



## *New Features & Products – Feb 2021*

- *PR1ORITY updates*
- *Cloud Security*
- *VPN/Router focused searches*

***Pioneering Artificial Intelligence Delivering  
Real Business Outcomes for Cybersecurity.***



## CYR3CON upgraded features:



### PR1ORITY User Interface

- \* `_sidekick` - **On screen filtering of saved uploads**
- \* Alerts - **Opt-in for daily or weekly alerts**  
(My Account -> Alert Panel)



### PR1ORITY API

Vulnerability Essentials call

- \* **vulnerability metrics from within our collection**

**The newest PR1ORITY Collection can imported at:**

<https://www.postman.com/collections/e0b10b7759684de71af4>





# Vulnerability Essentials API

A search that provides vulnerability metrics from within our collection.

Provides lists of:

- Dates of when discussed by hackers
- Number of times collected
- Number of times discussed by language

```
..{"type": "Vulnerability Essentials",  
.. "message": "SUCCESS",  
.. "results": [  
.....{  
.....  "cve": "cve-2020-1530",  
.....  "smCount": 2,  
.....  "rmtFirstSeen": "2020-08-12",  
.....  "rmtLastSeen": "2020-08-25",  
.....  "rmtUserCount": 3,  
.....  "rmtWebsiteCount": 3,  
.....  "arabicCount": 0,  
.....  "chineseCount": 0,  
.....  "englishCount": 6,  
.....  "russianCount": 0
```

**The newest PR1ORITY Collection can imported at:**  
<https://www.postman.com/collections/e0b10b7759684de71af4>

## New CYR3CON features:



Threat Prediction for the cloud

- \* **CLOUD** \* **New API Collection**

- AWS ECR container vulnerability scanning with CyRating
- AWS Inspector for security assessment service for applications deployed on AWS

- \* **Kubernetes security controller (webhook)**



Router Vulnerability API

- \* **Vulnerability prediction for your network's routers**



VPN Vulnerability API

- \* **A detailed search of specific VPN names or services**

# Machine Learning Threat Prediction for the Cloud





# CYR3CON and AWS



CYR3CON integrates with **AWS ECR** to scan containers and provide vulnerability information to include likelihood of exploit (CyRating).



**Amazon Inspector** performs an assessment and produces a detailed list of security findings, prioritized by level of severity and CyRating. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.



**Kubernetes security controller** determines changes in security and vulnerabilities over specified time span. Allows for custom decision criteria (i.e. indicators, CyRating score) to support decisions in container deployment security.



# Containers: Challenges and Opportunities

Containers have revolutionized dev-ops and represent a major trend for the enterprise

Threat intelligence products are not well-suited for container environments

Decentralization and speed of container deployment make manual security methods ineffective

CISO's will find that current threat intelligence solution will fall short for container security



## Why current threat intelligence falls short.



Current threat intelligence focuses on the analyst, not **automated decision making**



Current threat intelligence provides only data (i.e. "feeds") but does not **make quantified predictions**



Current threat intelligence solutions lack **key integrations and strong API's to automate workflows**





# CYR3CON Supports Automated Decision Making

**CYR3CON combines strong API's with predictive machine learning to allow automated policy-driven response to emerging threats to containers.**

*The CYR3CON API can be easily used to drive decisions about emerging predicted exploitation of the vulnerabilities prior to FireEye releasing a list of the vulnerabilities exploited by its stolen penetration testing tools.*

## **-- Decision Criteria --**

**\* customizable parameters \***  
**CyRating, date periods, indicators**

- ❖ **New vulnerability?**
- ❖ **Change of CyRating within last month?**
- ❖ **Proof of Concept?**
- ❖ **Implemented in a Pentest Framework?**
- ❖ **Exploit in the Wild?**

