JUNE 2019

HOW TO MEASURE WHAT HACKERS KNOW ABOUT YOU

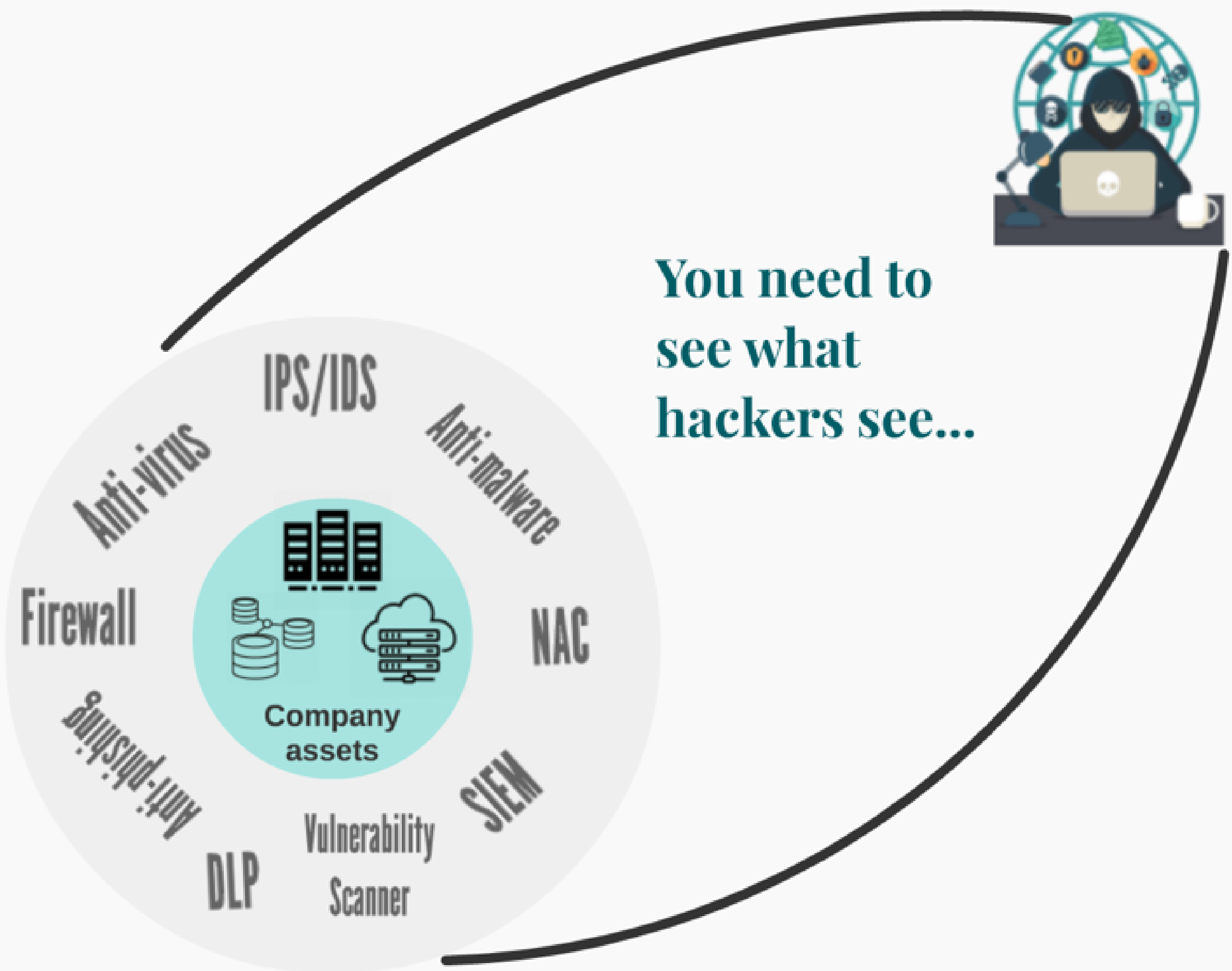
NormShield

www.normshield.com

Can you measure how safe you are?

Companies invest in cyber security to protect themselves against cyber attacks. They get cyber security products/solutions from SIEM solutions, SOC services to Firewalls, IPS/IDS devices, etc. to detect and remediate cyber incidents.

