

Blue Team Level 1 Certification
(Standard)

7 Topics

Security Controls

5 Topics 1 Quiz

Networking 101

6 Topics 1 Quiz

Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

PA2) Types of Phishing Emails

10 Topics 2 Quizzes

PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

PA6) Taking Defensive Actions

12 Topics 1 Quiz

PA7) Report Writing

7 Topics 1 Quiz

PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

T11) Introduction to Threat Intelligence

7 Topics

Section Introduction, Threat Intelligence

Threat Intelligence Explained

Why Threat Intelligence can be Valuable

Types of Intelligence

[The Future of Threat Intelligence](#)

Further Reading, Threat Intelligence

Threat Intelligence Glossary

T12) Threat Actors & APTs

6 Topics 2 Quizzes

T13) Operational Threat Intelligence

7 Topics 1 Quiz

T14) Tactical Threat Intelligence

7 Topics 1 Quiz

T15) Strategic Threat Intelligence

5 Topics 1 Quiz

T16) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN

DF1) Introduction to Digital Forensics

5 Topics

DF2) Forensics Fundamentals

10 Topics 5 Quizzes

DF3) Digital Evidence Collection

The Future of Threat Intelligence

Blue Team Level 1 Certification (Standard) > T11) Introduction to Threat Intelligence > The Futur...

IN PROGRESS

Threat Intelligence THE FUTURE OF THREAT INTEL

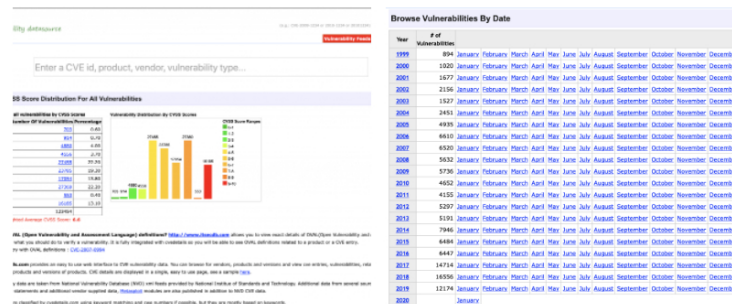


Threat intelligence is ever-changing. One big step forward in the threat intelligence and vulnerability management world is the development of **predictive prioritization** by Tenable, the company behind the Nessus vulnerability scanners and auditing tools. Before we cover it, we need to set the scene and introduce some vulnerability management basics as it is out of scope for this course.

CVEs AND CVSS SCORES

What are CVEs?

- CVEs (common vulnerabilities and exposures) are a method of uniquely tracking publicly-reported vulnerabilities. If someone finds a vulnerability in the Windows operating system, they'll report it and apply for a CVE. If granted, a CVE value is generated based on the year and the number of the vulnerability. An example of this is CVE-2019-0708 which was a critical vulnerability in the Remote Desktop Protocol (RDP) in 2019. Using CVEs makes sharing information easier – you can simply provide someone with a CVE number, and they can lookup the ID and find all the information they need (provided it has been published). Revisiting [CVE-2019-0708](#), you can view information about this specific vulnerability by visiting the [National Vulnerability Database](#) offered by NIST (just click the CVE number in this sentence!).
- <https://cvedetails.com> is a security vulnerability database that has lots of information, and can allow us to search for specific CVEs, or even look at vulnerabilities sorted by release date.



What are CVSS scores?

- Example CVSS rating: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H.



This is the Common Vulnerability Scoring System, used to help rank vulnerabilities based on their attributes. Whilst this may look like some confusing code, it's actually fairly simple. **Base Score: 8.8 HIGH** tells us that this vulnerability has a high severity. The idea behind these scores is that it provides value at a glance, so you can look at the score and immediately tell if this vulnerability is bad. Obviously, this is a generic score, and what may be a critical vulnerability for one company may not affect another company at all – it all depends on the products and versions you're using, the security controls you have in place, and a number of other factors, so this score should only be taken as a

the security controls you have in place, and a number of other factors, so this score value should only be taken as a generic guideline.

VULNERABILITY CONTEXT

The issue with CVSS scores is that a vulnerability which may be rated 10.0 CRITICAL might not actually affect some organizations, as it depends on the technology that is being used. A vulnerability in Solaris systems isn't going to affect a company that uses only Windows systems.

Another issue is that whilst some vulnerabilities could be very damaging if executed correctly, hackers might not actually bother trying to exploit them due to factors such as technical complexity. If no threat actors are exploiting a critical-rated vulnerability, then there is less of a risk than a high-rated vulnerability which is actively being exploited in the wild (a term used to describe activity across the internet).

It's all about context and tracking exploitation activity to determine the prioritization rating for the organization. But the guys and girls over at Tenable have had a very clever idea.

PREDICTIVE PRIORITIZATION

Tenable claims that predictive prioritization will help "focus first on the security issues that matter most". Predictive Prioritization combined vulnerability data with threat intelligence to provide context, and generate new scores that consider which vulnerabilities are most likely to actually be exploited. The new scoring system, named Vulnerability Priority Rating, or VPR, is a dynamic value that will change based on threat intelligence updates – if a previously quiet vulnerability was suddenly seen being exploited in the wild, the VPR number would go up, so that security teams know it has a higher priority for remediation. This is the perfect case study to talk about when considering how threat intelligence will change the future of cybersecurity. By providing scores that actually reflect the genuine risk of a vulnerability being exploited, organizations can patch security issues that need to be done as a priority, instead of completing remediation work that will have immediate defensive benefit.

Want to read more about VPR? Check out [Tenable's site](#).

[Previous Topic](#)

[Mark Complete](#) ✓
Back to Lesson

[Next Topic](#)

8 Topics1 Quiz

DF4) Windows Investigations

3 Topics3 Quizzes

DF5) Linux Investigations

4 Topics2 Quizzes

DF6) Volatility

3 Topics1 Quiz

DF7) Autopsy

4 Topics1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics1 Quiz

SI2) Logging

6 Topics2 Quizzes

SI3) Aggregation

2 Topics1 Quiz

SI4) Correlation

6 Topics1 Quiz

SI5) Using Splunk

5 Topics2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

8 Topics1 Quiz

IR2) Preparation Phase

10 Topics2 Quizzes

IR3) Detection and Analysis Phase

7 Topics4 Quizzes

IR4) Containment, Eradication, and Recovery Phase

5 Topics1 Quiz

IR5) Lessons Learned and Reporting

7 Topics

IR6) MITRE ATT&CK

13 Topics2 Quizzes

BTL1 EXAM

Exam Preparation

Using RDP and SSH

How to Start Your Exam