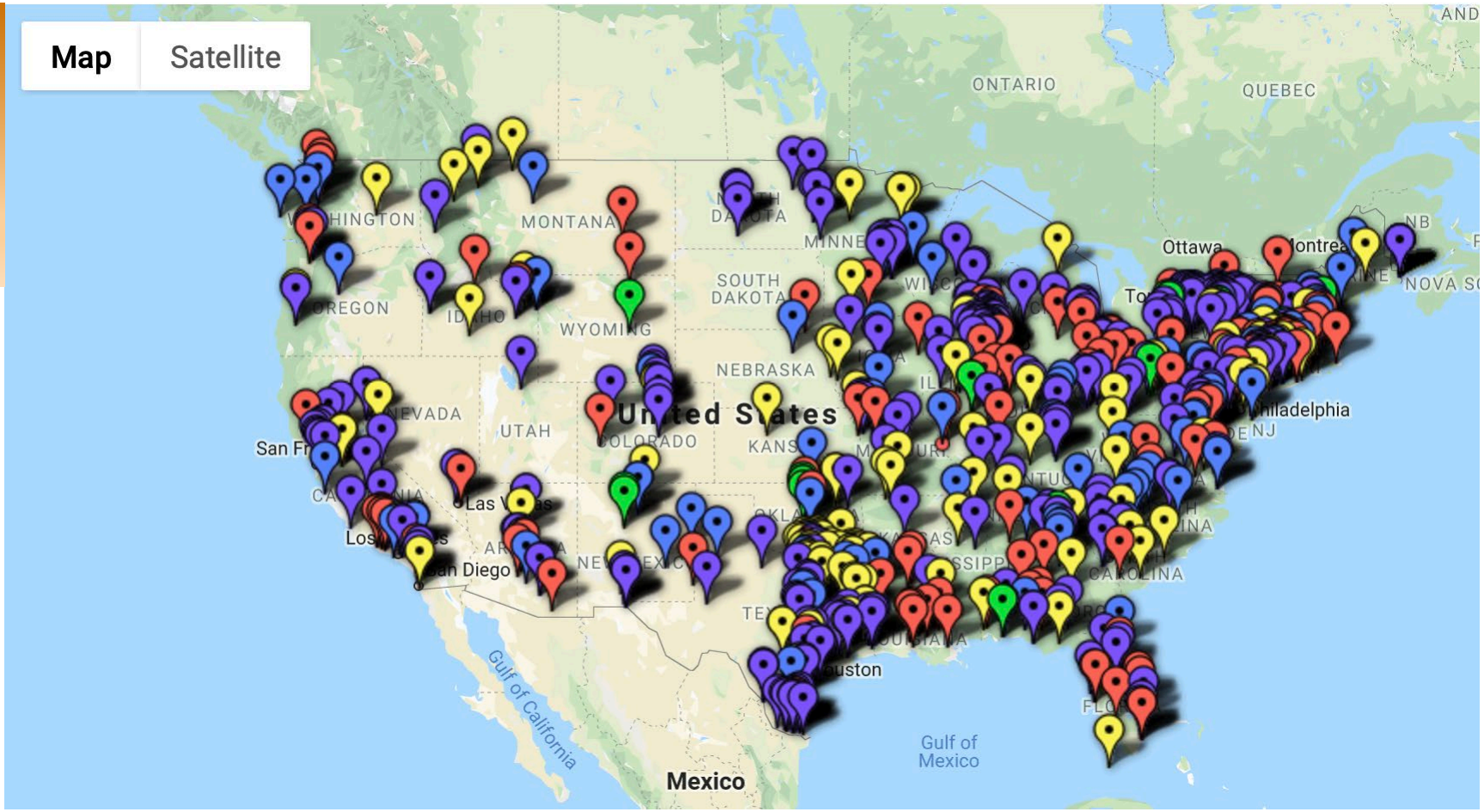
©2019 RiskSense, Inc.