With all these security measures, how safe are you? Is there a way to measure it? Or in other words, is it possible to assess your cyber risk? Sure once-a-year penetration tests and risk assessments through internal audits give some answers, but an outside-in approach with easy-to-understand monitoring helps you understand your cyber security posture. In order to do that, you need to see what hackers see…



"You can't manage what you can't measure."

- P. Drucker

Holistic view to determine cyber risk

In ancient Indian philosophy, there is a story about blind men and an elephant where blind men touch a certain part of an elephant and try to describe it. The one who touches the trunk describes it as a snake, while the one who touches the tail thinks it is a rope, etc. The story tells us how we define the reality around us:

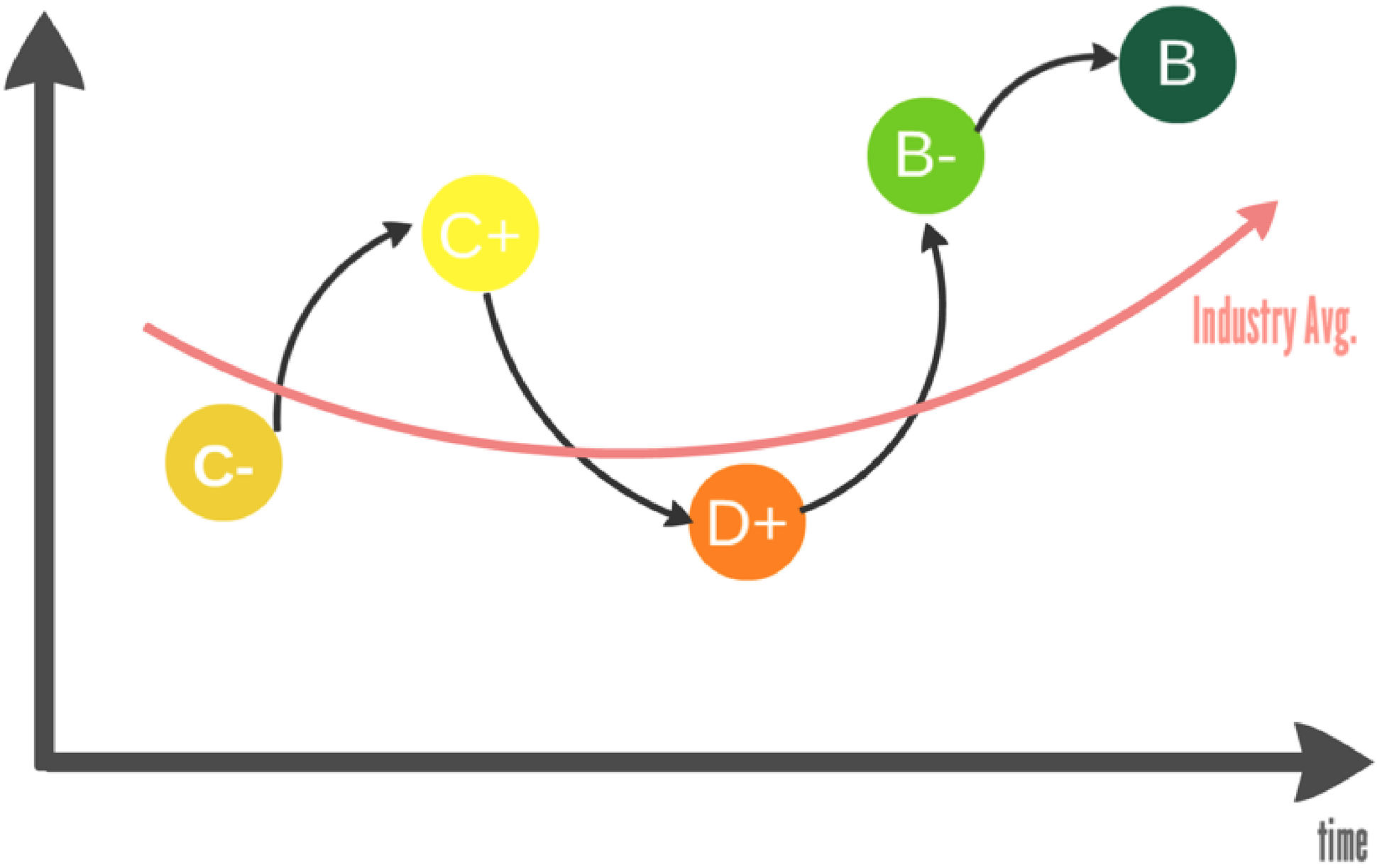
We describe the universe false and deficient because of our limited perception.

