PreTA

Predictive Threat Assessment

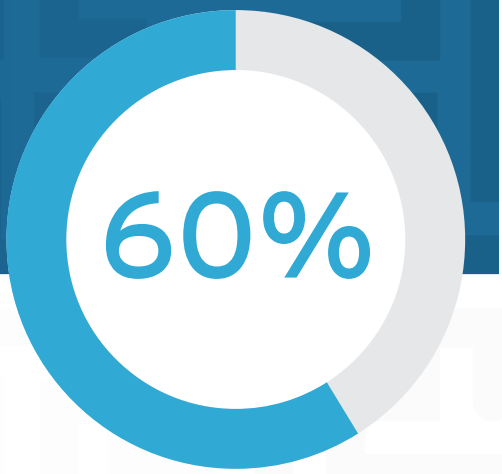
Vulnerability Assessment Available from CYR3CON

Predict hacker-targeted CVEs in your organization with CYR3CON PR1ORITY

cyr3con®
be in the know, now.

A key challenge facing cybersecurity professionals today is the ever-expanding number of software vulnerabilities.

An incredible 60% of enterprises are breached due to **known unsecured systems** they didn't secure.



Source: 2019 Cost and Consequences of Gaps in Vulnerability Response (Ponemon) (ponemon-state-of-vulnerability-response.pdf)

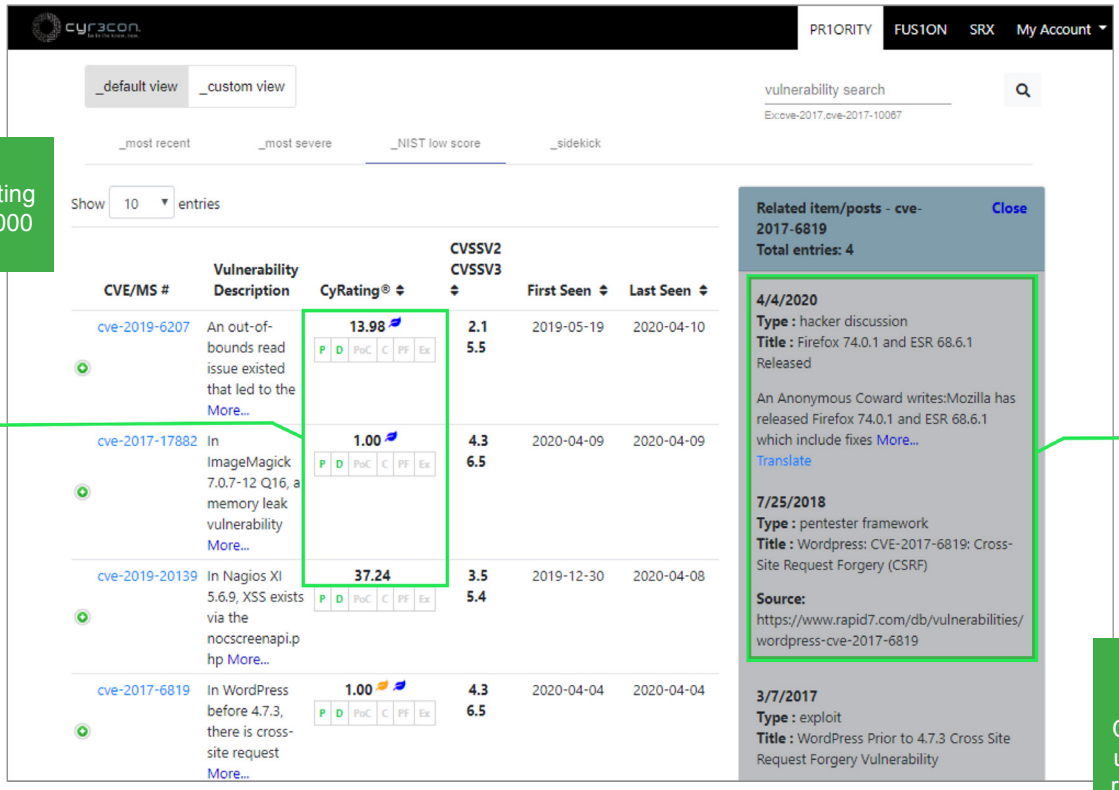
The world's top vulnerability management teams address this problem using intelligence analysts to research vulnerabilities – manually making the call on what hackers are likely to exploit.

