KENNA Security

Taking a modern approach to security

What You've Always Done Isn't Sufficient Anymore

Jeff Aboud

Director of Product Marketing

Setting the stage

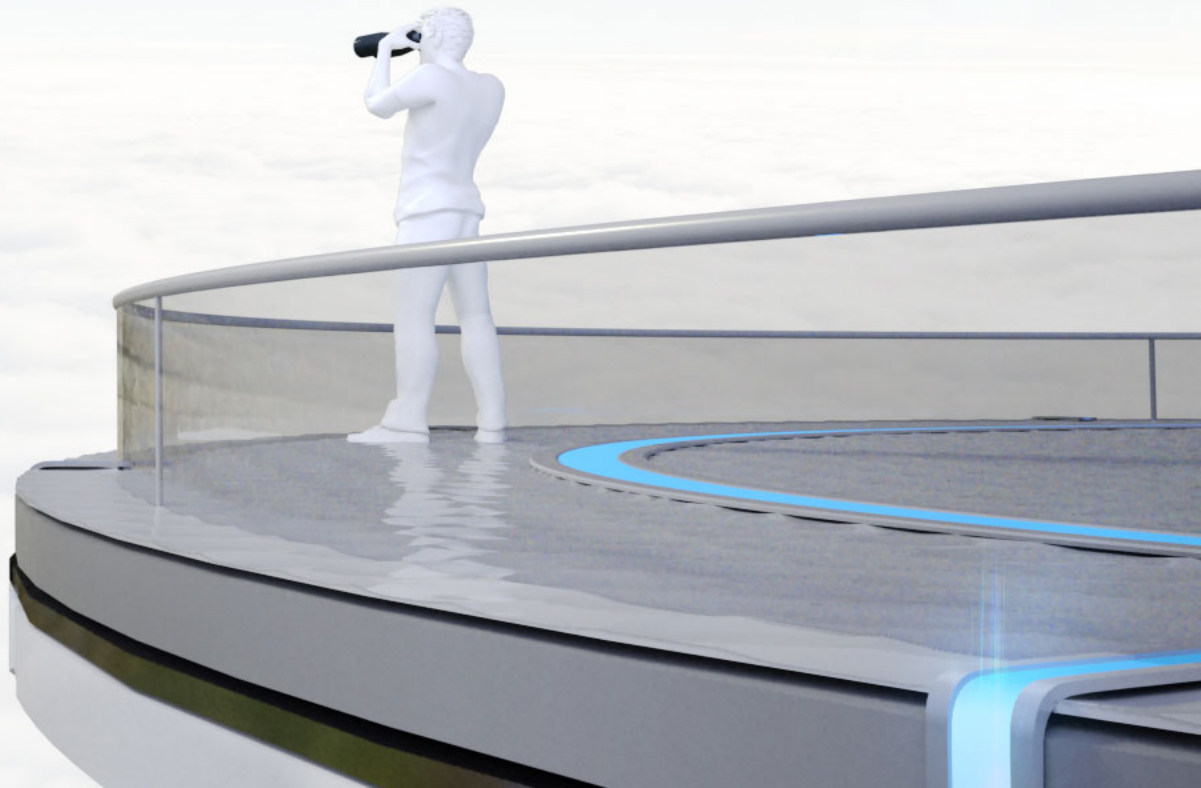
KENNA Security

> ***If You Always Do What You've Always Done, You Always Get What You've Always Gotten***
>
> Jessie Potter

> ***Insanity is Repeating the Same Mistakes and Expecting Different Results***
>
> Narcotics Anonymous

KENNA Security

Understanding the Problem



Cyber attacks always follow the same path …

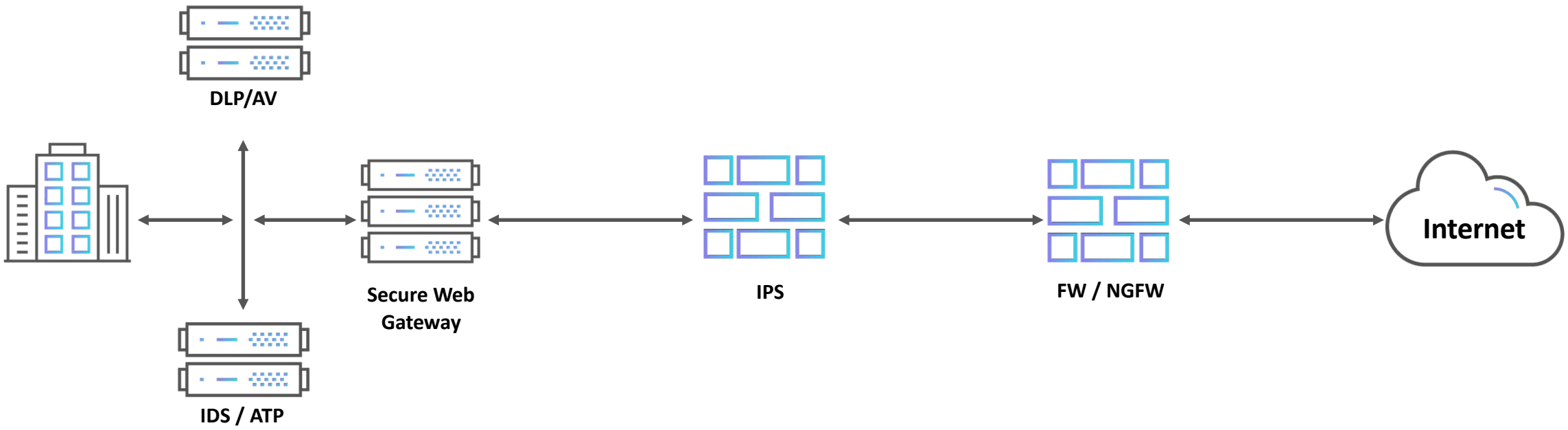
KENNA Security

… Yet we've historically only treated the symptoms

KENNA Security

Traditional Approach to Security

KENNA Security



Problems with this approach

KENNA Security

Reactive

Focuses the majority of our time at the end of the chain

Results in a wide range of disparate tools that don't communicate well with one another

Many attempts to solve the problem

KENNA Security

Assemble a Single Vendor Solution

- Incomplete solution
- Ignores best of breed
- Still doesn't necessarily communicate effectively

Custom Build Through a Systems Integrator or Consultant

- Expensive/time-consuming
- Substandard communication
- Changes/finger pointing/etc.