RISKSENSE

The National Landscape of K-12 Cyber Attacks

727 Reported Incidents Since January 2016

Yellow = Ransomware
Purple = Breach
Blue = Phishing
Red = other incident



Source: https://k12cybersecure.com/map/

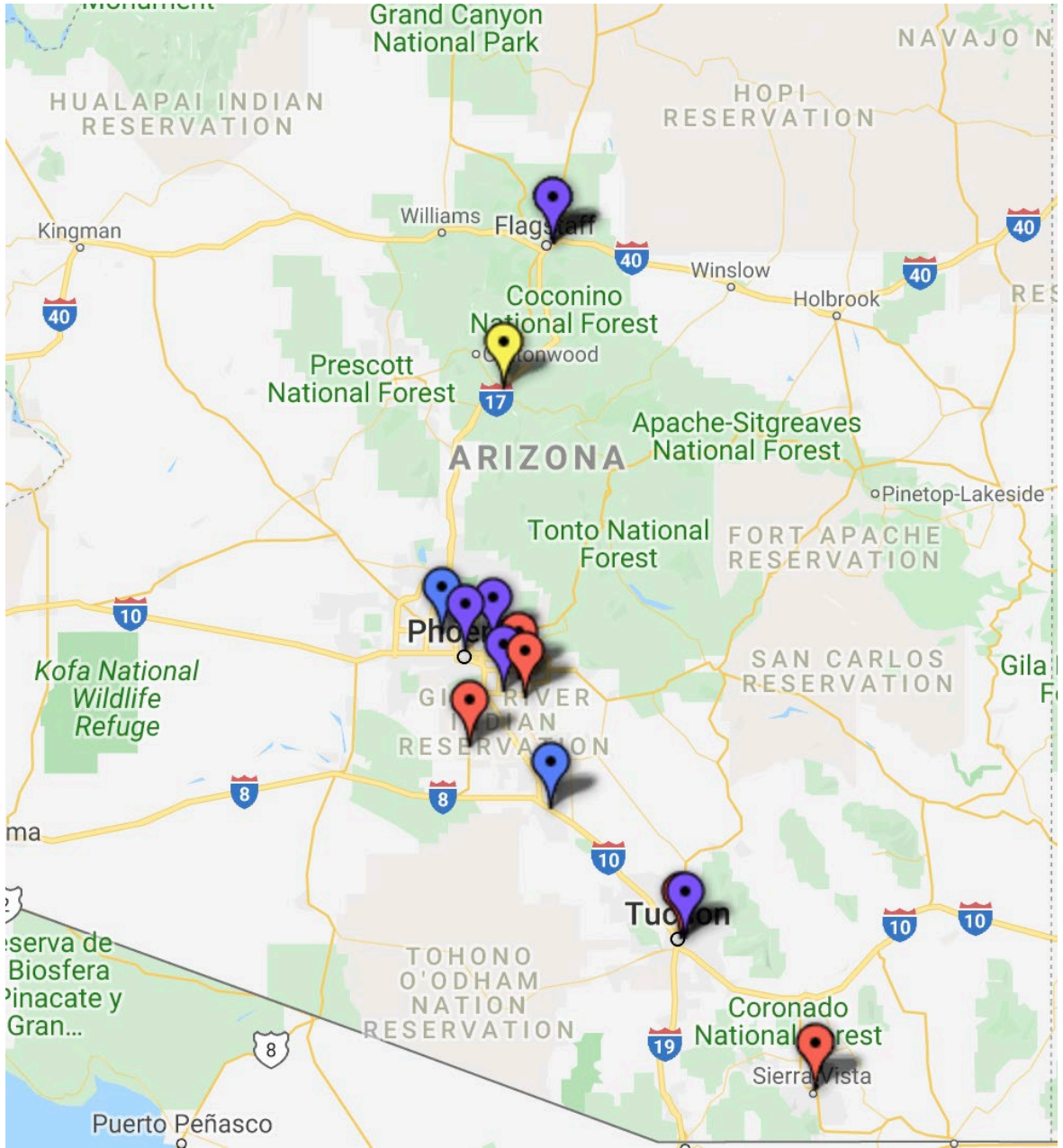
©2019 RiskSense, Inc.

