NormShield

Cyber Risk Scorecard Documentation

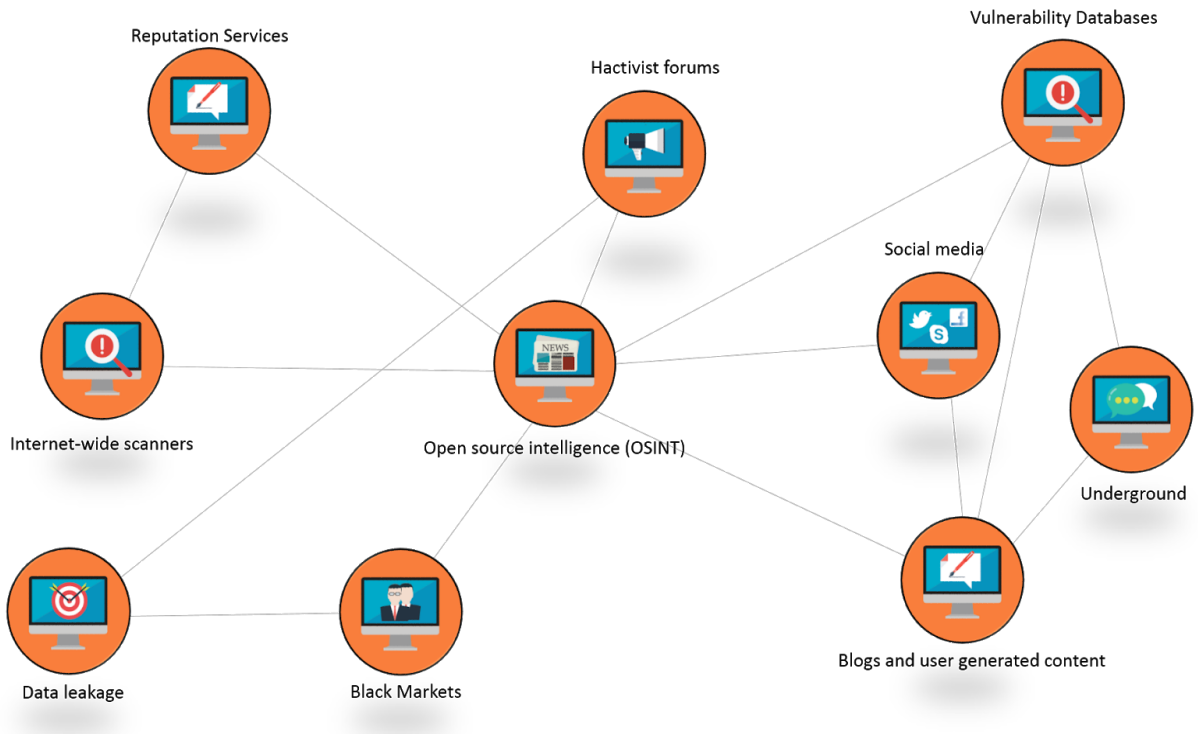
May 30th, 2018

8200 Greensboro Drive, Suite 900
McLean, VA 22102
+1 (571) 335-0222

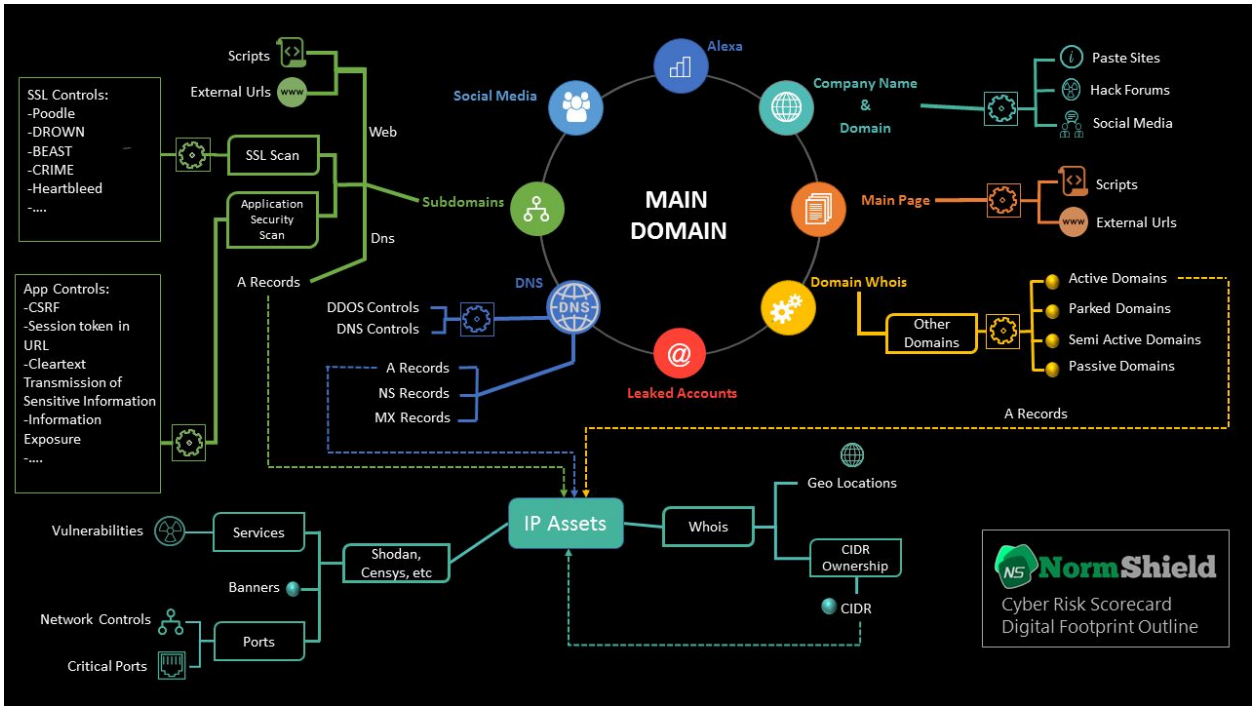
How NormShield Risk Scorecard Works

NormShield provides a service that scans your business's public access methods for possible security risks, such as known but unpatched vulnerabilities or open network ports. NormShield also monitors social media, dark-web forums, and other sources of information leaks, searching for information about your company such as compromised passwords, email addresses, or network structure details. Other vital attack methods such as fake/fraudulent websites or programs masquerading as legitimate sites or products of your business are also hunted down.