**Gives decision makers the information they need to make smart decisions about secure container deployment.**

# CYR3CON Predictions in Practice

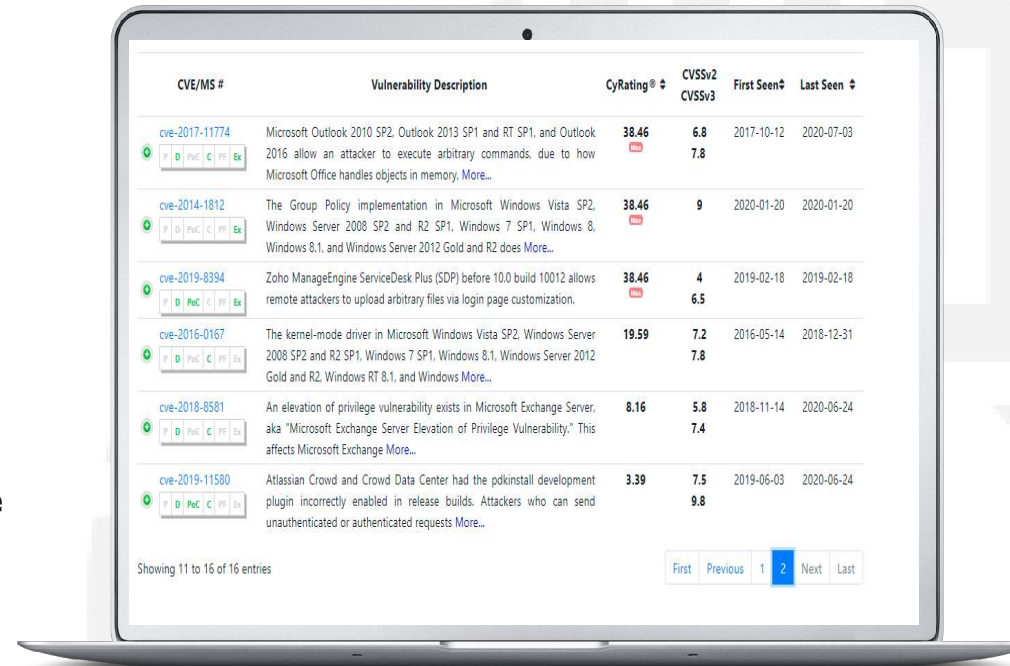


**In December 2020, nation state hackers breached FireEye and obtained cutting-edge tools used to for penetration testing.**

After the attack, FireEye disclosed vulnerabilities used by the tools.

CYR3CON predicted exploitation of all the vulnerabilities months before the disclosure.

*Screenshots at the right show CYR3CON predicted exploitation of the vulnerabilities prior to FireEye releasing a list of the vulnerabilities exploited by its stolen penetration testing tools.*



**Actual CYR3CON predictions on FireEye penetration testing tool vulnerabilities**



# CYR3CON is Predictive

## INTELLIGENCE



What the hackers are saying, who they're talking to, and their reputations



Variety of sources including surface Internet, deep/dark web, and social media



Information includes both white hat and black hat security postings

## ATTACK DATA



Models trained on data of actual exploits used in attacks



Attack data is multi-sourced, meaning it is closer to reality than single-sourced data



Attack data continually updated so models can predict the latest threats

## MACHINE LEARNING



Models leverage state-of-the-art peer reviewed technology, such as knowledge graphs



Over 60 different machine learning models process data to make predictions



Predictions provides as a relative likelihood, allowing for cost analysis of actions