Employ an Integrated Platform

- Few integrations
- Require expensive PS engagements
- Little value beyond basic correlations

Inherent problems remain!

Still Reactive!

- Late in the process
- End up chasing everything

Inside-out perspective

Predominantly manual

Manual remediation is a never-ending battle

KENNA Security

Complexity Abounds

Multiple patch releases from major vendors, including microcode updates Incompatible Antivirus or Endpoint protection

Massive Array of Devices Affected

Affects Printers, Thermostats, Door Locks, Cameras, Phones, etc.
Intel's Nehalem and Westmere (released in 2008 and 2010) affected

Not Just Patches

Code "should be recompiled with the /Qspectre switch enabled"

Facing the facts

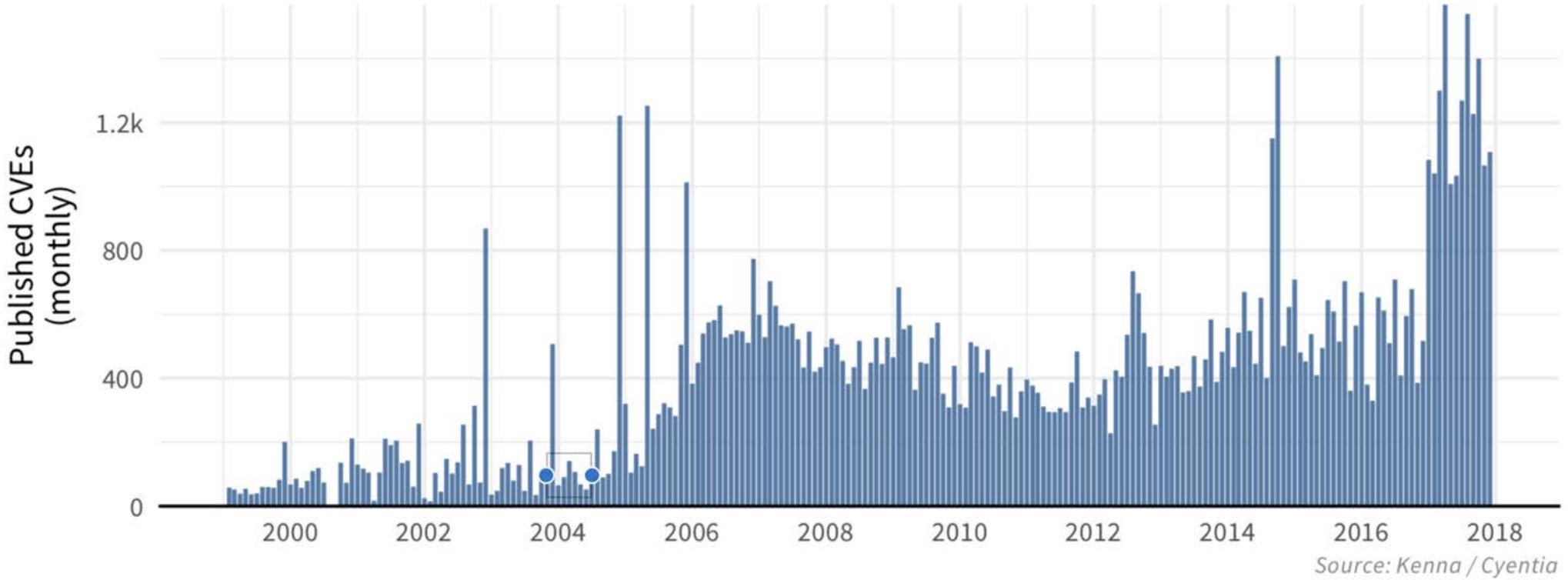
KENNA Security

No matter the size of your organization, you will never have enough human or financial resources to fix everything

Vulnerability volume increasing

KENNA Security

Volume of published CVE's from 1999 through 2017



[1] *For discussion of these biases and other CVE-related issues, see 2013 BlackHat presentation titled "Buying into the Bias: Why Vulnerability Statistics Suck" from Brian Martin and Steve Christy.*

Attacker velocity increasing

Average Days from
Publish to Exploit

(639 / 8%):

19.68 Days

Average Days from
Publish to Event

(36 / 0.5%):

27.36 Days

Shortest Avg Window:
Adobe Reader (days)

Longest Avg Window:
IE Edge (months)