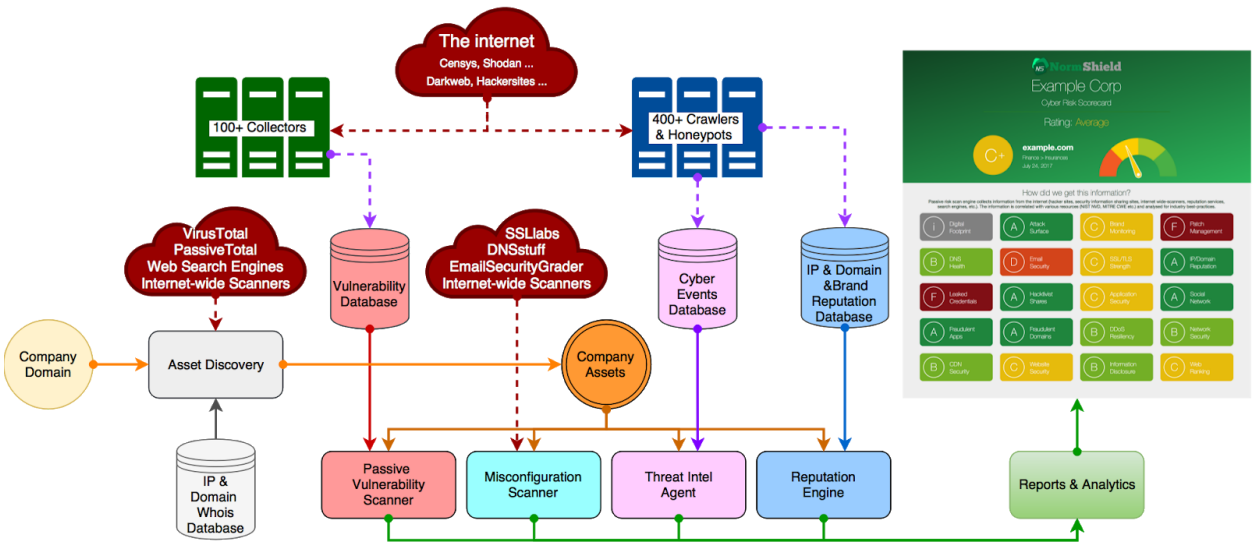
NormShield uses open-source intelligence (OSINT) techniques to gather information. Both hackers and legitimate security companies continually scan social media websites and networks for information on vulnerabilities and publish their findings on the internet. The following map shows how hackers can leverage their attack vectors by using OSINT resources, namely hacker forums, social networks, Google, leaked database dumps, paste sites, and even legitimate security services like VirusTotal, Censys, Cymon, Shodan, and Google Safe Browsing. NormShield's risk scorecard gathers data from all these sources and performs contextualization and analysis to convert data to "risk" intelligence in the form of a scorecard.