Like this story, every cyber risk assessment with different tools/solutions has limited view on cyber security posture. They specialize in solutions for a certain problem in cyber security universe. So we can change the word universe in the above sentence with the word cyber security: We describe the cyber security false and deficient because of our limited perception. Thus, to measure what hackers really know about you, you need a holistic view to cover every aspect of cyber security.

Normshield

Monitoring cyber risk with security ratings

Some companies including NormShield provide cyber risk scores or security ratings to measure cyber security posture of a company. The scores/ratings help organizations to monitor their cyber risk to see how they are doing compared to past or compared to industry. They can see the return on investments and in which parts of their system that they need to harden cyber security.

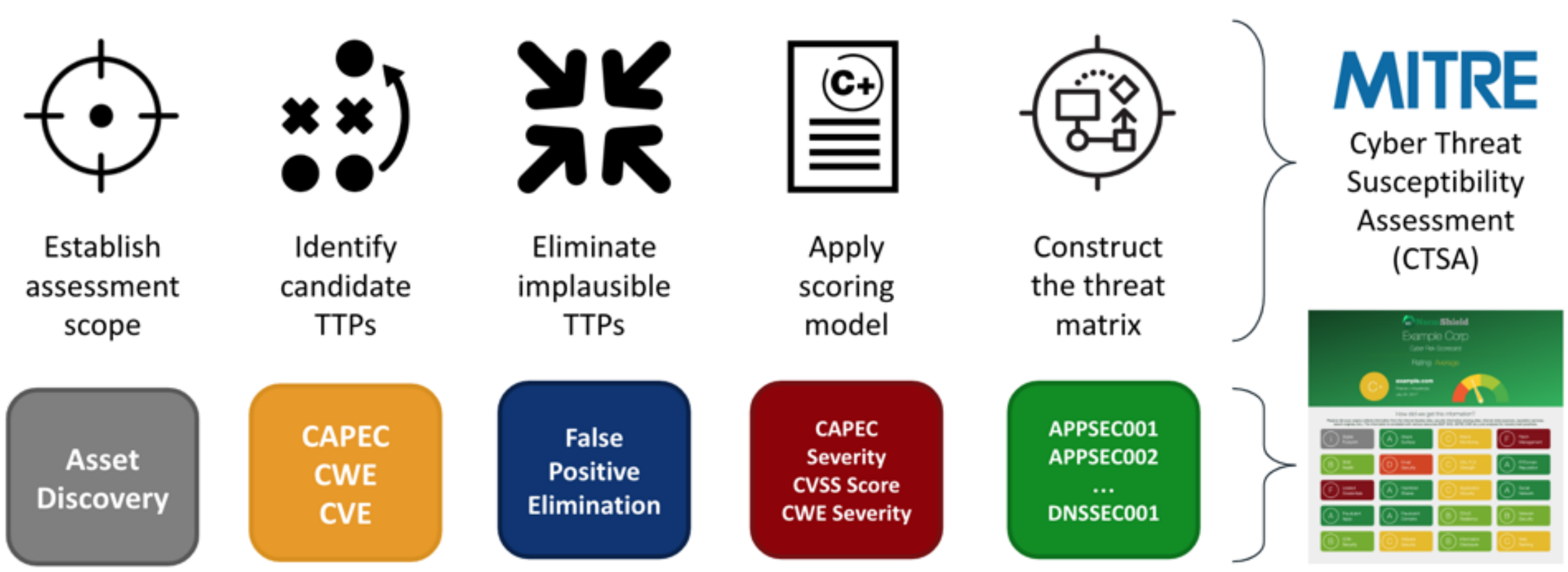


Easy-to-understand grades create a common language

The easy-to-understand scores and ratings can be represented by letter grades like credit ratings published by FICO, S&P, etc. Letter grades create a common language across the organizations and improve communication between executives and technical security teams.“By 2022, cybersecurity ratings will become as important as credit ratings when assessing the risk of existing and new business relationships.” - GartnerWhen an undergrad student who pursues a BS degree in Electrical Engineering shows her transcript with a B+ grade in Electromagnetics course to her parents, they can understand that their daughter is doing great in that course without further knowledge of Electromagnetics in details. Similarly, when an executive sees a B+ in Patch Management, then s/he can assume that they look good on that area without detailed knowledge of new vulnerabilities published.