It's a question of focus

KENNA Security

67,354

Threat Events

1,405

Malware Samples

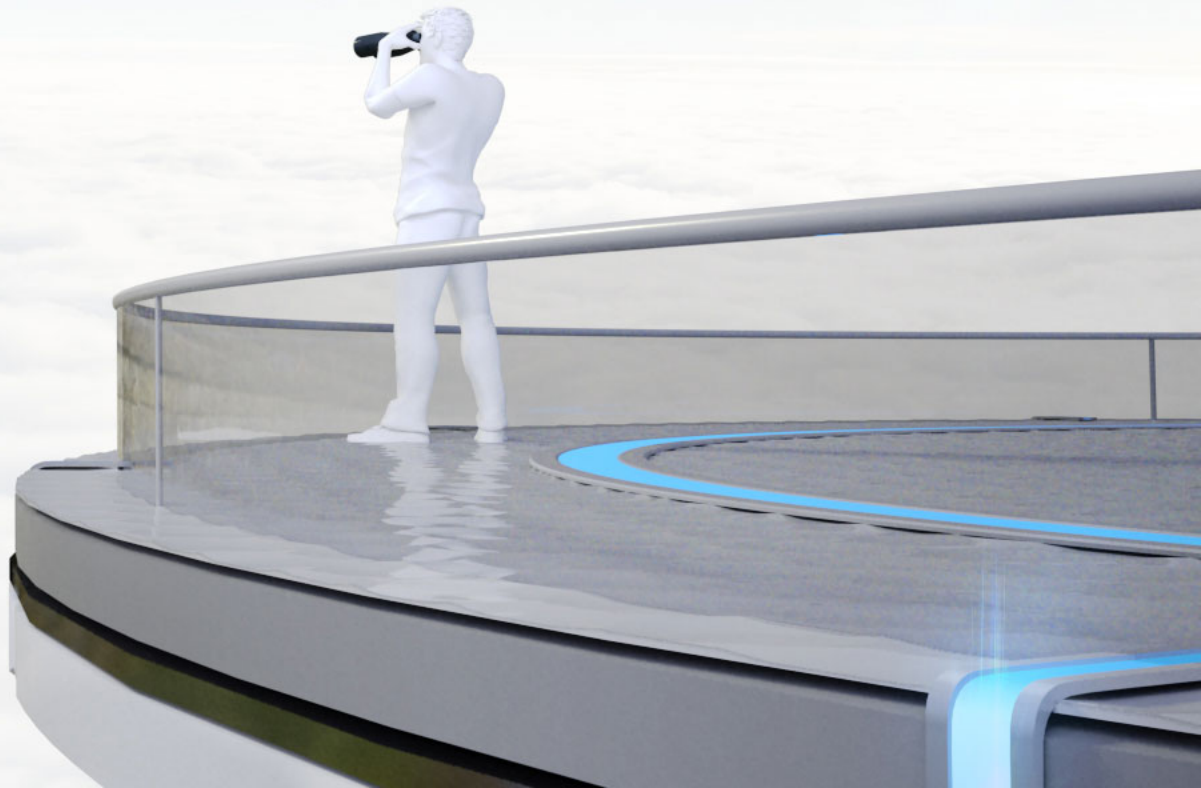
1

Vulnerability

KENNA Security

Applying the Solution

Step 1: Shift Your Focus



Taking a next-generation approach

- *Proactive* Security Posture
  - Focus on the root of the problem
- Comprehensive View
  - Variety of data sources deliver comprehensive insights
  - Strong correlations turn data into intelligence
  - Intelligence sharing improves decision-making and MTTR
- Automated way to understand, correlate, and disseminate
  - Avoid human latency
  - Ensure scalability

Understand: asking the right questions

KENNA Security

Does it Matter?

Is the Indicator Malicious?

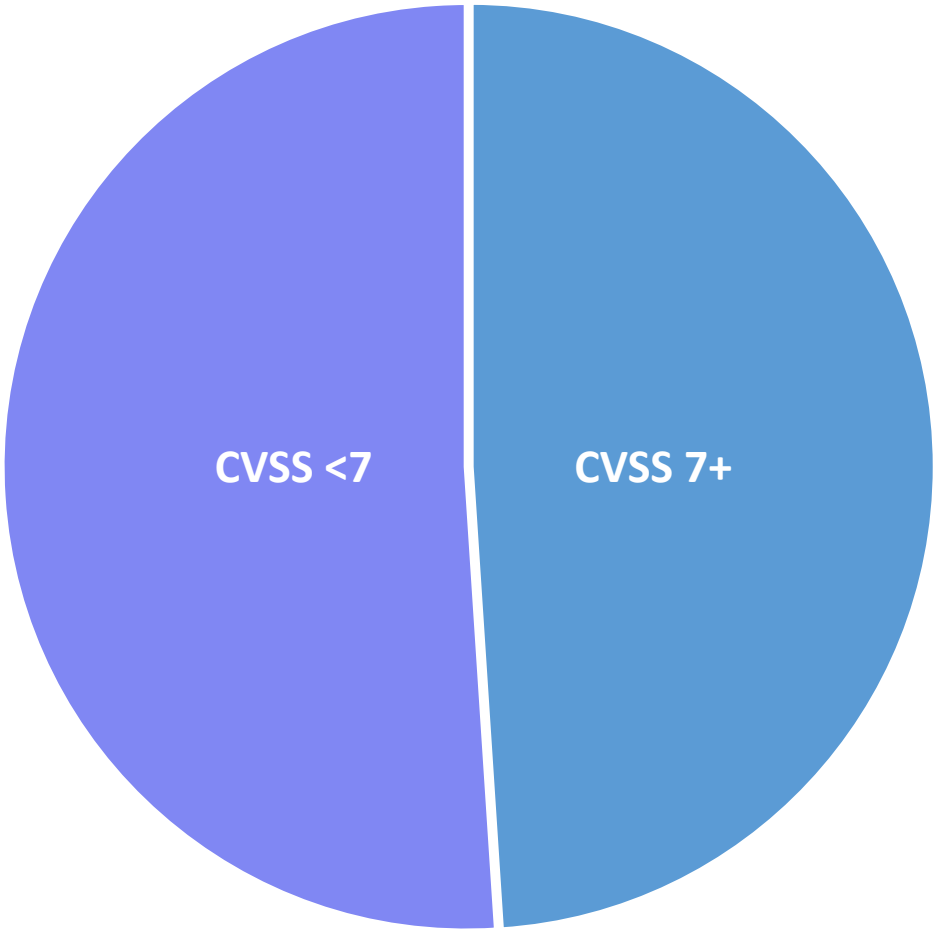
Is a Successful Exploit Likely?

What's the True Risk?

