Information Security Workgroup
July 8, 2022
Zoom Session

Present:	Kelly Sebastian, Office of the President	Margie Coolidge, HR/AP
	Joe Borzellino, SEM	Joan Pedersen, UCM
	Trish Brock, R-EDGE	Craig Nelson, UD
	Rick Salomon, Student Affairs	Derek Gragson, CSM
	Bill Hendricks, CAFES	Dale Kohler, ITS Client Services (B)
	Arthur Heubner, ITS Client Services (A)	Doug Lomsdalen, ITS
	Troy Weipert, ITS Client Services (C/D)	Gary McCrillis, ITS
	Jon Vazquez, ITS	
Absent:	Jennifer Haft, A&F	Cheryl May, AA
	Matthew Ryan, CPC	Charles Chadwell, CENG
	James Mwangi, CAED	Kristy Cutter, OCOB
	Josh Machamer, CLA	Kyle Gustafson, ITS

I. ICT True-up Project

Overview of our 2021/22 ICT numbers:

- Total: 1,466 (completed/in-progress
- 21/22 Recap:
    - Completed: 236
    - Still in Progress: 26
    - Total: 262

Thank you to everyone who had submitted updated ICTs for the Level 1 review. Next, we will begin the Level 2 ICT review. Due to the number of products, we will split into two parts (Vintage, never reviewed by security; Expired L2 Reviews). We will ask for round one feedback/submissions in 60 days. We'll provide concise list of software/applications via email with two asks:

- Is the product still in service?
- Yes, request user/owner submit ICT.

Second round will capture Level 2 ICTs, that have expired; same questions, 45 days (since there are significantly fewer).

II. Annual Risk Self-Assessment (ARSA22)

Thank you for everyone's participation in this year's ARSA, we had 100% participation and completion of the questionnaire's this year.

Two general observations, that we will be looking at this year:

- Level 1 data: Location and access reviews.
- Software Installs: Verify KeyServer and Qualys agent deployments

The reports will be sent out on July 25th.

III. Qualys Update

Qualys surprised us with a significant price increase (and capabilities we didn't need); after discussing with Qualys leadership, we were able to get pricing back to 2021/22 pricing; however, it will be going up next renewal. During this year, we will be working with SBSS to find a new company to provide vulnerability management solution to Cal Poly.

IV. KeyServer Update

KeyServer is a tool providing deep insights into our computer systems. The data available to ISCs and Zones provides greater Asset Visibility. Currently we have 7,600 active agents deployed on computers and servers across the entire campus.

V. SOC Student Projects

The information security office has had students working in a Security Operations Center since Fall 2019 (our SOC-Lite). It's evolved into a SOC that handles typical Tier 1 activities (e.g., addressing phishing emails, following up on suspicious logins, and dealing with the fallout of a phishing campaign…). During the summer we have the ability to up our student hires and have them work on a variety of projects (things we'd like to do, but don't have the time to commit resources). Here's the Summer 2022 list of projects:

- Create Splunk dashboards, reports, and alerts for security events in AWS.
- Use newly-acquired Splunk SOAR to improve existing login alerts.
- Use Splunk SOAR to automate containment of compromised workstation/servers.
- Perform adversary simulation to support ISO projects.
- Implement risk-based alerting in Splunk Enterprise Security.
- Update vulnerability management reporting tools.

VI. Disable Legacy Email Protocols

On March 31, Microsoft published via a notice they will be disabling legacy email protocols effective October 1, 2022. This welcome security move will improve the security surrounding email accounts and will enforce the use of MFA (Duo). ITS Operations sent out initial communication to impacted users, users are actively upgrading their apps to versions that support MFA.

VII. Action Items

None.

VIII. Next Meeting

a. October 7, 2022, 1:10 pm – 2:00 pm, via Zoom