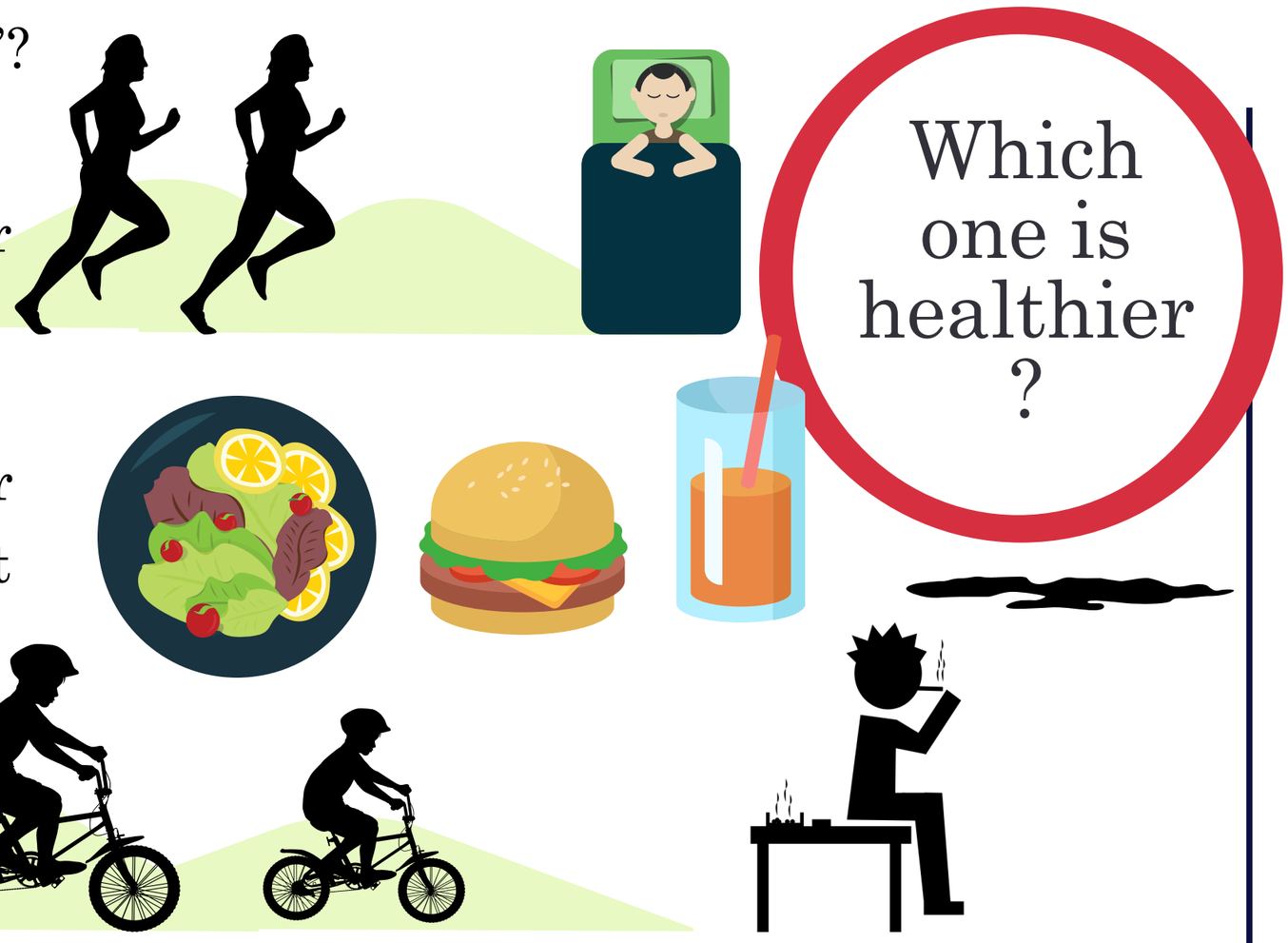
Objective and independent scoring is a must

Cyber risk assessment with security ratings should be independent and objective for any company. A grading methodology that depends on well-accepted frameworks is more transparent and objective. For instance, NormShield grading methodology depends on MITRE’s Cyber Threat Susceptibility Assessment (CTSA) Common Weakness Risk Analysis Framework (CWRAF™).