Understand: CVSS alone won't cut it

KENNA Security

1.3% resulted in a breach



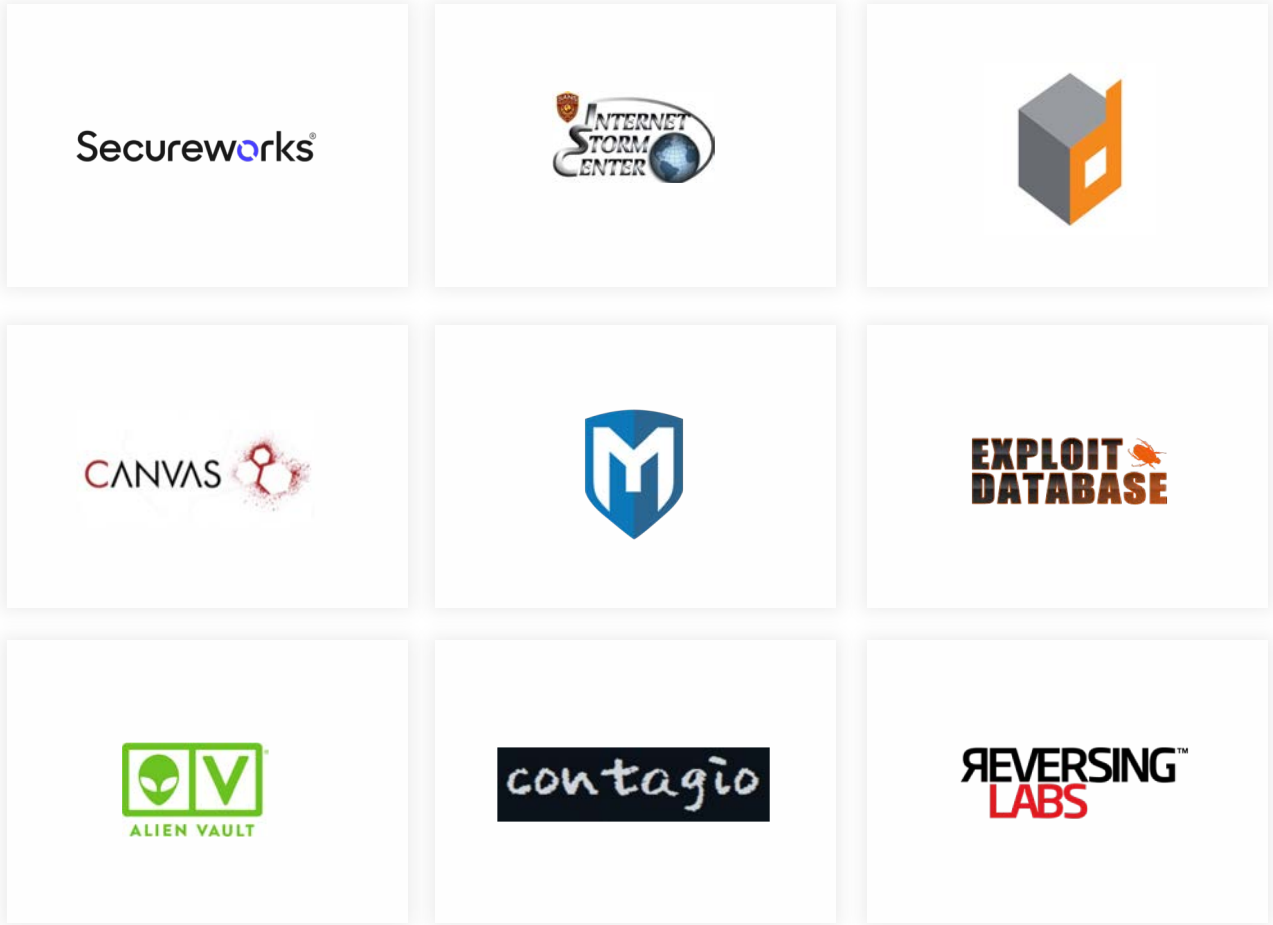
6.9% resulted in a breach

Correlate: Rich data sets from myriad sources

KENNA Security

Correlate: real-time exploit intelligence

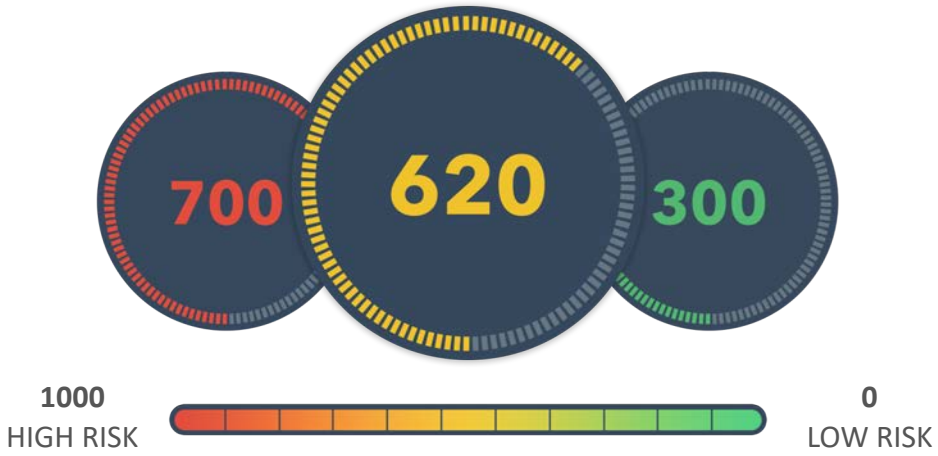
KENNA Security



Correlate: operationalizing intelligence

KENNA Security