CYR3CON PR1ORITY automates the process – enabling you to analyze all vulnerabilities at scale – and in the process finding threats your vulnerability management team may not be remediating.

CYR3CON PR1ORITY approaches cybersecurity from the hacker's world view, identifying real threats to your assets based on attacker behaviors.

Identify Unknown Threats To Your Vulnerabilities

Prioritizing patching of CVSS “critical” and “high” vulnerabilities is common practice, but hackers still exploit “medium” and “low” severity vulnerabilities in the wild (think HeartBleed). **CYR3CON PR1ORITY** identifies all vulnerabilities, regardless of CVSS category, that have piqued hackers’ interest and helps ensure you properly PR1ORITY-ize them based on threat - even when it is where most enterprises may least expect.



Scales
Currently supporting clients with 350,000 endpoints

CyRating® 86% precision
3% for CVSS

Intelligence Driven
Over 1,000 sources easily organized

Supports Decisions
Customers routinely use results to justify resources endpoints

PR1ORITY identifies the vulnerabilities you should be paying attention to – not just those identified as critical or high. Justify the expense and showcase the value of vulnerability management up and down the management chain within your organization.

Scale the Analytical Process

You're concerned that different vulnerabilities pose unique real-world risk for the varied mix of platforms, devices, and applications in your enterprise. **CYR3CON PR1ORITY** enables enterprise scale threat research using objective AI backed by world-wide hacker community data. With **CYR3CON PR1ORITY** (available via web-based, REST API, or on-prem solutions) you can rapidly query, prioritize, and get updates on any vulnerabilities of concern.

Prioritize Remediation

Focus your teams on the specific and likely vulnerabilities that need attention, rather than the ever-growing list of possibilities.

You're prioritizing vulnerability scan results, and by CVSS score, which is common industry practice. But you've still got a lot of work to do. Studies show that only a fraction of vulnerabilities are actually exploited-in-the-wild. **CYR3CON PR1ORITY** uses peer-reviewed attacker-focused AI to determine which vulnerabilities are most likely to be targeted.

Use PR1ORITY to go through your scan results and prioritize based on real-world threat. Once PR1ORITY identifies the vulnerabilities most likely to be exploited, use PR1ORITY to determine if and where a patch is available.

Vulnerability Management with CYR3CON PR1ORITY

Client Case Study

A large financial institution recently underwent a Predictive Threat Assessment with CYR3CON, revealing several vulnerabilities with known threats. In this case study, we highlight one such vulnerability.

Here we see OpenSSL vulnerability CVE-2018-5407. It had a low/medium rating by the NIST CVSS scoring system, so it was not prioritized for remediation.

However, after a single mouse click, CYR3CON PR1ORITY identified significant threats to this vulnerability. CYR3CON's patent-pending machine learning powered CyRating® raised the attention immediately to the team and revealed that not only had the vulnerability been exploited in the wild, but there was an available proof-of-concept code and numerous pieces of threat intelligence from various hacker communities discussing the availability of an exploit.

Here, as with many other customers, CYR3CON PR1ORITY was able to predict targeted vulnerabilities.

An Overlooked Threat - Found.

CVE/MS #	Vulnerability Description	CyRating®	First Seen	Last Seen
cve-2018-5407	Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.	38.46 P D PoC C PF Ex	2018-11-06	2019-06-02

- NIST rating was medium/low
- CYR3CON's machine learning & intelligence driven CyRating® was much higher - over 38 times more likely for exploitation
- Supporting intelligence is provided and shown below

CVSS V2 – 1.9 Low
CVSS V3 – 4.7 Medium

Intelligence: -уязвимость в smt/hyper-threading, позволяющая определить ключи шифрования чужих процессов уязвимость в smt/hyper-threading, позволяющая определить ключи шифрования чужих процессов тгруппа исследователей из университета технологий в тампере (финляндия) и гаванского технологического университета (куба) продемонстрировали уязвимость (cve-2018-5407) в технологии одновременной многопоточности (smt или hyper-threading) на примере процессоров intel...