RISKSENSE

The Arizona Landscape of K-12 Cyber Attacks

13 Reported AZ K-12 Incidents Since January 2016

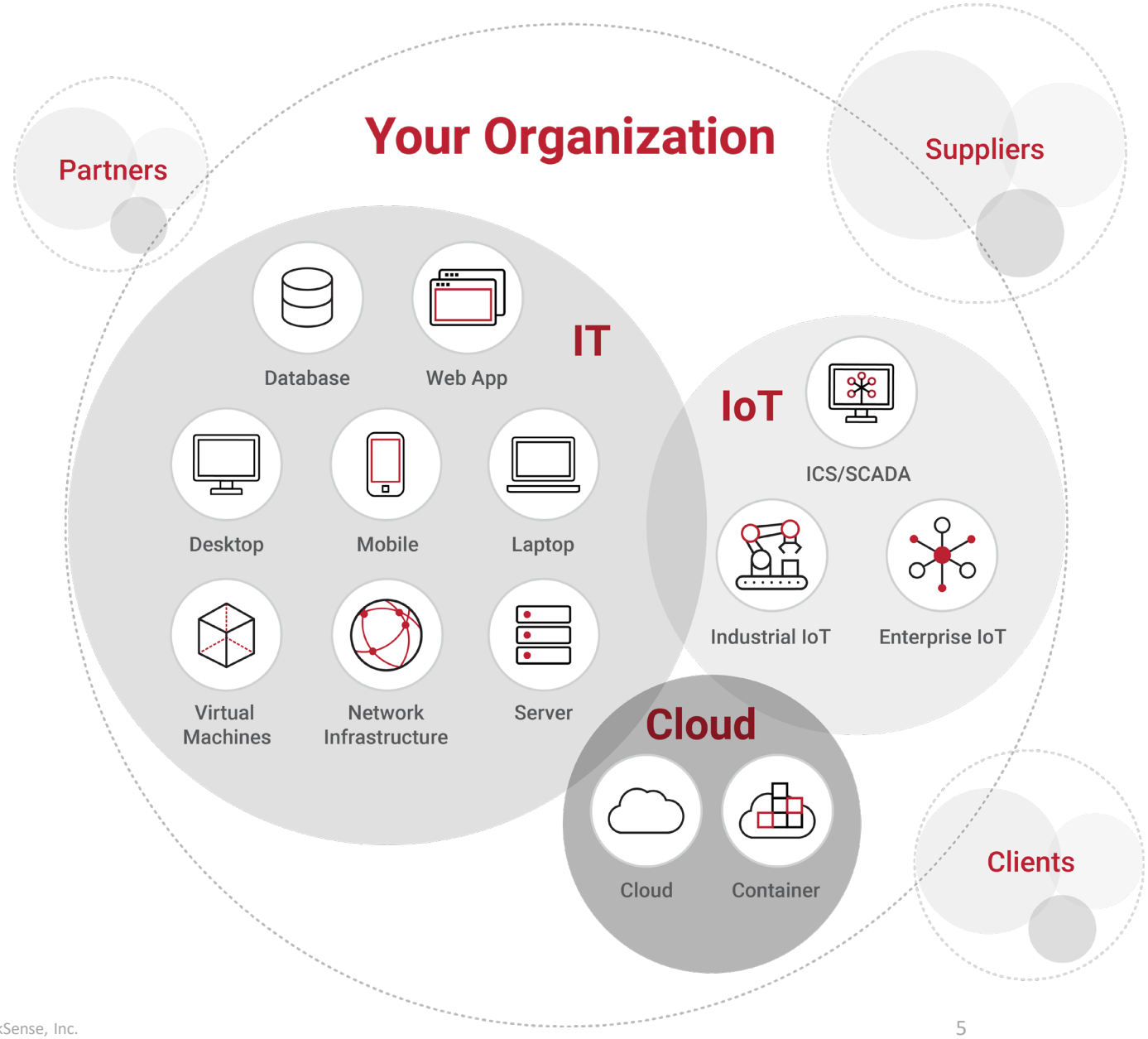
Yellow = Ransomware
Purple = Breach
Blue = Phishing
Red = other incident



Source: https://k12cybersecure.com/map/

©2019 RiskSense, Inc.

Attack Surface Problem



7X

Number of Assets

Critical Vulnerabilities *per Asset* (avg)

69+

Days

Time to Remediate a Critical Vulnerability (avg)

25%

Waste

Time consumed gathering, researching, normalizing, & correlating threat data

©2019 RiskSense, Inc.