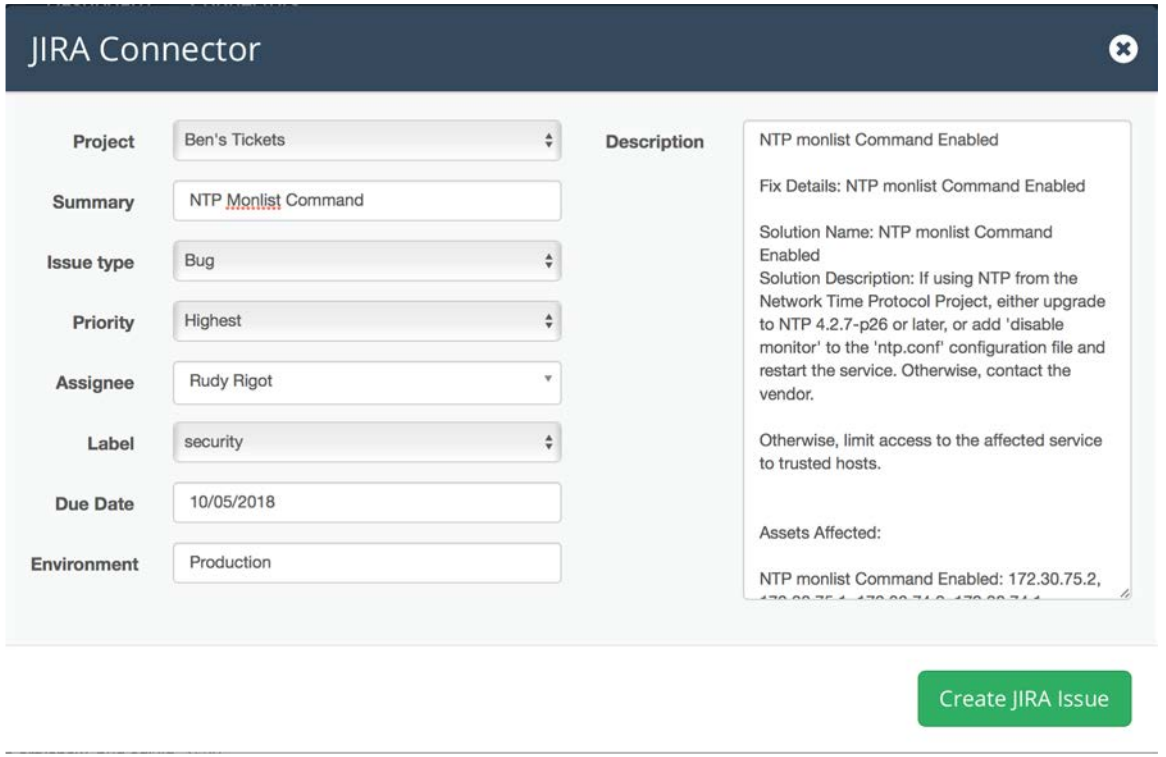
- Match to vulnerabilities, weaknesses or misconfigurations
- Remove duplicate information
- Correlate to (current) fixes



Disseminate: taking action on intelligence

KENNA Security

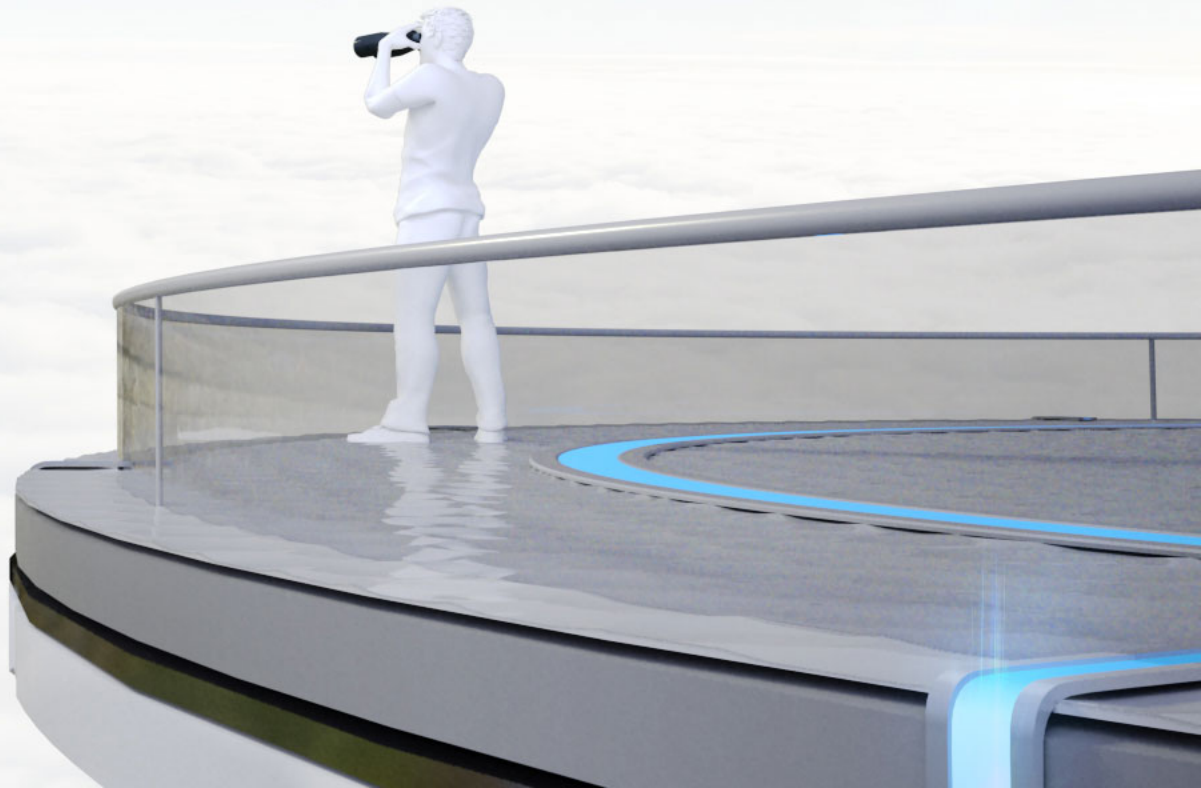
- Integrate with tools used by IT
- Ensure real-time bi-directional communication
- Automate tracking to completion