To generate the scorecard, NormShield requires only domain name of a company. The asset-discovery engine collects the related information from VirusTotal, PassiveTotal, web search engines, and other Internet-wide scanners. NormShield has one of the largest IP & Domain Whois database that holds more than one billion historical items. The asset-discovery engine searches the database to find all IP address ranges and domain names related to the company.



The results generated by the asset-discovery engine, company assets, are used as the input for passive vulnerability and configuration scanners, threat intelligence agent, and reputation engine.



NormShield has more than 100 data collectors, 400 crawlers, and tens of honeypots. The crawlers and collectors continuously collect IP & domain reputation feeds, cyber events, hacker shares, social-media shares, and known vulnerabilities. They also collect Internet-wide scanner (Censys, Shodan) databases and put the results into the corresponding data stores. The reports and analytics agent then analyzes the findings and generates the scorecard.

This data is analyzed and compiled by NormShield into a simple, readable report with letter-grade scores to help identify and mitigate potential security risks and to alter technical data into business concepts. NormShield does all of this information gathering and analysis in a non-intrusive way, i.e., without scanning or modifying any of the company's business assets.

Grading Methodology

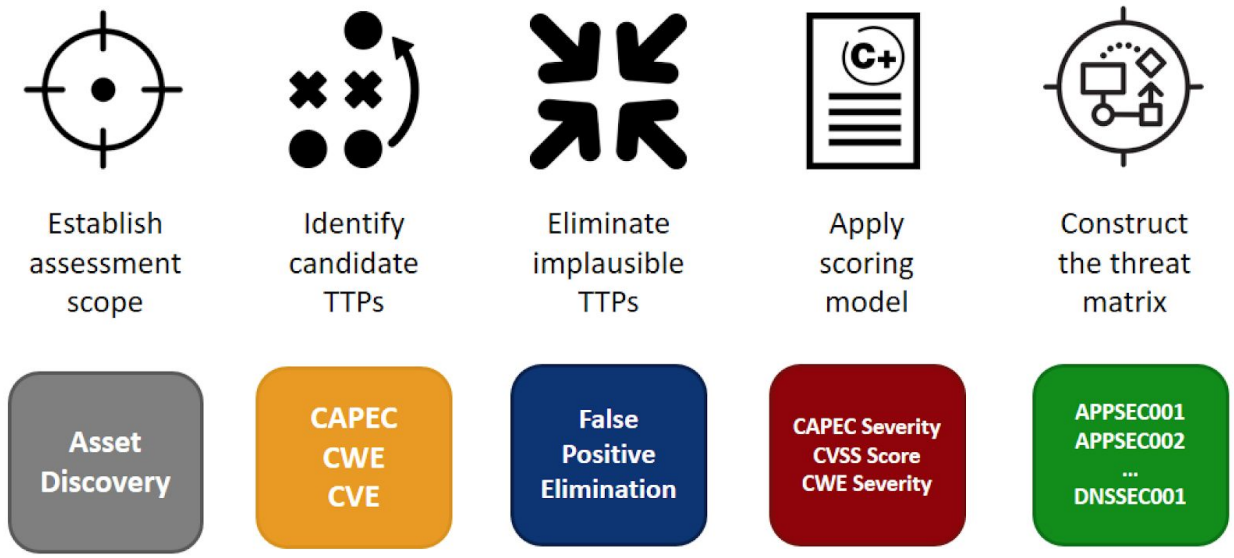
Grading is assessing the risk and converting it into numbers and easy-to-understand letters grades. In our grading methodology, we follow and apply well-known and commonly-used Cyber Threat Susceptibility Assessment (CTSA) and Common Weakness Risk Analysis Framework (CWRAF™) which are developed by the MITRE Corporation; and combine it with our own proprietary methods for data gathering and analytics. CTSA and CWRAF provide a framework for scoring software weaknesses in a consistent, flexible, open manner, while accommodating context for the various business domains.

