7.3 CVD Staffing Considerations

Vulnerability analysis and response may require networking and forensics skills for certain classes of vulnerabilities, but often also requires some mix of the following skills:

- Programming skills, especially in common languages (C, C++, Python, Java)
- Reverse engineering and debugging
- Knowledge of low-level operating system features for Windows, Mac and/or Linux
- Hardware architecture and basic electrical engineering
- Software security testing
- Virtualization and some infrastructure automation
- Written communications
- Customer-service mindset

In most organizations, these skills will likely be dispersed among a team of people rather than expecting a single person to be fluent with all of these topics.

Beware Analyst Burnout

Some organizations may have a small enough flow of incoming vulnerability reports that all the CVD-related roles can be fulfilled by a single team, or even a single person. Other organizations might choose to split the technical analysis roles apart from the more human-oriented communication and coordination roles. No matter the arrangements, it is important that vendors and coordinators establishing a CVD capability mitigate the potential for analyst burnout. Burnout of security analysts is well-documented phenomenon [1,2,3]. Analysts working full-time in a CVD process are at risk of this too. A vendor's CVD capability may receive a large amount of incoming reports each week, especially at larger vendors. This can result in CVD staff becoming stressed and having low job satisfaction, leading to lower quality of work and ultimately employee attrition. The costs of lower quality work (e.g., missing an important report), employee turnover (e.g., hiring and training a new analyst), and associated damage to the vendor's reputation suggest that this problem should be addressed ahead of time with reasonable precautions. At the CERT/CC, we have attempted to mitigate this issue with reasonable success by implementing the suggestions below. Research has shown that many of these are effective responses to commonly-held morale problems [3].

- *Staying well-staffed and rotating responsibility.* Organizations may choose to have several team members, trained in the CVD process and tools, who can temporarily assist should a regular CVD analyst be unavailable for any reason, even if these additional team members do not typically do CVD day-to-day. Of course, handing off reports between temporary and full-time analysts leads to other operational concerns as previously discussed, so this must be done carefully. Organizations must also take care that these temporary team members are not pulled away from their own work so often that they themselves experience burnout.

A related possibility shared with us by a vendor is the possibility of *work rotation,* whereby team members are rotated in and out of CVD roles; rather than temporary, the rotation is permanent among a larger group of team members. An example would be an analyst spending one week in a CVD role, followed by two to three weeks on a different project or role. The same concerns in our above discussion would apply; organizations must be careful to balance time in and out of CVD roles in order to maximize the effectiveness of the rotation.

- *Allowing analyst independence.* Generally, you should trust your analysts to make good decisions during the report triage process, and empower them to make CVD decisions. Allowing analyst autonomy with management's specific blessing provides relief to analysts attempting to prioritize reports. Many reports will be incomplete, inaccurate, unimportant, or not actionable; allowing analysts to make the judgment on which reports deserve priority and which should be closed may help reduce work-related stress.
- *Allotting professional development time*. Analysts schedule some time each week to focus on professional development or projects. During these times, the analyst is not expected to perform CVD duties. Providing this time in whole-day chunks is preferable to spreading it out across the week. It is also important that during these days the analyst not be disturbed; urgent tasks should be handled by other on-duty analysts as much as possible. This suggestion may be combined with work rotation to allow for regular project work outside of the scope of CVD.
- *Seeking out automation*. We have encouraged analysts to document procedures and processes that need updating or could even be automated. Prototypes can be implemented and rolled out to decrease the cognitive workload of analysts. Processes and tools should be reviewed regularly to ensure they are aiding the analyst, rather than fighting the analyst.

Due to the possibility of burnout and the associated costs, the CERT/CC recommends that CVD capability be established within a well-resourced team or teams specifically created for this task, rather than concentrating the responsibilities to a small team, or even a single person. Our suggestions above may be helpful to combat analyst burnout, but do not form an exhaustive list of possible actions.

< 7.2 Operational Security | 8. Open Problems in CVD >

References

1. B. Rothke, "Building a Security Operations Center (SOC)," 29 Feb 2012. [Online]. Available: https://www.rsaconference.com/events/us12/agenda/sessions/683/building-a-security-operations-center-soc. [Accessed 24 May 2017].
2. S. Ragan, "Avoiding burnout: Ten tips for hackers working incident response," 30 April 2014. [Online]. Available: http://www.csoonline.com/article/2149900/infosec-careers/avoiding-burnout-ten-tips-for-hackers-working-incident-response.html. [Accessed 24 May 2017].
3. S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh and S. R. Rajagopalan, "A human capital model for mitigating security analyst burnout," in *Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, July 2015.