Vulnerability Versus Exploit

vul·ner·a·bil·i·ty

noun

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

ex·ploit

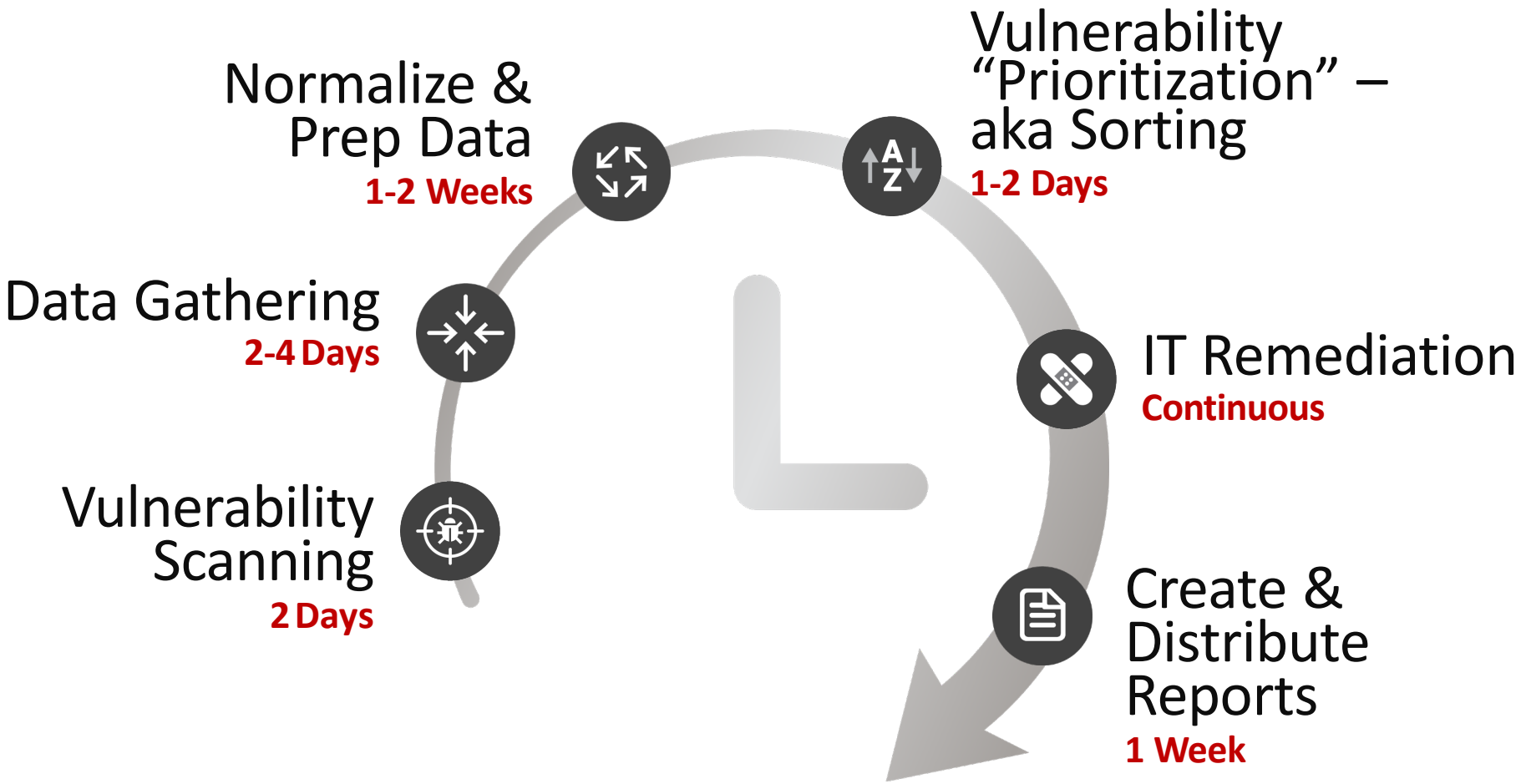
noun

/ˈekˌsploit/

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack.

©2019 RiskSense, Inc.

Typical Approach: Unscalable & Unsustainable

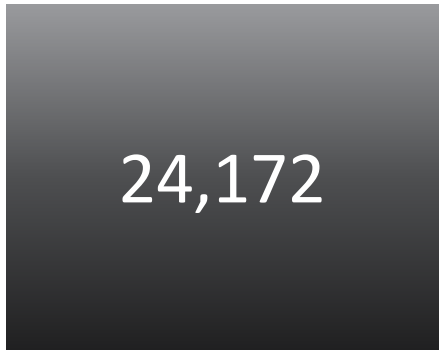


More People, Wrong Metric?

Brute force – using more people – isn't effective. More vulnerabilities are reported as remediated, but little improvement in security posture results.

©2019 RiskSense, Inc.