CTSA and CWRAF benefits:

- Include mechanisms for measuring risk of security errors ("weaknesses") in a way that is closely linked with the risk to an organization's business or mission.
- Support the automatic selection and prioritization of relevant weaknesses, customized to the specific needs of the organization's business or mission.
- Can be used by organizations in conjunction with the Common Weakness Scoring System (CWSS™) to identify the most important weaknesses for their business domains, in order to inform their acquisition and protection activities as one part of the larger process of achieving software assurance.

Cyber Threat Susceptibility Assessment (CTSA)

Cyber Threat Susceptibility Assessment (CTSA), developed by MITRE, is a methodology for evaluating the susceptibility of a system to cyber-attack. CTSA quantitatively assesses a system's [in]ability to resist cyber-attack over a range of cataloged attack Tactics, Techniques, and Procedures (TTPs). CTSA consists of the following steps:



Establish Assessment Scope: The first step in CTSA is to establish the scope of the evaluation, which can be characterized in terms of;

- The set of system assets being evaluated,
- The range of attack TTPs being considered,
- The types of adversaries.

NormShield establishes the assessment scope during the asset discovery process, which discovers all publicly visible/accessible domains, subdomains, IP/CIDR ranges, etc.

Identify Candidate TTP: Once the scope of CTSA is established, the next step is to evaluate the cyber asset's architecture, technology, and security capabilities against TTPs in the Mission Assurance Engineering (MAE) Catalog. Unclassified sources of adversary TTPs in the catalog include MITRE-hosted resources such as Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Enumeration (CWE), and Common Vulnerability Enumeration (CVE). CAPEC is a compilation of attack patterns derived from specific real-world incidents. CWE is a catalog of software weaknesses and defects that adversarial TTPs may exploit. CVE catalogs vulnerabilities found in Commercial off-the-shelf (COTS) hardware and software products.

Eliminate Implausible TTPs: This initial set of candidate TTPs undergoes a narrowing process to eliminate TTPs considered implausible. Several factors can make a TTP an implausible method of cyber attack. Many TTPs have prerequisites or conditions that must hold true in order for that TTP to be effective.

Apply Scoring Model: Candidate TTPs that cannot be eliminated are ranked using a scoring model. The TTP scoring model assesses the risk associated with each TTP relative to other

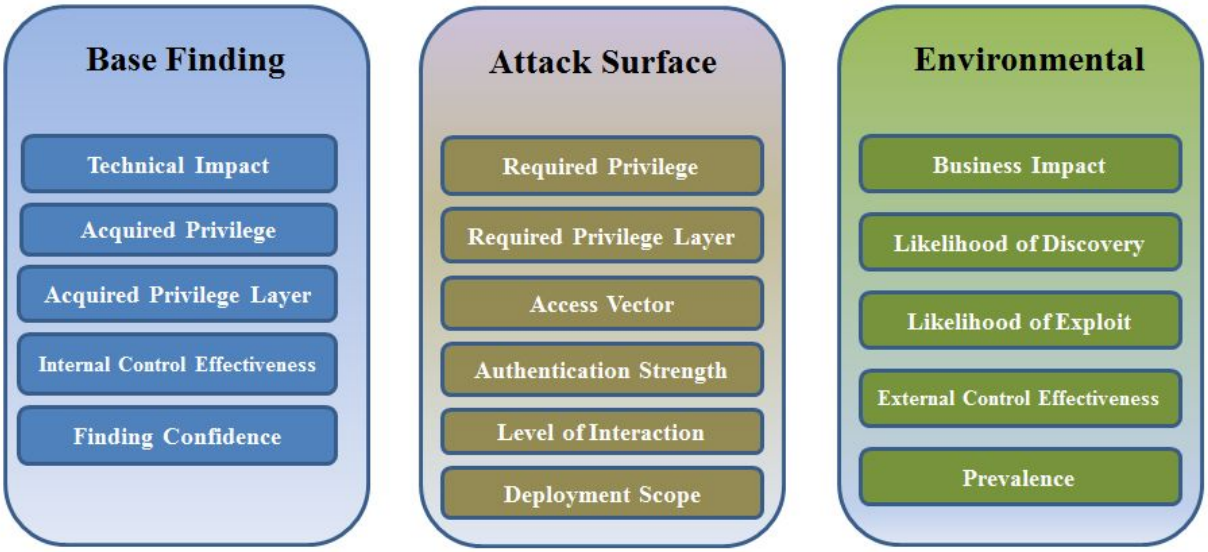
plausible TTPs considered in the assessment. This ranking helps set priorities on where to apply security measures to reduce the system's susceptibility to cyber attack. CAPEC severity levels, CVSS scores and CWE severity ranks are the main parameters to calculate the TTP risk scores.

