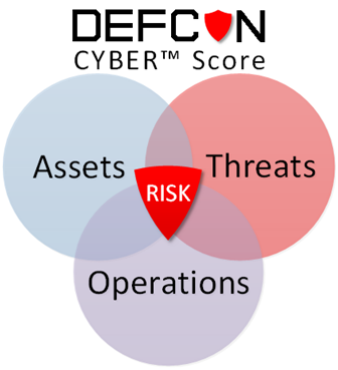
DEFCON CYBER™

How it works…..

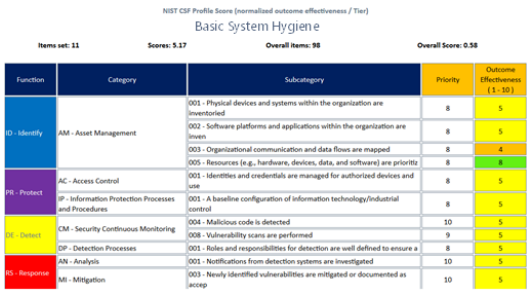
Our DEFCON CYBER™ software solution enables you to define and prioritize your business cybersecurity risk mitigation *strategy* via the NIST Cybersecurity Framework (CSF), or equivalent method. It then aligns your operations to execute the prioritized strategy, identifies gaps and challenges, and measures the organization's ability to execute its priorities. It assimilates all aspects of a cybersecurity program (all 5 functions of the CSF) including its Asset Value to adversaries, strength of its Risk Mitigation Strategy, and its Ability to Execute – inclusive of its operational effectiveness: indicator responsiveness, threat intelligence responsiveness, vulnerability & patch management effectiveness, network design effectiveness, and the cybersecurity posture of its Supply Chain and business partners, into a continuously updated meaningful measurement.

The DEFCON CYBER™ Score effectively communicates the organization's current cybersecurity posture, posture trend, and what is currently driving its cybersecurity risk, thus enabling informed enterprise risk management decisions. DEFCON CYBER™ can help an organization improve its cybersecurity by measuring three fundamental elements.



FIRST: Design Your Cybersecurity Strategy

Your organization must define a strategy for addressing the business problem of cybersecurity risk. To address the business problem of cybersecurity risk, your organization must decide what it is willing to do, or what it needs to do well to protect its Critical Data Assets from its Threats.


NIST CSF Profile Score (normalized outcome effectiveness / Tier)

Basic System Hygiene

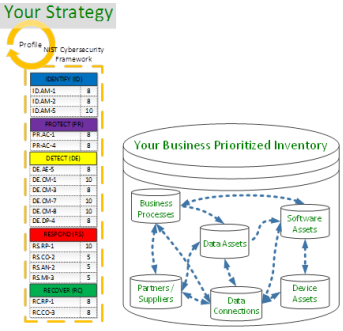
Items set: 11 Scores: 5.17 Overall items: 98 Overall Score: 0.58

Function	Category	Subcategory	Priority	Outcome Effectiveness (1 - 10)
ID - Identify	AM - Asset Management	001 - Physical devices and systems within the organization are inventoried	8	5
		002 - Software platforms and applications within the organization are inven	8	5
		003 - Organizational communication and data flows are mapped	8	4
		005 - Resources (e.g., hardware, devices, data, and software) are prioritiz	8	8
PR - Protect	AC - Access Control	001 - Identities and credentials are managed for authorized devices and use	8	5
	IP - Information Protection Processes and Procedures	001 - A baseline configuration of information technology/industrial control	8	5
DE - Detect	CM - Security Continuous Monitoring	004 - Malicious code is detected	10	5
		008 - Vulnerability scans are performed	9	5
	DP - Detection Processes	001 - Roles and responsibilities for detection are well defined to ensure a	8	5
RS - Response	AN - Analysis	001 - Notifications from detection systems are investigated	10	5
	MI - Mitigation	003 - Newly identified vulnerabilities are mitigated or documented as accep	10	5

Using a risk analysis approach, such as the NIST Cybersecurity Framework, identify your critical data assets, likely high impact threats, and determine what "best practice outcomes" (i.e., CSF Subcategories) need to be achieved, in priority order, and within what timeframes to protect your critical assets from your threats. Your strategy may begin simply with performing five best practices for "Basic System Hygiene" or may include up to all 98 of the CSF best practice outcomes, or more as needed to address your organization's unique cybersecurity risks. DEFCON CYBER™ uses your Target Profile information as the representation of your organization's cybersecurity risk mitigation strategy, and automatically computes your "strength of strategy" cybersecurity posture score component.