Vulnerability Baseline – National Vulnerability Database



Weaponized
with Exploit/Malware

Capable
of Remote Code Execution

Trending
Exploit/Malware with RCE

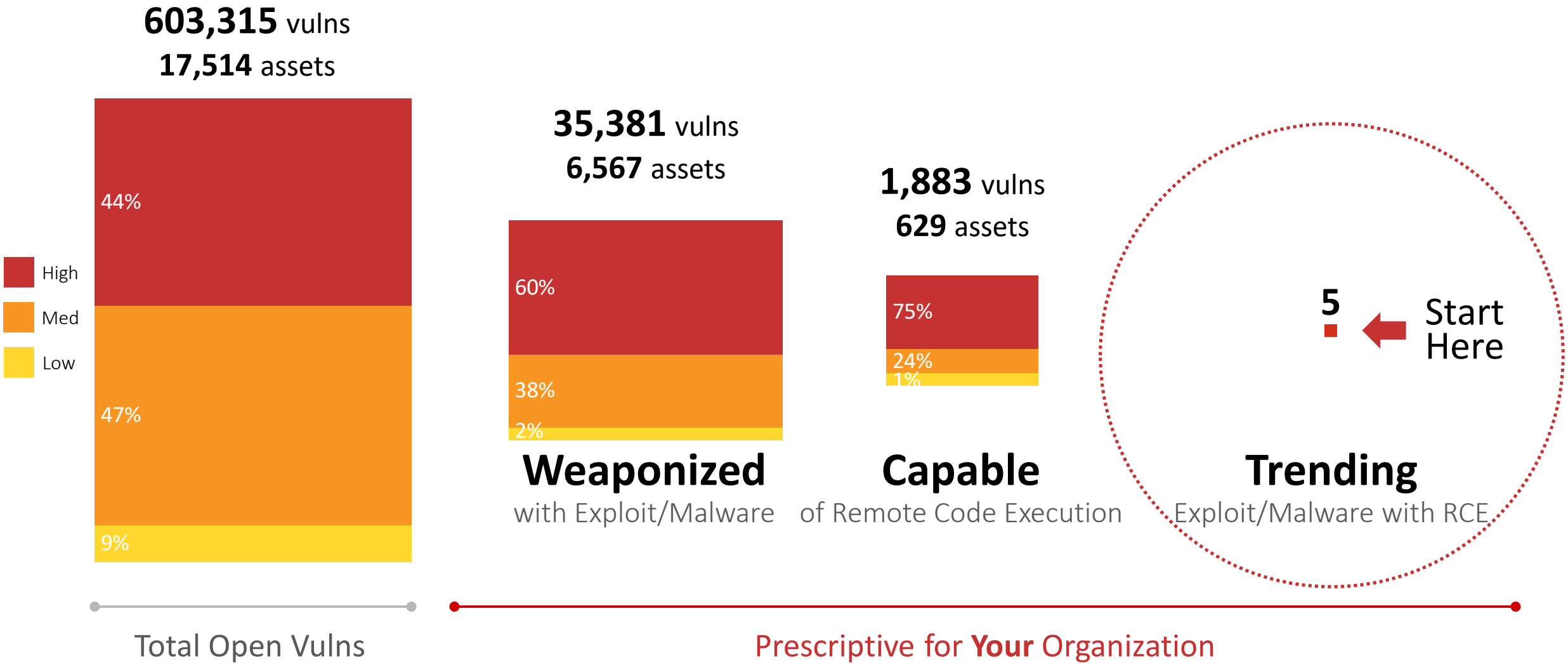
U.S. NVD CVE ID Total

Interesting for an Organization

Data current as of 07 Nov 2019

©2019 RiskSense, Inc.

Focus On Vulnerabilities That Matter – Yours



Industry: Government

©2019 RiskSense, Inc.

Where Does That Leave Us?

In an era where *known* security vulnerabilities are the leading cause of data breaches, most organizations are suffering with tools and processes that:

Offer no/poor **visibility**, lack context, and make it hard to collaborate

Make it hard, if not impossible, to measure, manage, and **control** risk

Lack meaningful prioritization and **reporting** to direct activities and align expectations

©2019 RiskSense, Inc.