Construct a Threat Matrix: CTSA produces a Threat Matrix, which lists plausible attack TTPs ranked by decreasing risk score and their mapping to cyber assets as a function of adversary type. NormShield has over 500 TTPs (APPSEC001, APPSEC002, … DNS001, DNS002,… etc.) with different risk scores.

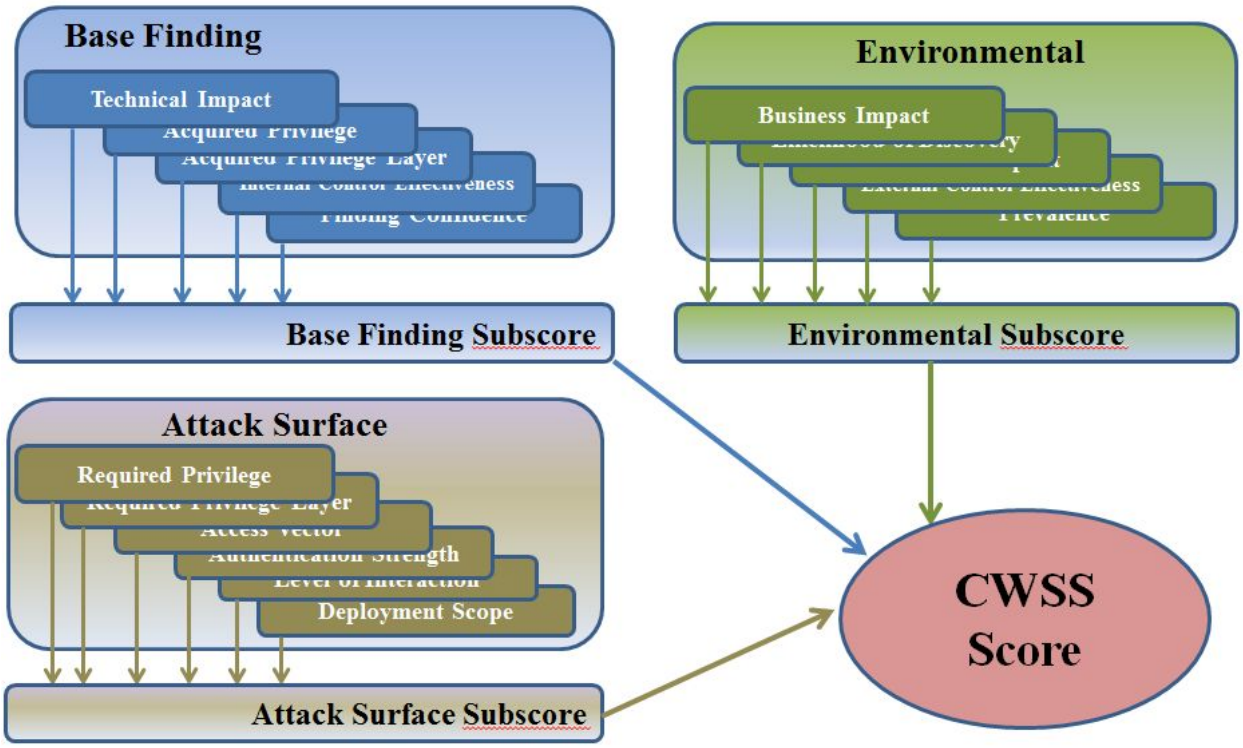
The NormShield threat matrix is calculated by using Common Weakness Scoring System (CWSS™) that provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner. It is a collaborative, community-based effort that is addressing the needs of its stakeholders across government, academia, and industry. When used in conjunction with the Cyber Threat Susceptibility Assessment (CTSA) or Common Weakness Risk Analysis Framework (CWRAF™), organizations are able to apply CWSS to those CWEs that are most relevant to their own specific businesses, missions, and deployed technologies.