Indicators of safety

How do you understand that your company is “safe”? Before elaborating more on indicators of safety, let’s look at indicators of health for a human being.Which human looks “healthier”?



(A) The one who regularly exercise or
(B) the one who gets lazy every day

(A)The one who eats vegetables or
(B) the one who eats unhealthy fast food

(A) The one who gets fresh air or
(B) the one who smokes

The reasonable answer to all the questions above would be (A). Similarly, by looking at a company from outside, we can derive a similar approach to determine the cyber security posture of a company.

Which one looks “safer” to you?
(A) a company that actively use SPF, DMARC, DKIM records or
(B) a company that has no security measures for e-mail exchanges

(A) a system with up-to-date patches or
(B) a system that lacks relevant security patches

(A) a company whose IP assets are listed in blacklists (have become a member of a botnet or part of a spam propagation) or
(B) a company whose IP assets are not listed in blacklists.

(A) a corporation with high employee awareness where employees do not use corporate e-mails in non-business platforms or
(B) a corporation whose employee credentials are leaked in dark/deep web.

Again, the reasonable answer to all the questions above would be (A). For different cyber security metrics, similar control questions can be derived to understand what hackers see when they look at a company in cyber space.

Components of cyber risk in a holistic view

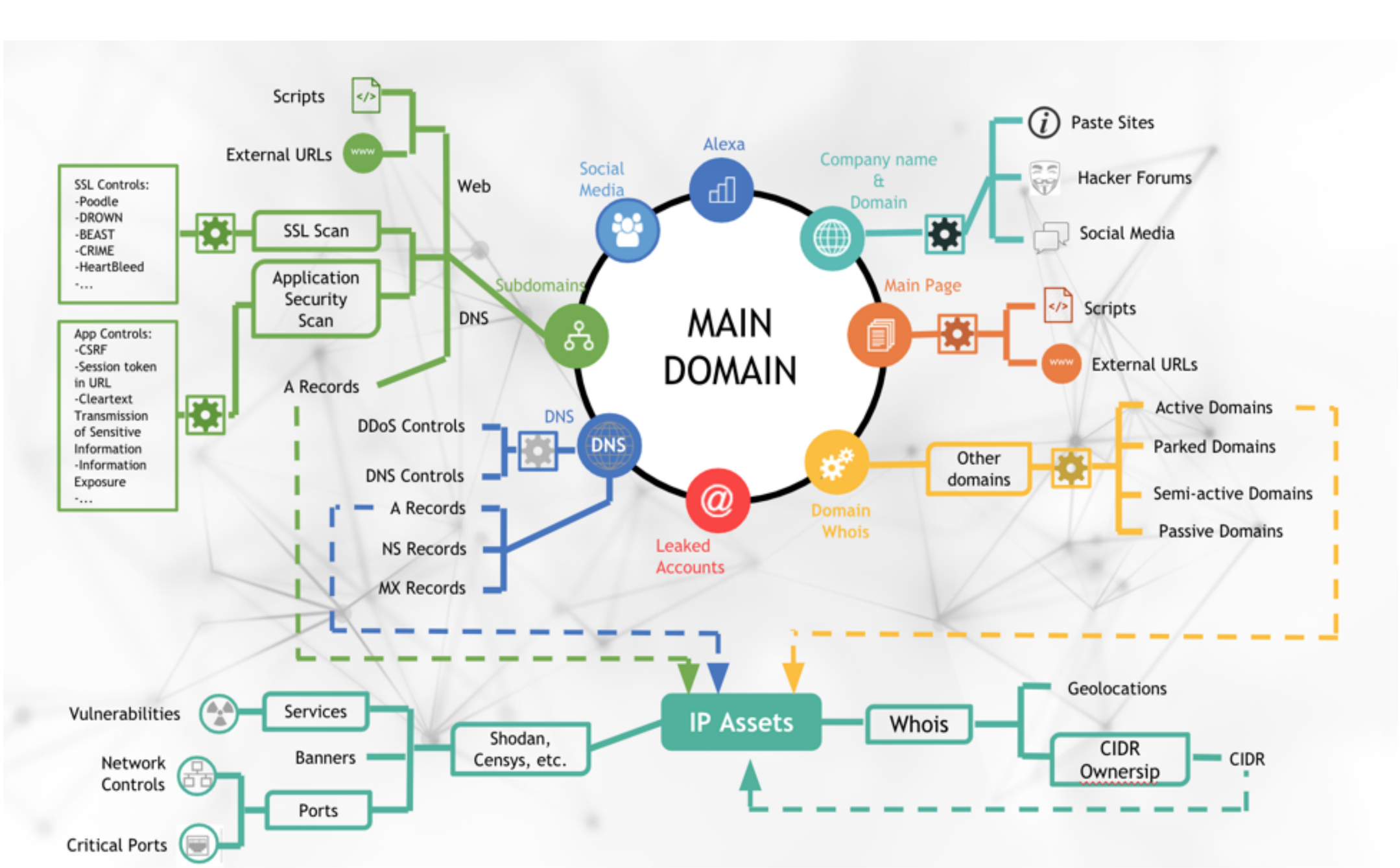
There can be many metrics that can be used to assess external cyber risk of a company. As aforementioned above, we need a holistic view that covers many areas to get the right metrics. Since cyber security space is too large, one can find hundreds of control items in tens of different areas. For instance, NormShield covers 500+ control items in 20 different categories.