SECOND: Prioritize Actions and Measure Response

DEFCON CYBER™ operates by assigning action items to the appropriate team or teams, based upon the priorities you assigned in your organization's cybersecurity risk mitigation strategy, combined with the prioritized assets that are the subject of alerts, threat intelligence, vulnerabilities, and other indicators.



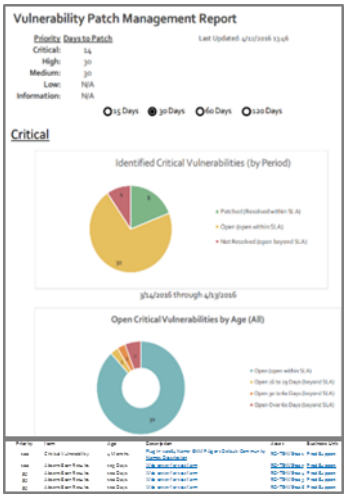

Your Response Team Structure

DEFCON CYBER™ identifies people responding to, and closing assigned actions, and measures the actual timeliness with respect to response thresholds you define in your Priority Profile.

Closing an indicator results in the identification of a false alarm, documentation of remediation action, the initiation of more in-depth analysis, or Response Team initiation.

DEFCON CYBER™ brings qualities of process control to key cybersecurity workflows by employing prioritization, effectiveness and response parameters, and out of tolerance alerting.

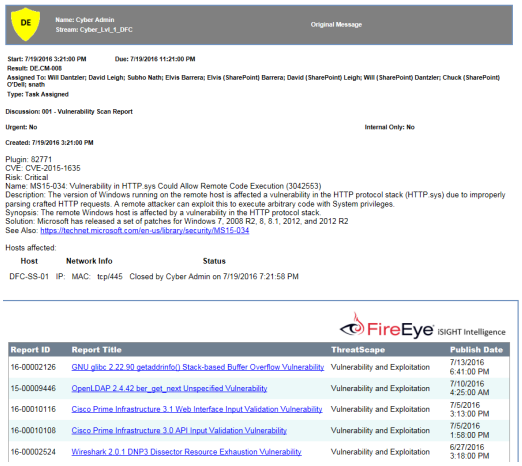
Vulnerability and patch management is a foundational component to "Basic System Hygiene", and is a critical best practice to all cybersecurity programs.



DEFCON CYBER™ integrates vulnerability scan results along with software update availability services to prioritize and measure patch updates within your specified Service Level Agreement (SLA) periods pertaining to vulnerability severity levels. Prioritization is based on the organization's priority for patching in its cybersecurity risk mitigation strategy, the severity of the vulnerability, and the priority of the affected asset. The DEFCON CYBER™ vulnerability and patch management workflow is tightly integrated with the organization's priority asset inventories, enabling DEFCON CYBER™ to identify "unknown" devices, and devices that have been missing vulnerability scan results.

In addition to the core responsiveness measures, DEFCON CYBER™ provides tailored dashboards and reports providing important patch management status and measures: vulnerability SLA status by period, vulnerability age by severity, and the Top 10 items driving your vulnerability score.

Threat Intelligence & information sharing (TI/IS) information for many organizations is yet another contributor to operational noise – *another indicator that should be responded to*. DEFCON CYBER™ integrates different kinds of threat intelligence (TI) and information sharing (IS) services, depending upon your needs and your organization's priority for threat intelligence in its cybersecurity risk mitigation strategy.



TI/IS has been integrated in two ways:

When DEFCON CYBER™ receives a priority alert, it will query TI/IS active services for relevant information pertaining to the alert.