***Machine learning associates intelligence with attack data to make predictions.***





# Cloud is all about assessing costs – intelligence should support these quantifications



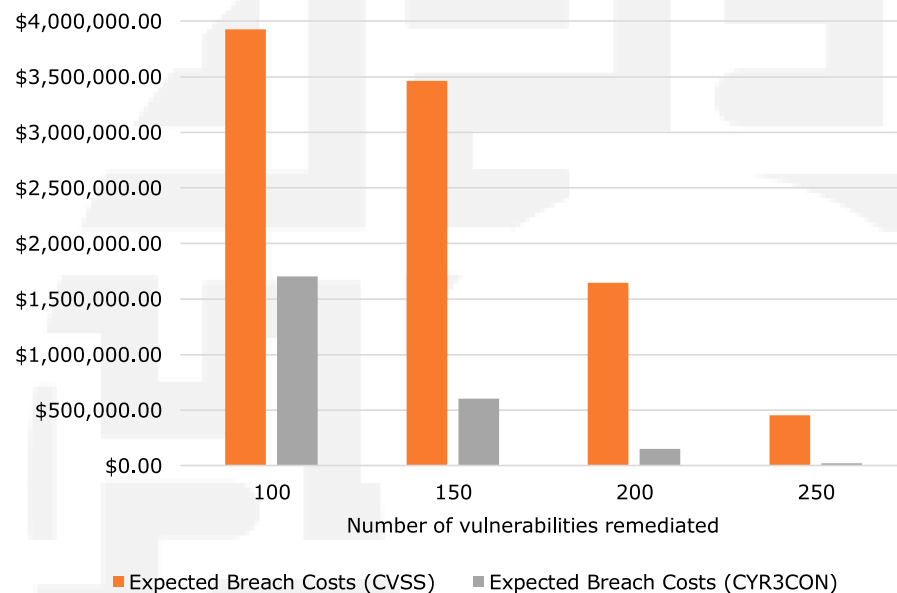
The cloud has allowed for better accounting of computing costs



Customers will need to perform ROI calculations on security cloud resources



By providing probabilistic predictions of exploits, CYR3CON directly supports these calculations



*Actual client analysis*

# CYR3CON supports key Workflows



## CI/CD



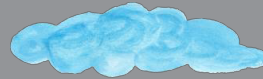
GitHub plugin allows CYR3CON to be used in the development environment



CYR3CON constantly collects intelligence on opensource platforms and libraries



Attack data continually and dynamically updated – track threats post-deployment



## INFRASTRUCTURE PROTECTION



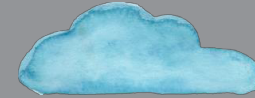
CYR3CON routinely predicts threats to container infrastructure



Early warnings provided by CYR3CON allow teams to better plan infrastructure upgrades



Get info on hacker interest in misconfigurations through CYR3CON API's



## WORKLOAD PROTECTION



Direct integration with Kubernetes through webhooks

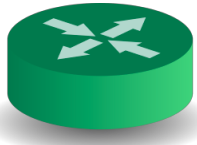


CVE-based exploit prediction works with any major vulnerability scanner



Robust REST API and Python SDK already in use by multiple OEM's





# Router Vulnerability API

Provides vulnerability information on routers located within your network.

Based off network scan of your environment.

Provides:

- Protocol and Port ID
- Product and version
- CVE ID and CyRating
- Indicators (PoC, Code posted, Pentest Framework, Exploited)
- NIST CVSS ranking
- Recent posts

| Protocol | Port ID | Name   | Product      | Version | OSType | CVE ID        | PoC  | Code Posted | Pentest Framework | Exploit in the Wild | CyRating | firstSeen | lastSeen   | CVSSV2 | CVSSV3 | PoC Link1                                                               | Pentest Link                                | Exploit Link1                               | Recent post1  |
|----------|---------|--------|--------------|---------|--------|---------------|------|-------------|-------------------|---------------------|----------|-----------|------------|--------|--------|-------------------------------------------------------------------------|---------------------------------------------|---------------------------------------------|---------------|
| tcp      | 80      | http   | Apache httpd | 2.2.8   |        | cve-2017-9798 | TRUE | TRUE        | FALSE             | TRUE                | 38.46    | 9/18/2017 | 12/15/2020 | 5      | 7.5    | <a href="https://old.exploit-db.com/">https://old.exploit-db.com/</a>   | <a href="https://exchai">https://exchai</a> |                                             | 前言面对高         |
| tcp      | 80      | http   | Apache httpd | 2.2.8   |        | cve-2017-9788 | TRUE | TRUE        | FALSE             | TRUE                | 38.46    | 7/31/2017 | 12/15/2020 | 6.4    | 9.1    | <a href="https://nvd.nist.gov/vuln/fu">https://nvd.nist.gov/vuln/fu</a> | <a href="https://exchai">https://exchai</a> |                                             | 前言面对高         |
| tcp      | 53      | domain | ISC BIND     | 9.4.2   |        | cve-2011-1910 | TRUE | TRUE        | FALSE             | TRUE                | 38.46    | 5/31/2011 | 7/12/2020  | 5      |        | <a href="https://nvd.nist.gov/vuln/fu">https://nvd.nist.gov/vuln/fu</a> | <a href="https://exchai">https://exchai</a> |                                             | Source BUGTR  |
| tcp      | 80      | http   | Apache httpd | 2.2.8   |        | cve-2011-3368 | TRUE | TRUE        | TRUE              | TRUE                | 38.46    | 10/6/2011 | 7/5/2020   | 5      |        | <a href="https://packe">https://packe</a>                               | <a href="https://www.">https://www.</a>     | <a href="https://exchai">https://exchai</a> | Source Bugtra |
| tcp      | 53      | domain | ISC BIND     | 9.4.2   |        | cve-2012-1667 | TRUE | TRUE        | FALSE             | TRUE                | 38.46    | 6/6/2012  | 7/5/2020   | 8.5    |        | <a href="https://nvd.nist.gov/vuln/fu">https://nvd.nist.gov/vuln/fu</a> | <a href="https://exchai">https://exchai</a> |                                             | Source BUGTR  |