How to assess cyber risk of a company with cyber intelligence

Once the metrics are determined, it really depends on how to collect the relevant data. Gathering data directly from the company by asking a set of questions would help, but it is a very slow process with subjective results. Instead, gathering information about a company from cyber space with open source intelligence (OSINT) techniques can help to assess the cyber risk of any company in an independent and objective way.

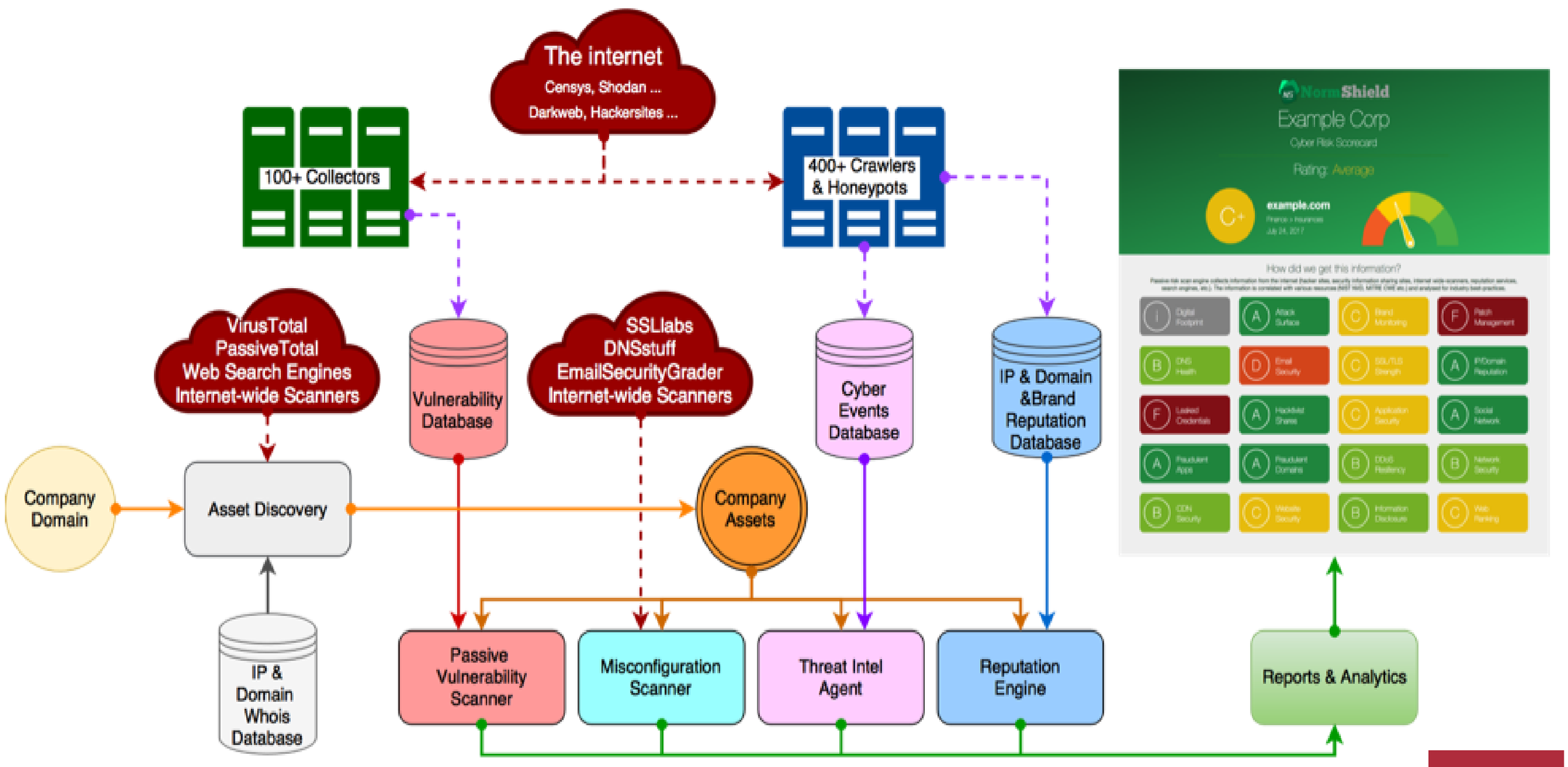
Digital Footprint

The very first step on such external cyber risk assessment is to map the digital footprint of the company. Starting with only domain name, there are many information can be found. From DNS records of main domain, subdomains, and related domains, IP assets can be found. Websites can be visited like a regular visitor to determine JavaScripts used and externals URLs given on the website. Leaked databases can be searched from leaked credentials. Hacker forums, paste sites, social networks can be crawled for the company and domain names. IP assets can be searched on internet-wide scanners like Shodan, Censys, Zoomeye, etc. to determine services on those IP assets and open ports on IP addresses. The amount of information that can be mounted just from a domain name is quite rich to map the digital footprint of a company and it can be obtained in seconds with the right tools and experience.



Converting data to intelligence

Asset discovery is just the beginning of what hackers know about you. To determine the indicators of safety, you have to think of every aspect. What are the possible vulnerabilities that seen from outside? Are there any misconfigurations that are visible? Are there any leaks disclosed in hacker forums or paste sites? Are there any IP assets blacklisted because they were part of a botnet or spam propagation? All these information can be gathered from the cyberspace by asking the questions into right places. Once all these collected, it has to be converted to meaningful intelligence and be reported with easy-to-understand grades.



Prioritization of issues

Now, you have a holistic view of what hackers know about your company and an independent and objective measurement of your cyber security posture. What's next? Fixing the cyber security posture.Since there are hundreds - even thousands- of findings, you need to prioritize the issues. Using a standard-based approach on grading now helps, because these standards provide severity levels along with detailed scores such as Common Vulnerability Scoring System (CVSS), Common Weakness Scoring System (CWSS), etc. You can draw a priority matrix for the findings to better determine on which ones to focus first.

Security Rating Service Providers

Any company can do measurement of their external cyber security posture with open source intelligence, but it would take time, manpower, and requires expertise. Thus many company prefers to work with security rating service providers like NormShield.