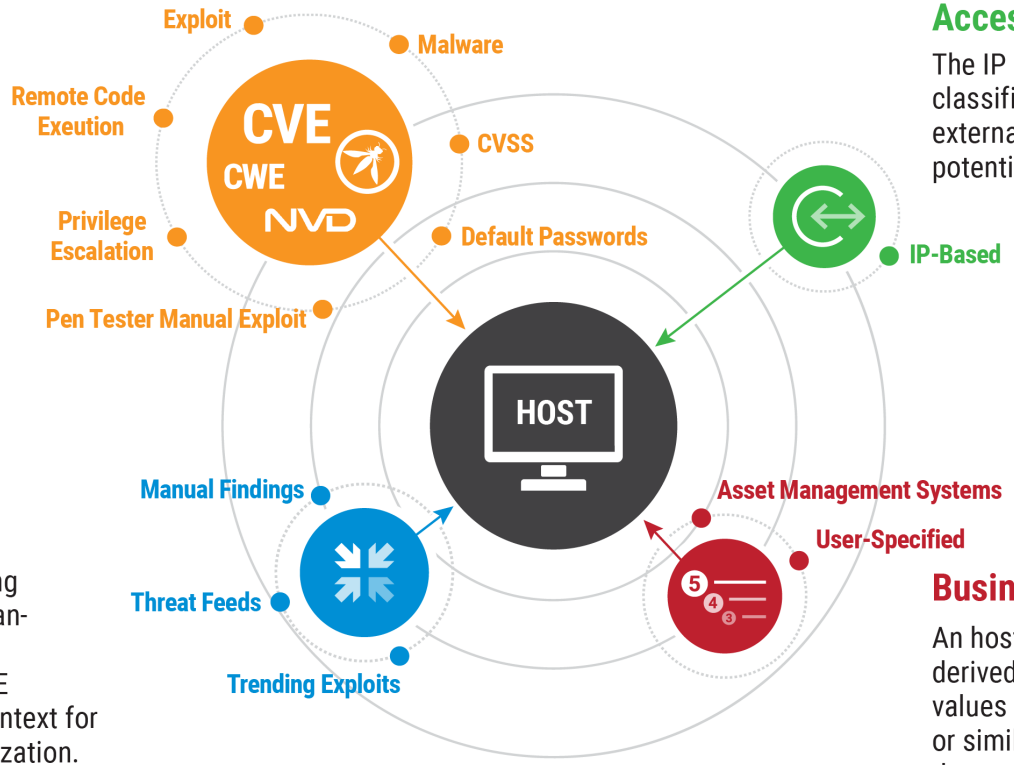
RiskSense Security Score (RS³) Model

Vulnerability Risk Rating

Each identified vulnerability receives a Risk Rating, indicating how much of a threat it poses according to its impact and ease of exploitability. Risk is computed using a combination of CVSS v3 vectors, threat classifications, and RiskSense exploit validation data.

Accessibility

The IP address of each host is classified as internally or externally accessible to reflect its potential exposure.

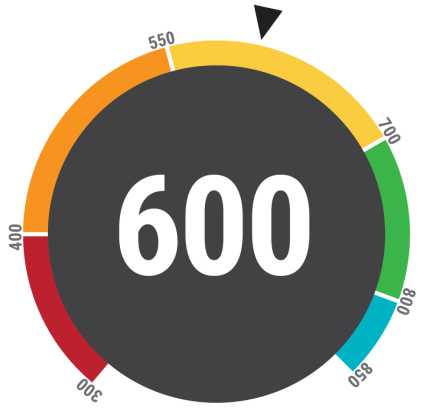


RiskFusion

Over 100 threat feeds, trending exploit information, and human-identified exploit data are all correlated to vulnerability CVE information, providing rich context for intelligent scoring and prioritization.

Business Criticality

An host's business criticality is derived from user-specified values in the RiskSense platform or similar values imported from the organization's asset management system.



RiskSense Security Score (RS³)
for individual hosts, groups, and consolidated organizational score

The RiskSense Security Score represents an organization's cybersecurity posture, measuring risk posed by existing vulnerabilities as well as current and trending threats, while accounting for each host's business criticality and probability of breach.

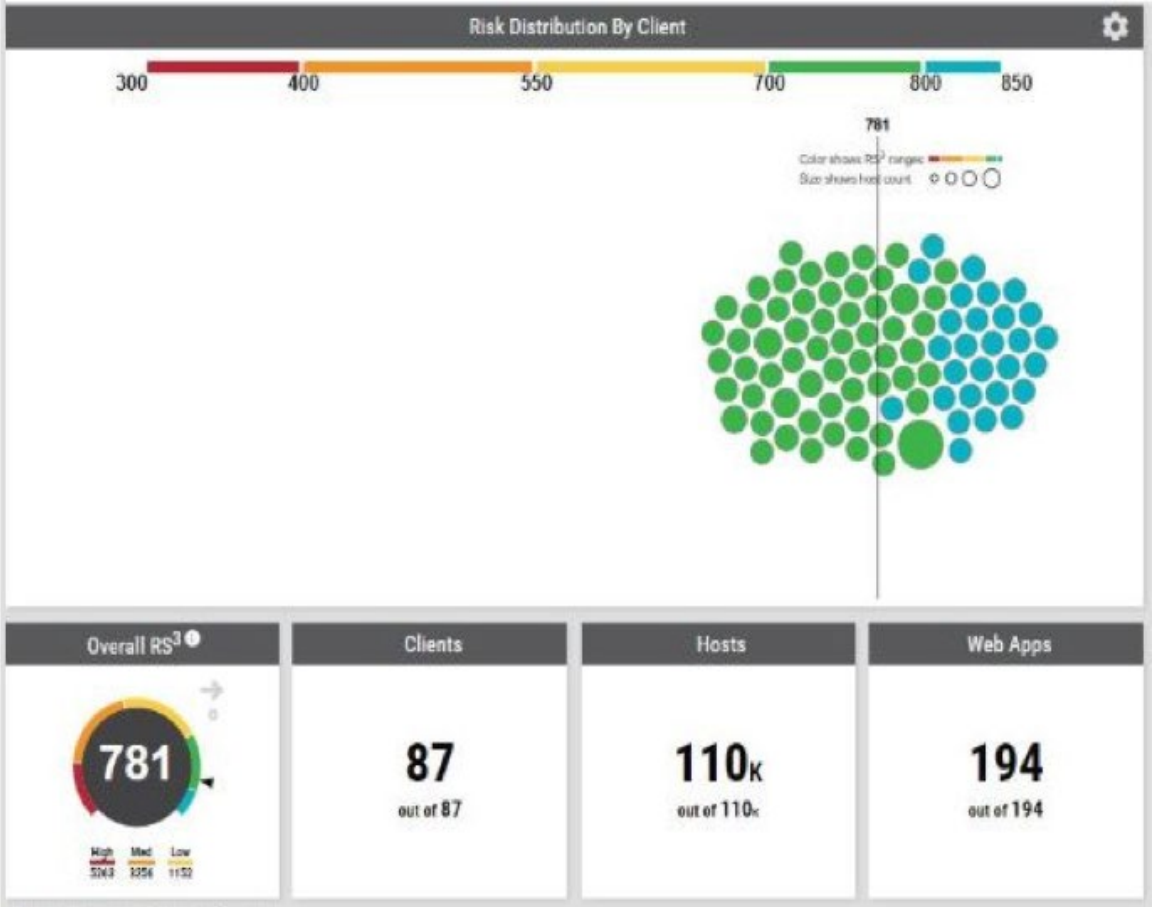
©2019 RiskSense, Inc.