KENNA Security

Applying the Solution

Step 2: Work Smarter, Not Harder



Real world example

KENNA Security

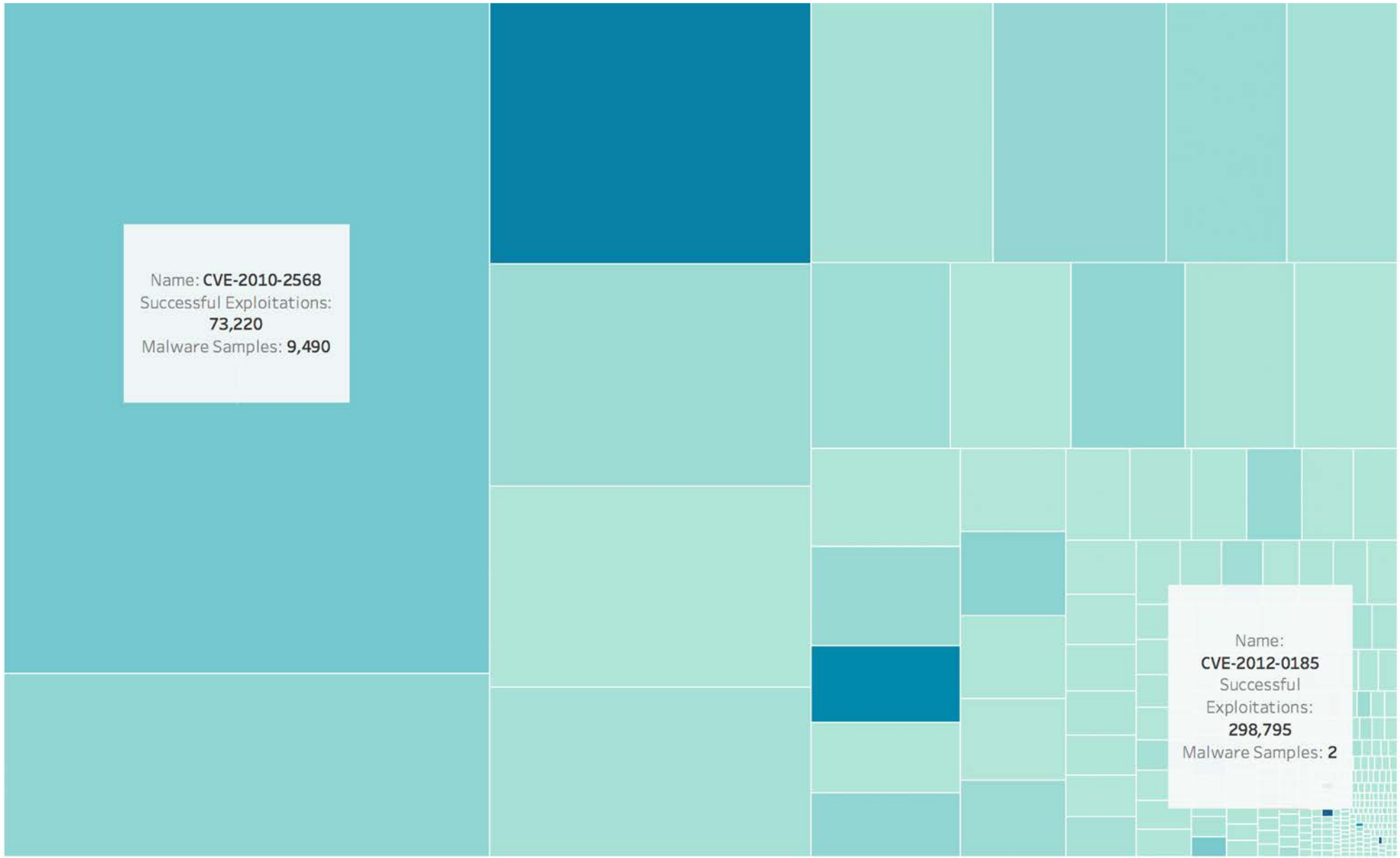
3,200,000
Vulnerabilities

64,200
Malware Exploitable

22,300
Malware + Remote Code

14,100
Malware + RCE + Popular Target

Number of Malware Samples by Vulnerability, Color= Prevalence



KENNA Security

44 MM

Alerts

299

Vulnerabilities

Your choice to make:

KENNA Security

Deal with

44,000,000

Alerts

Or

Fix

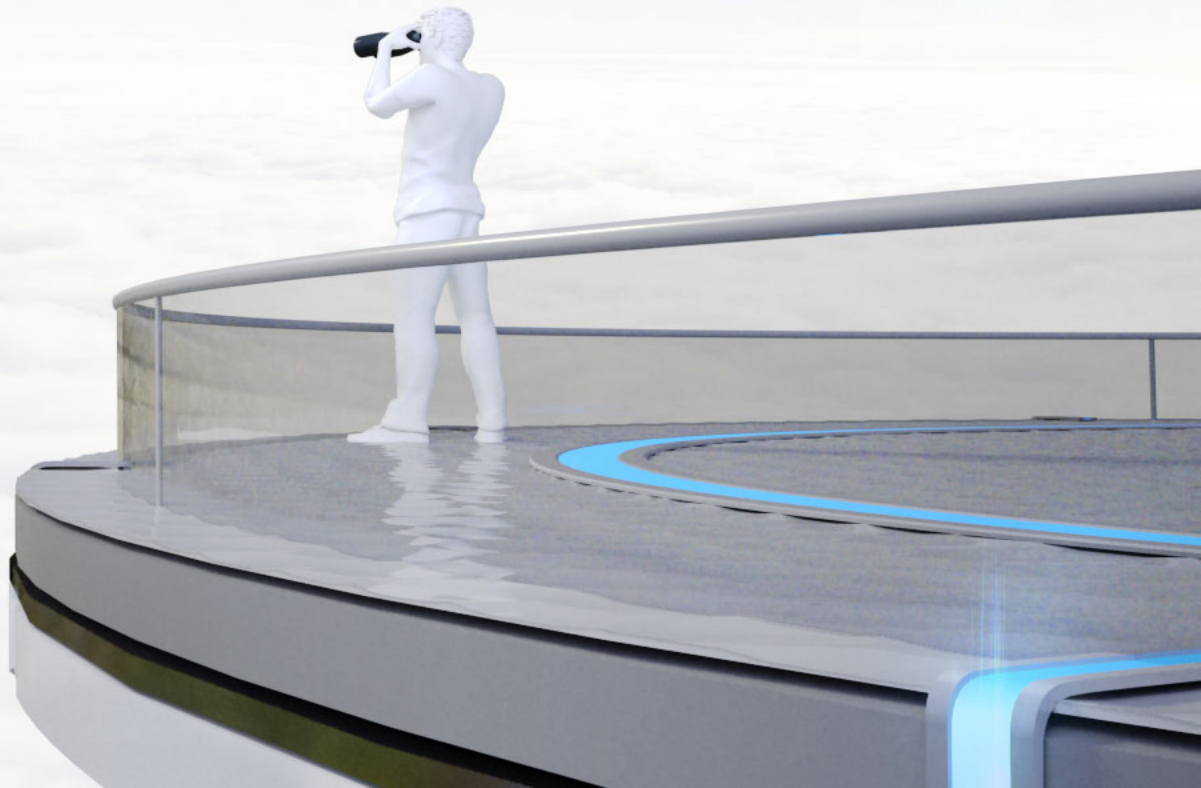
299

Vulnerabilities

KENNA Security

Applying the Solution

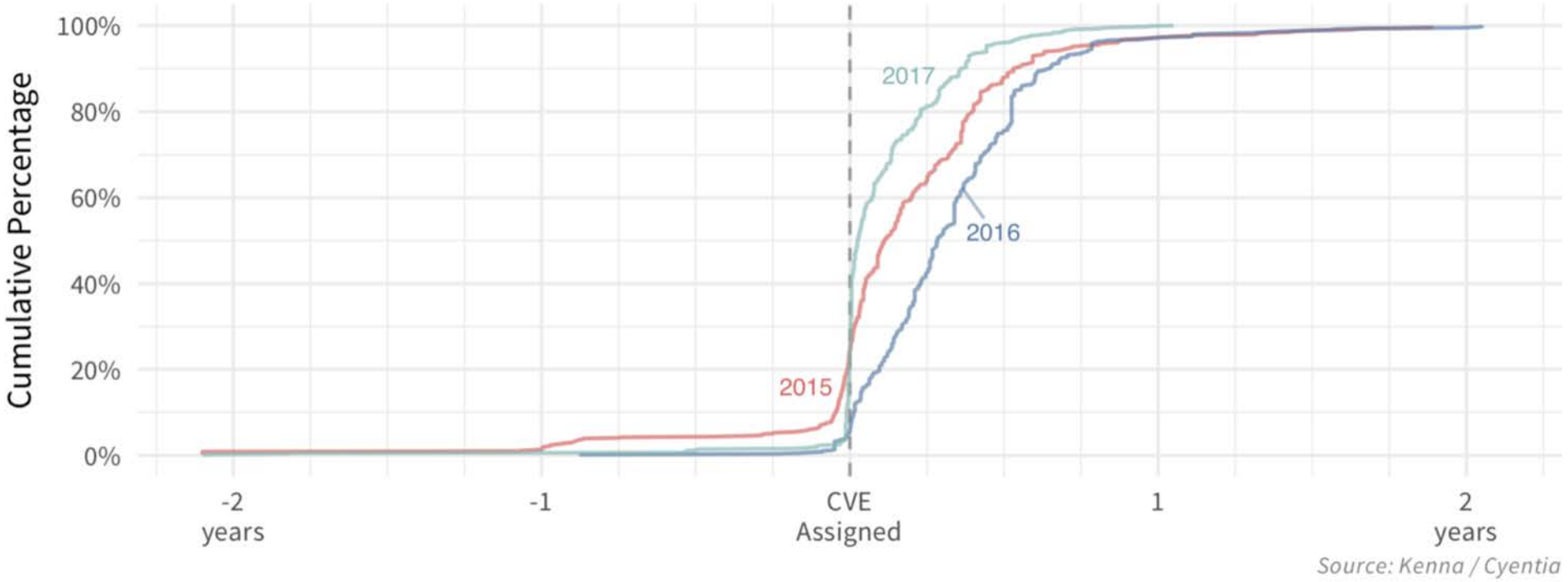
Step 3: Predict the Future



The final step: prediction

KENNA Security

Exploit publication date relative to the CVE *assigned* date (cumulative)



Building a prediction model

KENNA Security

- Employs supervised machine learning to predict public exploit or public event
- Uses random forest vs. many features from vulnerability description and metadata
- Trained on 70% labeled vulnerability data and evaluated on remaining 30%
- Provides a score between 0 and 1. Currently marks predicted at 0.4

Measuring predictive capabilities

KENNA Security

Coverage: Of the vulnerabilities we fixed, did we pick enough to fix?

Efficiency: Of the ones we ended up fixing, did we fix the ones that mattered?