# VPN Vulnerability API

A search that provides information on the desired VPN name or service.

Focused on hacker discussion  
(dark & deep web, social media)

Provides lists of:

- Dates of when discussed by hackers
- Associated CVEs and CyRatings

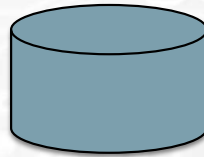
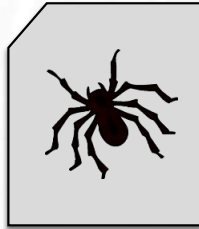
```
"type": "VPN Information",
"message": "SUCCESS",
"results": [
  {
    "dates": [
      "2021-01-18",
      "2021-01-19",
      "2021-01-21",
      "2021-01-24",
      "2021-01-25",
      "2021-01-27",
      "2021-02-03"
    ],
    "cve": "CVE-2017-17410",
    "vpnName": "bitdefender"
  }
]
```



# Automated Collection at Scale

**CYR3CON infrastructure collects hacker discussions at scale.**

***Social media, deepweb, darkweb, chan sites, paste sites, OSINT, security websites, repositories, etc.***



**1,000+  
sources**

**Millions of  
OSINT  
pages per  
day**

**170,000+  
deepweb/  
darkweb  
posts per  
day**

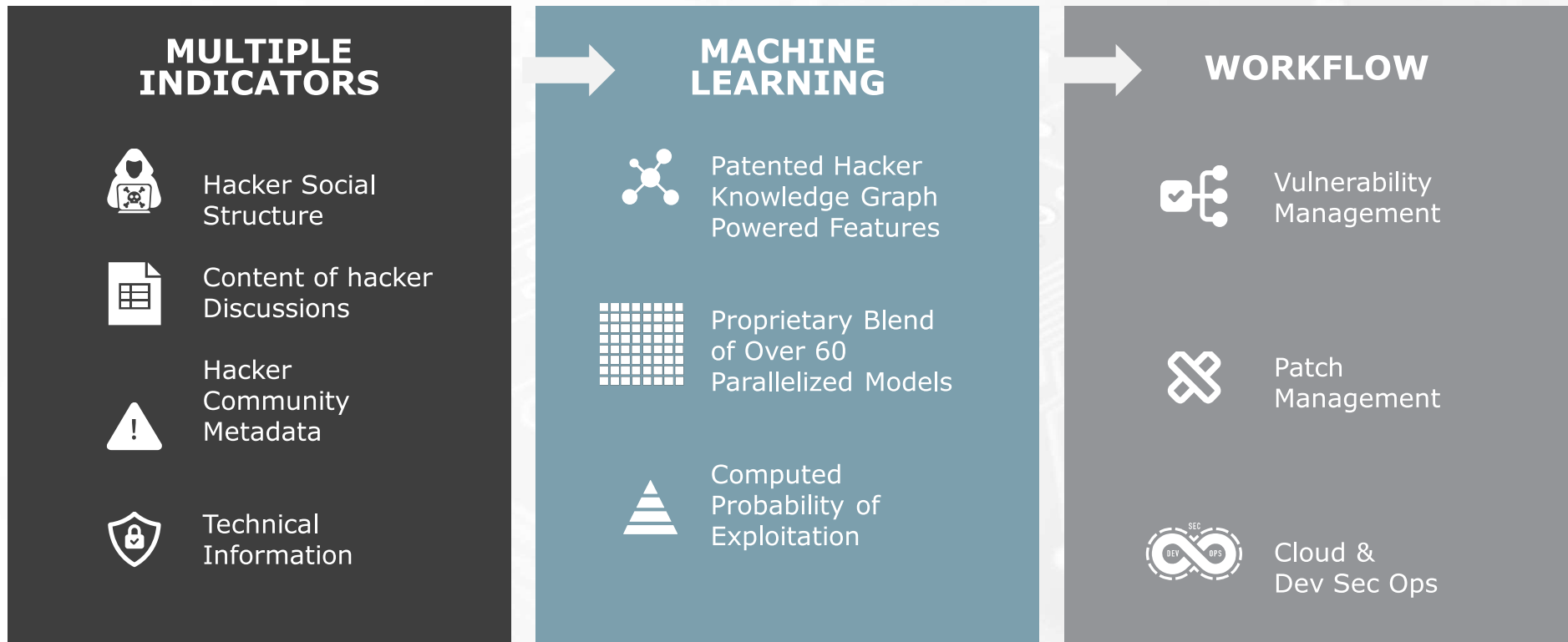
**80,000+  
social  
media  
posts per  
day**

**CYR3CON-owned data collection.  
Data collected by 100% legal means.  
Existing European customers.**





# Highly Accurate Machine Learning





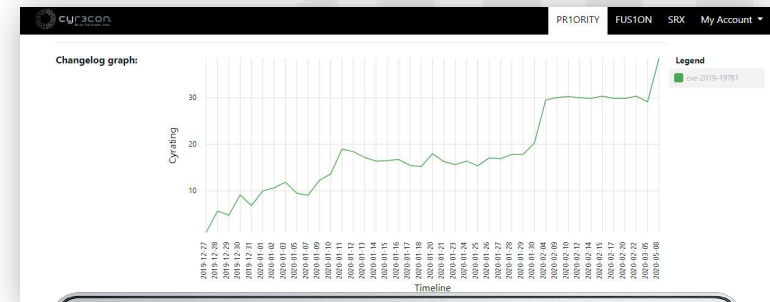
# Example Case Study: CozyBear and COVID-19 Research



**In July, 2020, Russian hacking Group, CozyBear is actively exploiting multiple vulnerabilities to steal US and UK COVID-19 related research data.**

All were predicted by CYR3CON in 2019

*Screenshots at the right show CYR3CON predicted exploitation of the vulnerabilities prior to this attack.*



PRIORITY

Enter your keywords here

default view custom view

most recent most severe NIST low score sidekick Analysis

| CVE/MS #       | Vulnerability Description                                                                                                                                                                 | CyRating# | CVSSV2 | CVSSV3 | First Seen | Last Seen  |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|--------|--------|------------|------------|
| cve-2019-10781 | An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.                                     | 38.46     | 7.5    | 9.8    | 2019-12-17 | 2020-07-08 |
| cve-2019-11510 | In Pulse Secure Pulse Connect Secure (PCS) before 8.1R15.1, 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthorized remote attacker can send a More...           | 38.46     | 7.5    | 10     | 2019-08-21 | 2020-07-08 |
| cve-2019-13379 | An improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") in Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12 under SSL VPN web portal More... | 38.46     | 5      | 9.8    | 2019-08-14 | 2020-06-12 |
| cve-2019-9670  | mailbox component in Synacor Zimbra Collaboration Suite 8.7.x before 8.7.11p10 has an XML External Entity injection (XXE) vulnerability.                                                  | 38.46     | 7.5    | 9.8    | 2019-03-13 | 2019-03-13 |