Multi-Client Dashboard

CASE STUDY – STATE OF ARIZONA

- Driving Outcomes with RS^3
  - Group scores are used to compare agencies with one another
  - Internal RS^3 awareness creates competition
  - Pair strong performers with those needing help
  - 18-month journey has resulted in all agencies achieving risk score targets

After



©2019 RiskSense, Inc.

Groups Cards Provide Quick Organizational Comparison

- Easily see how groups, departments, and business units compare to one another
- Quickly see risk-based funnel for a specific group to determine what needs attention

©2019 RiskSense, Inc.

RiskSense Customer ROI – Arizona State University

5-Month ROI

- 90% time reduction to identify and analyze vulnerabilities
- Deployed and operationalized RiskSense in 2 months
- Now, time is spent in the RiskSense platform on high-value remediation assignment, tracking, and validation activities, achieving massive security posture improvements
- Increase scanning to weekly cadence
- 50% reduction in risk exposure

ARIZONA STATE UNIVERSITY

"RiskSense is our go-to partner for cybersecurity. Excellent partner for consulting and work."

– CIO, ASU

©2019 RiskSense, Inc.

RISKSENSE

RiskSense Solution

RISKSENSE

The Solution – Proactively Reduce Cyber Risk

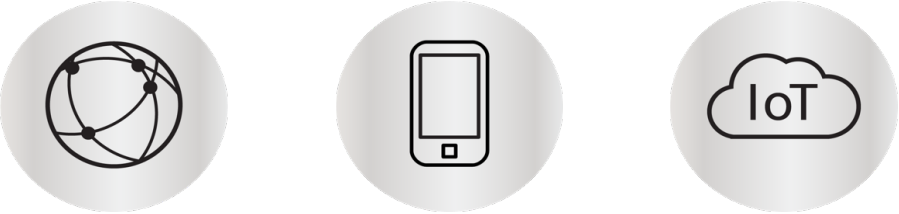
RiskSense RBVM

- Vulnerability and Threat Prioritization
- Cyber Risk Profiling (Risk Score)
- Attack Susceptibility and Early Warning

RiskSense Services

- Pen Testing (Web Apps, Network, IoT)
- Exploit Development
- Weaponization Analysis