In-system translation: vulnerability in smt/hyper-threading, allowing to determine the encryption keys of other people's processes, a group of researchers from the University of Technology in Tampere (Finland) and the Havana University of Technology (Cuba) demonstrated a vulnerability (cve-2018-5407) in the technology of simultaneous multi-threading (smt or hyper-threading) on the example of intel processors...

Automatic translation of non-English threat intelligence provided in-platform.

Take advantage of the **CYR3CON PR1ORITY** Predictive Threat Assessment (PreTA) from the industry's most accurate predictive scorer of weaponized exploits today.

CYR3CON PR1ORITY

Predict hacker-targeted CVEs in your organization

One week access to CYR3CON's web based platform

Assessment report produced by CYR3CON personnel highlighting your predicted threats

Second training session to review identified threats and learn how to best communicate results to IT and management

Initial virtual instructional session -learn how the world's top vulnerability management teams use CYR3CON to get ahead of threats

A kick-off meeting with the CYR3CON team to help you understand the tool and the meaning of the indicators to get you started with the information you need to begin re-prioritizing your patching program.

CYR3CON will provide access to the **CYR3CON PR1ORITY** platform and an example analysis of your vulnerabilities to **identify vulnerabilities predicted to be targeted by hackers**. You will be able to use the CYR3CON platform as well as benefit from the assessment produced by the CYR3CON team based on the best-practices of vulnerability management we've learned while deploying CYR3CON technology to some of the world's top vulnerability management teams.

CYR3CON will then provide an out-brief to you and your team – highlighting the predicted threats and showing how the platform can be leveraged to produce the result. We also show how to showcase the results to management or IT personnel to justify the needed resources to avoid threats.

The Predictive Threat Assessment requires no effort on your part!

- Provide CYR3CON with a anonymized list of vulnerabilities (just CVE's, no IP addresses or endpoint information)
- Be sure to include vulnerabilities that you aren't currently remediating – full scan results are preferred
- Week-long platform access usage is optional – you get your assessment results regardless

Ready to start?

Sign Up Now

Predictive Threat Assessment

3 week difference in scan reassessment

July assessment

CVE ID	Proof of Concept	Malware Code	Pentest Framework Module	Exploit in the Wild	**CyRating**	CVSSV2	CVSSV3
cve-2018-XXXX	✓			✓	**38.46**	6.9	7
cve-2019-XXXX	✓			✓	**38.46**	4.3	6.5
cve-2017-XXXX				✓	**38.46**	4.3	6.5
cve-2019-XXXX					**38.46**	4	6.5
cve-2017-XXXX				✓	**38.46**	4.3	5.9
cve-2019-XXXX				✓	**38.46**	2.1	5.5
cve-2016-XXXX				✓	**38.46**	2.6	5.3
cve-2017-XXXX					**38.46**	4.3	4.3
cve-2014-XXXX		✓			**38.46**	4.3	3.4
cve-2020-XXXX					**38.46**	3.5	5.4

While the initial assessment shows the value of PR1ORITY through the identification of vulnerabilities likely to be targeted, the predictive ability of the platform becomes evident in the August re-assessment. All the additional checkmarks in yellow were additional indicators that appeared after PR1ORITY published the CyRating score, highlighting the correct prediction by the platform.

August re-assessment

CVE ID	Proof of Concept	Malware Code	Pentest Framework Module	Exploit in the Wild	**CyRating**	CVSSV2	CVSSV3
cve-2018-XXXX	✓			✓	**38.46**	6.9	7
cve-2019-XXXX	✓	✓		✓	**38.46**	4.3	6.5
cve-2017-XXXX		✓		✓	**38.46**	4.3	6.5
cve-2019-XXXX	✓	✓		✓	**38.46**	4	6.5
cve-2017-XXXX				✓	**38.46**	4.3	5.9
cve-2019-XXXX				✓	**38.46**	2.1	5.5
cve-2016-XXXX		✓		✓	**38.46**	2.6	5.3
cve-2017-XXXX				✓	**38.46**	4.3	4.3
cve-2014-XXXX	✓	✓	✓	✓	**38.46**	4.3	3.4
cve-2020-XXXX				✓	**38.46**	3.5	5.4

Web

https://cyr3con.ai

Send us an e-mail

sales@cyr3con.com

cyr3con. be in the know, now.