How does CWSS work?

CWSS scores CWEs using 18 different factors across three metric groups: (1) the Base Finding group, which captures the inherent risk of the weakness, confidence in the accuracy of the finding, and strength of controls; (2) the Attack Surface group, which captures the barriers that an attacker must cross in order to exploit the weakness; and (3) the Environmental group, which includes factors that may be specific to a particular operational context, such as business impact, likelihood of exploit, and existence of external controls.



Each factor in the Base Finding metric group is assigned a value. These values are converted to associated weights, and a Base Finding subscore is calculated. The Base Finding subscore can range between 0 and 100. The same method is applied to the Attack Surface and Environmental metric group; their subscores can range between 0 and 1. Finally, the three subscores are multiplied together, which produces a CWSS score between 0 and 100.



CWSS contains the following factors, organized based on their metric group:

Group	Name	Summary
Base Finding	Technical Impact (TI)	The potential result that can be produced by the weakness, assuming that the weakness can be successfully reached and exploited.
Base Finding	Acquired Privilege (AP)	The type of privileges that are obtained by an attacker who can successfully exploit the weakness.
Base Finding	Acquired Privilege Layer (AL)	The operational layer to which the attacker gains privileges by successfully exploiting the weakness.
Base Finding	Internal Control Effectiveness (IC)	the ability of the control to render the weakness unable to be exploited by an attacker.
Base Finding	Finding Confidence (FC)	the confidence that the reported issue is a weakness that can be utilized by an attacker
Attack Surface	Required Privilege (RP)	The type of privileges that an attacker must already have in order to reach the code/functionality that contains the weakness.

Attack Surface	Required Privilege Layer (RL)	The operational layer to which the attacker must have privileges in order to attempt to attack the weakness.
Attack Surface	Access Vector (AV)	The channel through which an attacker must communicate to reach the code or functionality that contains the weakness.
Attack Surface	Authentication Strength (AS)	The strength of the authentication routine that protects the code/functionality that contains the weakness.
Attack Surface	Level of Interaction (IN)	the actions that are required by the human victim(s) to enable a successful attack to take place.
Attack Surface	Deployment Scope (SC)	Whether the weakness is present in all deployable instances of the software, or if it is limited to a subset of platforms and/or configurations.
Environmental	Business Impact (BI)	The potential impact to the business or mission if the weakness can be successfully exploited.
Environmental	Likelihood of Discovery (DI)	The likelihood that an attacker can discover the weakness
Environmental	Likelihood of Exploit (EX)	the likelihood that, if the weakness is discovered, an attacker with the required privileges/authentication/access would be able to successfully exploit it.
Environmental	External Control Effectiveness (EC)	the capability of controls or mitigations outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger.
Environmental	Prevalence (P)	How frequently this type of weakness appears in software.

A CWSS 1.0 score can range between 0 and 100. It is calculated as follows:

`BaseFindingSubscore * AttackSurfaceSubscore * EnvironmentSubscore`

The Base Finding subscore (BaseFindingSubscore) is calculated as follows:

```
Base = [ (10 * TechnicalImpact + 5*(AcquiredPrivilege + AcquiredPrivilegeLayer)
+ 5*FindingConfidence) * f(TechnicalImpact) * InternalControlEffectiveness ] *
4.0

f(TechnicalImpact) = 0 if TechnicalImpact = 0; otherwise f(TechnicalImpact) =
1.
```