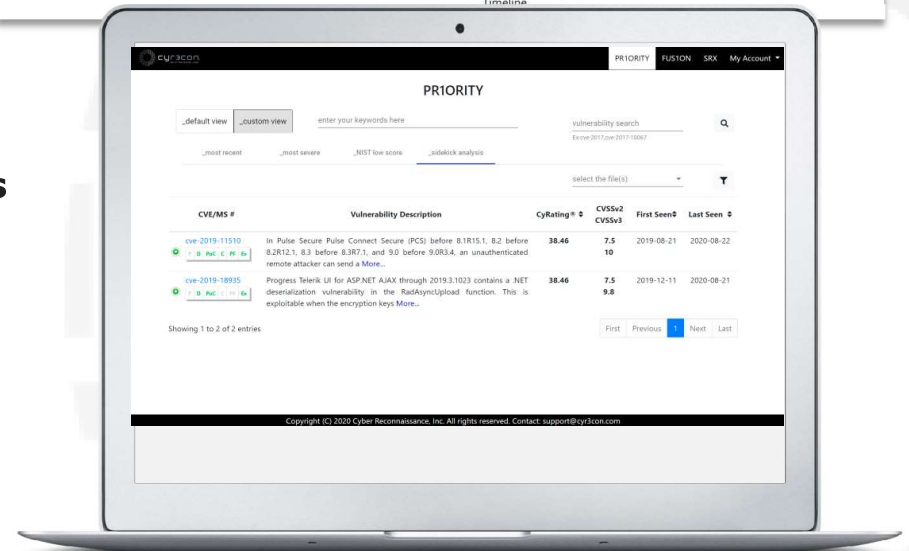
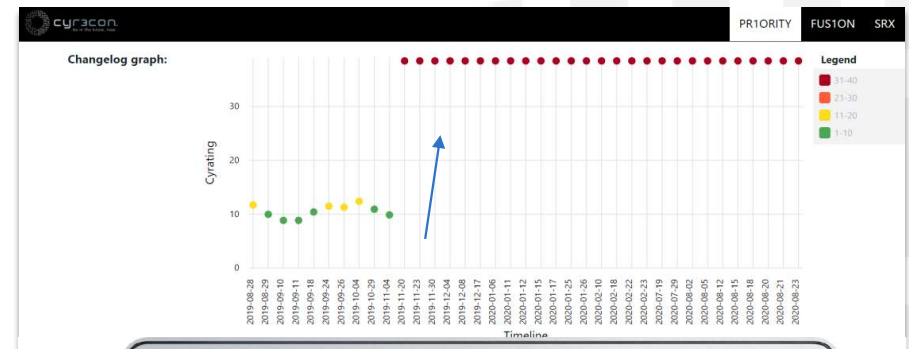
# Example Case Study: NetWalker Ransomware



**In August 2020, the University of Utah paid hackers \$457,000 due to a ransomware attack.**

The vulnerabilities used by the hackers were predicted by CYR3CON month prior to the attack

*Screenshots at the right show CYR3CON predicted exploitation of the vulnerabilities prior to this attack.*



# Why **CYR3CON**?

## Proven Prediction

- Backed by peer-reviewed research and government funded studies
- Predictive results of significant events featured in The Economist, CNN, and others
- Customer validation with 100% annual subscription renewals

## Attacker Focused

- Unique data collection infrastructure built and owned by CYR3CON
- Data collected from 1,000+ hacker sources
- Proprietary automated crawling and cleansing technology

## Transparent Results

- CYR3CON's data collection platform enables the inclusion of hacker discussions as evidence supporting threat prediction
- Ability to support predictions with data (i.e. hacker discussions) enables teams to justify expensive prevention and remediation efforts

## Ease of Deployment and Operation

- Flexible deployment methodologies (web UI, REST-based API, Python SDK)
- Rapid deployment, leverages industry standards like NIST

## Scalability

- Currently supporting global multiple Fortune 100 enterprises
- Over 400,000 endpoints supported in largest customer