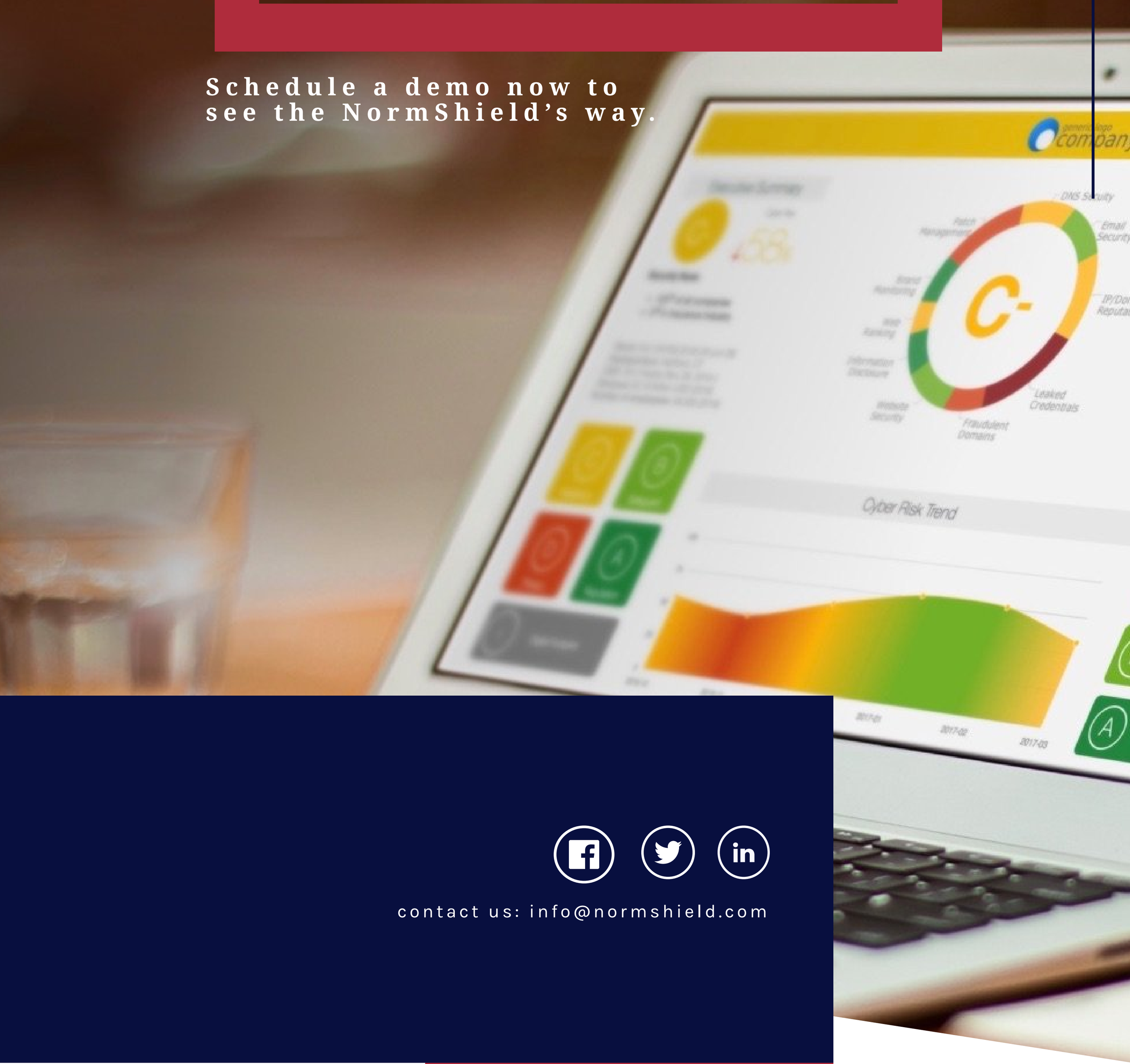
Security rating services provide continuous, independent, and quantitative technical analysis; and scoring for public-facing digital assets of organizational entities across geographies. The services gather data from public and private sources via non-intrusive means, analyze the data and then rate the target entity's security posture using proprietary scoring methodologies. These tools can be used for internal security, for cyber insurance underwriting, for mergers and acquisitions, and for third-party risk assessments and monitoring, including geopolitical risk.

The platforms offered by SRS vendors are relatively easy to use. Purpose-built services are subscription-based, and most are operated by assessing from the "outside-in," without the need to deploy equipment on-site or to configure devices. SRS vendors offer dashboards based on multiple security-relevant characteristics, providing customers with ongoing ratings of the relative security status of existing and potential partners. This is a convenient but incomplete way to monitor the security status of a large number of partners simultaneously.

The players in the market focus on publicly accessible data sources when performing vendor assessments and security benchmarking. Although each player has a different approach to analyze and evaluate the security posture of a company, all use similar resources and techniques to collect data. The difference mainly in coverage, grading methodology, and how they provide the data to users.

JUNE 2019

Schedule a demo now to see the NormShield's way.



contact us: info@normshield.com