The AttackSurfaceSubscore is calculated as:

```
[ 20*(RequiredPrivilege + RequiredPrivilegeLayer + AccessVector) +
20*DeploymentScope + 15*LevelOfInteraction + 5*AuthenticationStrength ] / 100.0
```

The EnvironmentalSubscore is calculated as:

```
[ (10*BusinessImpact + 3*LikelihoodOfDiscovery + 4*LikelihoodOfExploit +
3*Prevalence) * f(BusinessImpact) * ExternalControlEffectiveness ] / 20.0

f(BusinessImpact) = 0 if BusinessImpact == 0; otherwise f(BusinessImpact) = 1
```

Using the Codes as specified for each factor, a CWSS score can be stored in a compact, machine-parsable, human-readable format that provides the details for how the score was generated. This is very similar to how CVSS vectors are constructed.

Example: Business-critical application

Consider a reported weakness in which an application is the primary source of income for a company, thus has critical business value. The application allows arbitrary Internet users to sign up for an account using only an email address. A user can then exploit the weakness to obtain administrator privileges for the application, but the attack cannot succeed until the administrator views a report of recent user activities - a common occurrence. The attacker cannot take complete control over the application, but can delete its users and data. Suppose further that there are no controls to prevent the weakness, but the fix for the issue is simple, and limited to a few lines of code.

This situation could be captured in the following CWSS vector:

```
(TI:H,0.9/AP:A,1.0/AL:A,1.0/IC:N,1.0/FC:T,1.0/

RP:L,0.9/RL:A,1.0/AV:I,1.0/AS:N,1.0/IN:T,0.9/SC:A,1.0/

BI:C,0.9/DI:H,1.0/EX:H,1.0/EC:N,1.0/P:NA,1.0)
```

The vector has been split into multiple lines for readability. Each line represents a metric group.

The factors and values are as follows:

Factor	Value
Technical Impact	High
Acquired Privilege	Administrator
Acquired Privilege Layer	Application
Internal Control Effectiveness	None
Finding Confidence	Proven True
Required Privilege	Guest
Required Privilege Layer	Application
Access Vector	Internet
Authentication Strength	None
Level of Interaction	Typical/Limited
Deployment Scope	All
Business Impact	Critical
Likelihood of Discovery	High
Likelihood of Exploit	High
External Control Effectiveness	None
Prevalence	Not Applicable

The CWSS score for this vector is 92.6, derived as follows:

- BaseSubscore:
  - `[ (10 * TI + 5*(AP + AL) + 5*FC) * f(TI) * IC ] * 4.0`
  - `f(TI) = 1`
  - `= 96.0`
- AttackSurfaceSubscore:
  - `[ 20*(RP + RL + AV) + 20*SC + 15*IN + 5*AS ] / 100.0`
  - `= 0.965`
- EnvironmentSubscore:
  - `[ (10*BI + 3*DI + 4*EX + 3*P) * f(BI) * EC ] / 20.0`
  - `f(BI) = 1`
  - `= 1.0`

NormShield uses 0-to-10 scale and the CWSS score is divided by 10. The final score is:

```
96.0 * 0.965 * 1.0 / 10 = 92.64 / 10 ~= 9.2
```

Category Grades

The NormShield category (Patch Management, SSL/TLS Strength, DNS Security etc.) grades are calculated based on the following equation:

```
TheSuccessPoint = 100 - [Sum( CWSS * SeverityLevel * Status * (1/AgeOfFinding)
* (1/DenseOfFinding) / (1 or sqrt(TheSizeOfTheCompany)))] * CategoryMultiplier
```

Parameter	Description
TheSuccessPoint	This is the success percent of the category which can be translated into letter grades based on the American Grading System shown below.
CWSS	The CWSS score of each finding in the category. The calculation of CWSS score is given above. It could be between 0.0 (min) to 10.0 (max)
SeverityLevel	This is the Severity level of the finding and could be Info (0), Low(1), Medium (2), High (3) or Critical (4). This parameter is used to amplify the high severity weaknesses.
Status	This is the status of a finding and it could be Passed (0), Warning(0.5) or Failed(1). This parameter is used to fine tune the impact of some findings if there are other countermeasures.
AgeOfFinding	Each findings has a date and the age may reduce the impact on the grade. For example a leaked credential or a blacklisted IP lose the impact over the time.
DenseOfFinding	Some findings may frequently show up in each scorecards. Over the time the density of a finding inversely impact the grade since these types of findings become unimportant.
TheSizeOfTheCompany	The small and bigger companies have different constraints. The company grows, the harder to keep it secure. This parameter allows to optimize the difficulty of keeping the secure.
CategoryMultiplier	Since the control items in each category is different, this parameter allows to scale the each category to 0-to-100 scale.