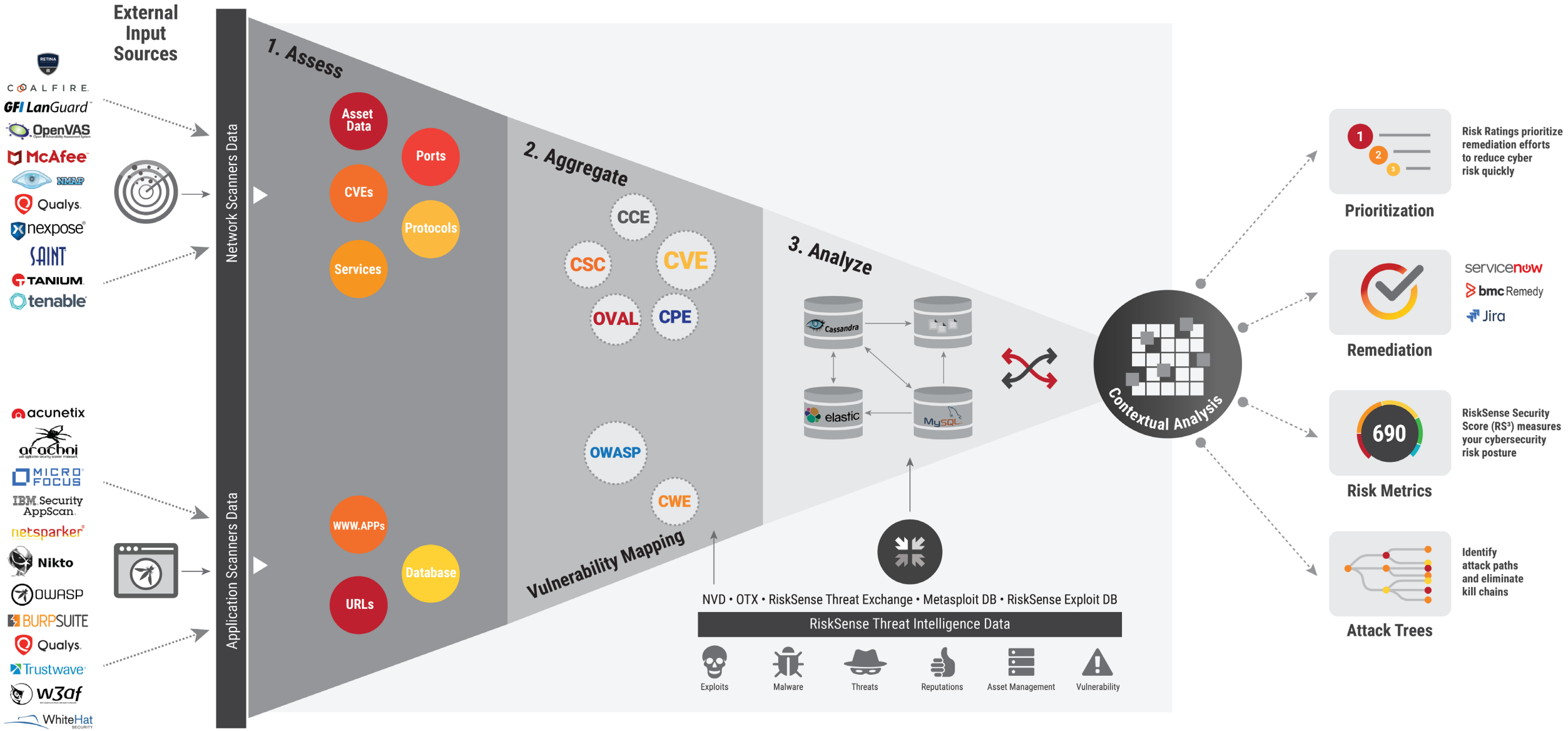
Empower business to focus on the threats and vulnerabilities that matter most



Network, Applications, & IoT

©2019 RiskSense, Inc.

RiskSense Platform



©2019 RiskSense, Inc.

RISKSENSE

RiskSense Services – Expertise Delivered

- Skill set and capabilities grounded in software development
  - Exploit writing
  - Web, Network, & IoT pen testing
  - Mobile application assessment
- Active production and use of AI-based tools
  - Toolkit expedites testing, instruments process
- Results delivered in near real-time via the RiskSense platform
  - Remediation guidance for immediate action
  - No more suffering from traditional “pen test latency”

Comprehensive Attack Surface Coverage

Intelligence-Driven Risk Analytics

Time-to-Value

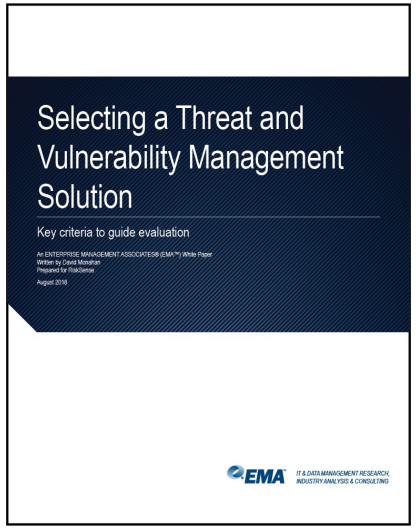
Shorten Time-to-Remediation

©2019 RiskSense, Inc.

RISKSENSE

Q&A and Resources

Enterprise Management Associates (EMA)
Top 10 Criteria for selecting a Threat and Vulnerability Management Solution



Case study – State of Arizona

Webinar – Predictive Intelligence: Vulnerability Weaponization and Exploitation with Dr. Srinivas Mukkamala

©2019 RiskSense, Inc.

New Era of Security

Your Organization Will Be Hacked and Breached

Are you prepared?

How fast can you respond?

RISKSENSE

RISKSENSE

RiskSense Platform

The industry's most comprehensive risk-based vulnerability management and prioritization platform

Visit our website at https://www.risksense.com/