Metrics in Cyber Security

Megan Leonard

ISEC 475

7/30/2023

When it comes to metrics within cyber security there are many different forms it takes. The metrics help collect usable data that can be used to define different goals or formulate questions such as how long a process will take.

Say we have a cyber security company that focuses on providing overall security to others. A metric we would be able to measure is security requirements. For example, if we are providing protection for other companies, we would use metrics to see the areas in which areas they are asking for the most security and what aspects they are requiring. One company may require more security for their database while another focuses on their network and firewalls.

Another possible metric would be the number of vulnerabilities as if they are paying you to take care of their security, then you need to understand what vulnerabilities you would have to solve and how many there are to work on.

Then there is the metric of time it would take to complete securing the company or finishing the security requirements. Time will vary based on the number of requirements but can be measured.

Next, we have the metric of intervals of vulnerabilities. This would be how long it takes between finding the first vulnerability to when the next one shows up as no matter how secure something may seem, there will always be a form of vulnerability.

Going along with intervals, we have the time between updates. This we can see as it changes based on scenario like when a vulnerability is found, or an operating system is updated.

Another metric would be the amount of training that is needed to work on these jobs. The cyber security company may have a standard training which is always about the same length in time or could have one based on the tasks at that given point in time.

There is also the metric which is how often a third party would have access. As you are securing the company, you need to know about how often they will be accessed so you know the chance incidents happening because of third parties.

Finally, we have tracked the traffic as you need to keep track of how much is incoming and outgoing. If there is a small amount of traffic then you need to be able to keep note of this and if there is a large amount, then you need to be prepared in case something tries to get through this area.

There are many different metrics in cyber security and the ones used vary based on the area of security. The database security may have different methods to the network while sharing some others.

Citation:

*21 Cybersecurity Metrics & Kpis to track in 2023*. SecurityScorecard. (2023, July 10). <https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track/>

CyberTalents. (n.d.). *Top 15 cybersecurity metrics and Kpis for better security*. CyberTalents Blog. <https://cybertalents.com/blog/top-15-cybersecurity-metrics-and-kpis-for-better-security>

GeeksforGeeks. (2022, February 23). *Cyber security metrics*. GeeksforGeeks. <https://www.geeksforgeeks.org/cyber-security-metrics/>

Mead, N. R., & Woody, C. C. (2017). *Cyber Security Engineering: A practical approach for systems and software assurance*. Addison-Wesley.