Once the category grades are calculated based on the equation given above, the grades are translated into GPA and Letter grades based on American Grading system. Below is a grading system used by NormShield.

Letter Grade	Percentage	GPA
A+	97%+	4.00/4.00
A	93%-96%	3.90/4.00
A-	90%-92%	3.67/4.00
B+	87%-89%	3.50/4.00
B	83%-86%	3.33/4.00
B-	80%-82%	3.00/4.00
C+	77%-79%	2.67/4.00
C	73%-76%	2.33/4.00
C-	70%-72%	2.00/4.00
D+	67%-69%	1.67/4.00
D	63%-66%	1.33/4.00
D-	60%-62%	1.00/4.00
F	0%-59%	0.00/4.00

The Grading Scale Table

Category Weights

The category grades are calculated once assessments on all the categories are completed. Each category has different weight in the overall grade as shown below.

Category Name	Weight (Total 100)		Category Name	Weight (Total 100)
Digital Footprint	0/100		IP Reputation	7/100
DNS Health	6/100		Hacktivist Shares	5/100
Email Security	6/100		Social Network	3/100
SSL/TLS Strength	6/100		Attack Surface	4/100
Application Security	9/100		Brand Monitoring	3/100
DDoS Resiliency	4/100		Patch Management	10/100
Network Security	6/100		Web Ranking	2/100
Fraudulent Domains	5/100		Information Disclosure	3/100
Fraudulent Apps	3/100		Website Security	6/100
Credential Mgmt.	9/100		CDN Security	3/100

The overall grade is calculated by the weighted arithmetic mean, which is similar to an ordinary arithmetic mean (the most common type of average), except that instead of each of the data points contributing equally to the final average, every category contributes proportionally with the weights.

So the final grade is calculated by:

```
TheOverAllGPA = Sum(TheGPAofTheCategory * WeightOfTheCategory)
```

The overall GPA is translated to letter grade and percent again using the same table (The Grading Scale Table) given above.

NormShield has analyzed data in different risk categories from 1,000,000 servers for hundreds of companies and calculated letter grades for the results. For example, a grade of 'B' indicates an organization has opened the door to a sophisticated hacker, a grade of 'F' means hackers of all types are being invited. The overall grade of cyber risk scorecard shows "how easy is it to hack the corresponding environment?"

Grade A
It would take world-class, state-sponsored hackers to exploit

Grade B
Skills of persistent, highly experienced hackers are required

Grade C
Average to professional hackers are capable of exploiting

Grade D
Beginner hacker practicing their skills

Grade F

Script kiddies can hack (i.e. 6th Graders)

References:

https://cwe.mitre.org/cwss/cwss_v1.0.1.html
https://cyber.riskscore.cards/grades
https://www.mitre.org/sites/default/files/pdf/11_4982.pdf
https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/cyber-threat-susceptibility-assessment
https://nvd.nist.gov/

Conclusion

Visibility into your cyber risks is critical to get ahead of hackers. By seeing the cyber weaknesses of your organization and vendors that hackers see, you can make the right decisions to protect your organization. The 20 letter grades with details in NormShield Cyber Risk Scorecards give you the visibility to outsmart your hackers.

About NormShield

With NormShield, automatically see, prioritize and act on cyber threats. The NormShield Cyber Risk Scorecard provides early warning to hacker threats through a thorough and reliable letter-grade report. The Scorecard presents grades in 20 risk categories so that CISOs and other security leaders can prioritize remediation rapidly and make informed resource decisions.

The NormShield cloud platform automates unified vulnerability management, cyber threat intelligence, and risk scoring. CISOs receive letter-grade risk scorecards to make informed decisions. Security teams receive orchestrated, prioritized reporting and automated ticketing for swift action.

normshield.com