From: Altaz Valani
Sent: Thursday, January 4, 2018 3:44 PM
To: cyberframework <cyberframework@nist.gov>
Subject: RFC on Version 1.1 Draft 2 of Cybersecurity Framework

Hi,

Thank you for the opportunity to respond. The framework has some missing elements around the software/application layer. I hope you can address those gaps in the final version.

Here are my comments for your consideration:

1. Line 321: It is unclear whether “systems” refers to the applications layer. Please specifically mention “software”.
2. Line 327: Please include “Application Portfolio Management” (as distinct from “Asset Management”).
3. Line 329: Please rephrase to “application and infrastructure services”.
4. Line 334: Please add “Software security”.
5. Figure 2: Please modify “Securing Critical Infrastructure” to “Securing Critical Infrastructure and Applications”.
6. Line 561: Please add “compliance, legal, and regulatory needs” (as distinct from “business needs”).
7. Line 564: Please modify “systems and assets” to “systems, software, and assets”.
8. Table 2, Page 26: ID.GV-1; please modify “information security policy” to “information and development security policy”.
9. Table 2, Page 29: ID.SC-4; please modify “Reviews of audits, summaries of test” to “Reviews of audits and threat models, summaries of test”.
10. Table 2, Page 40: DE.CM-8; please modify “Vulnerability scans are performed” to “Software security requirements are met and vulnerability scans are performed”.
11. Page 45: Kindly add ISO 27034 to the list

Thanks,

Altaz

Altaz Valani
Director of Research
Security Compass

From: Altaz Valani
Sent: Friday, January 5, 2018 1:10 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Re: RFC on Version 1.1 Draft 2 of Cybersecurity Framework

Addendum to my email below.

My colleagues and I feel the need to mention why we believe the software perspective is so critical today.

We have witnessed Equifax / Heartbleed / Shellshock which are all inherently software vulnerabilities. Yet secure development remains low on the priority list for organizations. As a community of practice, we have a responsibility to bring this issue into light.

Thanks again,

Altaz