Putting it all together

KENNA Security

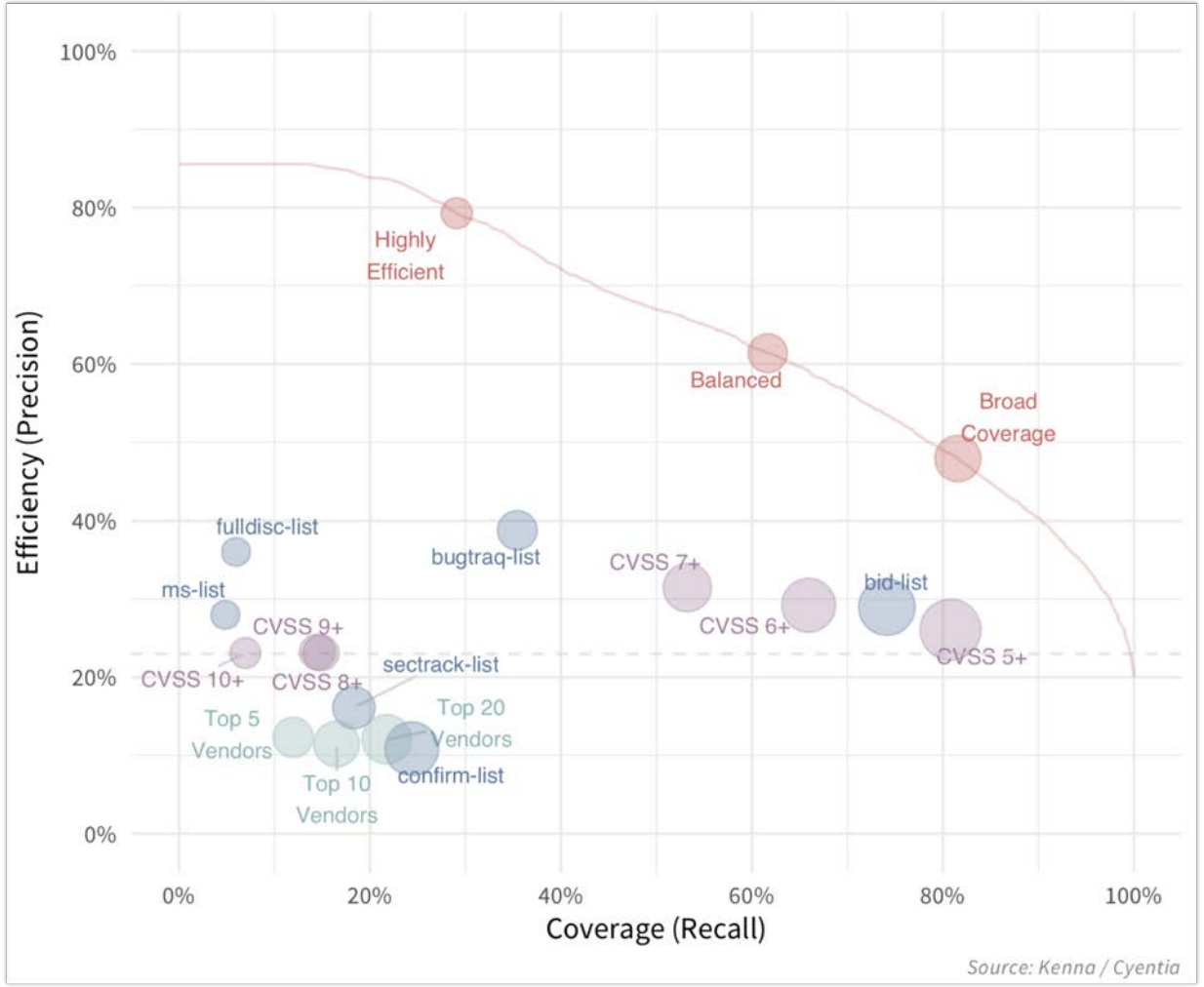
Kenna's Predictive Model

Twice the efficiency
61% vs. 31%

Half the effort
19K vs. 37K CVEs

One-third the false positives
7K vs. 25K CVEs

Better coverage
62% vs. 53%



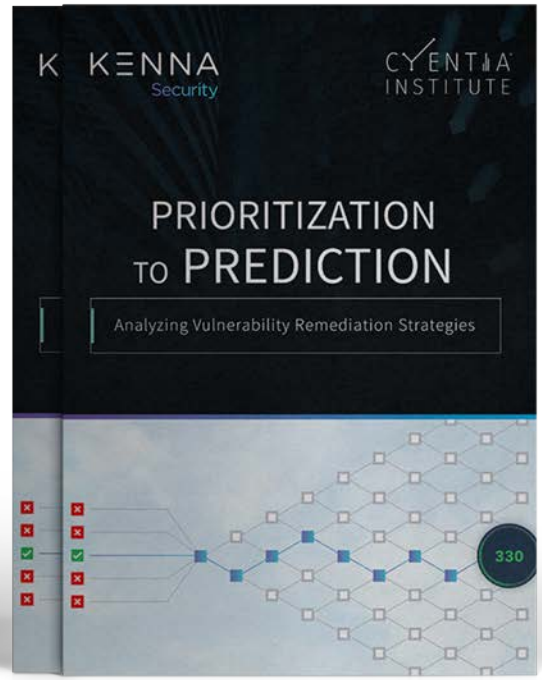
Summary

KENNA Security

- When dealing with a known linear process, you need to assert control
- Cure the source – or be relegated to treating the symptoms forever
- Resources are finite; sadly, vulnerabilities and threats are not
- Don’t waste your time – focus on what will move the needle
- Those who study history are in a better position to control the future

For more information …

- A detailed review of the data sources available
- A discussion of the vulnerability lifecycle
- Identification of the attributes of vulnerabilities
- A measurement of several remediation strategies



https://www.kennasecurity.com/prioritization-to-prediction-report/

KENNA
Security

THANK YOU

jeff.aboud@kennasecurity.com | @jeffaboud