TI/IS received directly from a service may be assigned to a response team for action or review.

DEFCON CYBER™ manages and measures TI/IS as all other indicators (of compromise, intelligence, vulnerabilities, or other actions) with respect to prioritization and action responsiveness.

Partner/Supply Chain risk management is critical to your organization since it is only as secure as its weakest link. Your business partners, law firms, consultants, accountants, technology partners, and others, hold portions of your critically sensitive information – i.e., critical data assets. Your partner's ability to protect your critical data and financial transactions (i.e., your partner's cybersecurity posture) directly affects your organization's risk posture.

With DEFCON CYBER™ deployed to your critical business partners and suppliers, your organization has an effective way to ensure that they are achieving their own cybersecurity at a level acceptable for maintaining your own organization's cybersecurity posture.

DEFCON CYBER™

THIRD: Establish Your Cybersecurity Posture

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

Cybersecurity Posture: A way to continuously examine the state of protection against the unauthorized use of electronic data or systems, or the measures taken to achieve such protection.

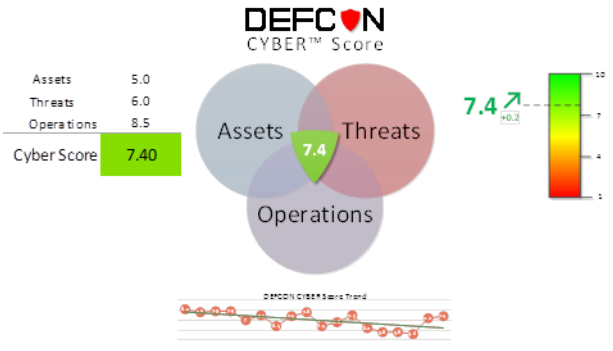
DEFCON CYBER™ integrates aspects of your organization's assessment and compliance analysis, your prioritized cybersecurity risk mitigation strategy (i.e., your Prioritized Cybersecurity Framework Target Profile, or equivalent), prioritized asset inventories, operational performance, and prioritized business partner cybersecurity posture into a holistic, standards based, effective Cybersecurity Posture Score.

The DEFCON CYBER™ Score is composed of three aspects:

Assets: What you have of value to high risk and high impact adversaries.

Threats: The risk environment in which you operate – who are your likely high risk and high impact adversaries. Is there risk activity in your operating environment that may affect your organization?

Operations: What you plan to do to protect your critical assets from the threats, and how well you are able to execute your strategy are the critical components of your cybersecurity posture. Other important components of cybersecurity posture are the importance of vulnerabilities in your assets and organization, and the cybersecurity posture of important business partners.

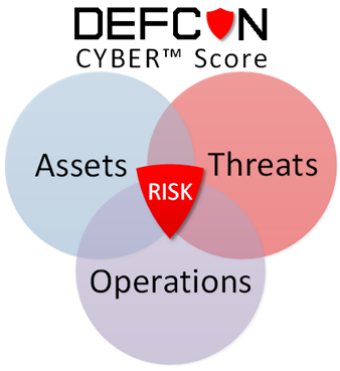


You may not be able to exert much control over the value of your assets to your adversaries as much is inherent to your industry or business, but it can be mitigated by your enterprise risk management strategy. You do not have much control over your threat environment either, other than controlling what connections you establish between components, business partners, and the internet. Your organization does have the control over the strength and breadth of your cybersecurity risk mitigation strategy, your operations ability to perform, and your business partners to perform at an acceptable level. The DEFCON CYBER™ Score reflects the degree to which the organization is responding to changes in asset values and threat environment in a comprehensive way.

Ease of Implementation

It is easy to get started with a Basic Cyber Hygiene template and Cloud Service in as little as two hours. It starts with the mapping of your security tools indicators to your risk management strategy, then identifying the response team members and the workflow path, then start adjusting the scoring parameters.

For more information on how DEFCON CYBER™ can help you prioritize your security operations, analytics and reporting needs, contact us at sales@roforicorp.com



www.DEFCONCYBER.com