CyberSecurity Devils

Newsletter

March 2021

Semester Kickoff
- Events
- Guest Speakers

What is Happening?
- CVE
- SolarWinds Reflecting

Announcements
- Interactive Security Certification Roadmap

Semester Kickoff

We have had some AMAZING guest speakers to start off this semester strong. Make sure to visit the Events Page to see the current schedule and upcoming events!

In case you missed it:

On February 3rd, we had **Tom Castellano**, Senior Federal Security Manager – Digital Security Engineering Cloud Security Engineer at Microsoft speaking about his experience from the federal sector to the private enterprise.

On February 10th, we had **Lou Arnold**, Cloud Security Engineer at VIVA HEALTH. Lou talked about the importance of winning the hearts and minds of your colleagues and the practices that he uses in his job.

On February 17th, we had **Dr. Raschid Muller** of the Defense Information Systems Agency share story working with high-profile US. Agencies and how the perception of the field has changed in recent years.

On February 24th, we had both **Rachel Slater**, Software Engineer at Microsoft, and **Ryan Cornateanu**, Security Researcher for Crowdstrike. Rachel had some great insight for finding your niche in the field, and Ryan showed us how important networking and connections are in cyber security.

On March 3rd, **Dr. Calvin Nobles** discussed the human factors in engineering and cyber security. Specifically the struggle to eliminate the blind spot in cyber security via human factors.

*Some quotes from speakers **Lou, Ryan, and Rachel** on engineering and security.*

*Some quotes from **Dr. Muller, Tom, and Dr. Nobles** on the practices and human factors of security.*

Common Vulnerabilities & Exposures (CVE) in the News

Netop, a fortune 500 company was found to have multiple critical security vulnerabilities. Netop connects more than 3 million teachers and students with its software. Netop Vision Pro allows teachers to remotely perform tasks on students' computers, such as monitoring and managing their screens in real-time, restricting access to a list of allowed Web sites, launching applications, and even redirecting students' attention when they are distracted (Lakshman, 2021).

The flaws were relatively egregious, for example, privilege escalation and allowing for files to be written over on Windows machines or unencrypting the traffic flowing from teacher to student.

Netop fixed the vulnerabilities but still has yet to address the unencrypted traffic.

The article lists the specific vulnerabilities (CVE-2021-27192 through CVE-2021-27195) and a YouTube video showcasing how the vulnerabilities can be exploited.

Lakshman, R. (2021). Popular Netop remote learning software found vulnerable to hacking. *The Hacker News*

SolarWinds

One of the biggest stories of the year is the of various organizations using SolarWinds' Orion IT platform which was defined as a "highly-sophisticated, targeted and manual supply chain attack by a nation state". According to various articles on the subject, it is suspected that Russia was behind the breach and was able to access the systems by tampering with software updates to hide malicious code and gain total control of the system. While still many things are misunderstood about the extent of the attack, it is understood to be one of the most significant breaches as it allowed the attackers to have access to countless sensitive documents for months without being detected. SolarWinds, a fixture in the cybersecurity community, has begun to rethink their security practices, posture, policies to ensure that this does not happen again. Many of the customers that were left vulnerable by the attack were military, government agencies, and large corporations, totaling to an estimated 18,000 businesses and organizations.

Read for yourself…

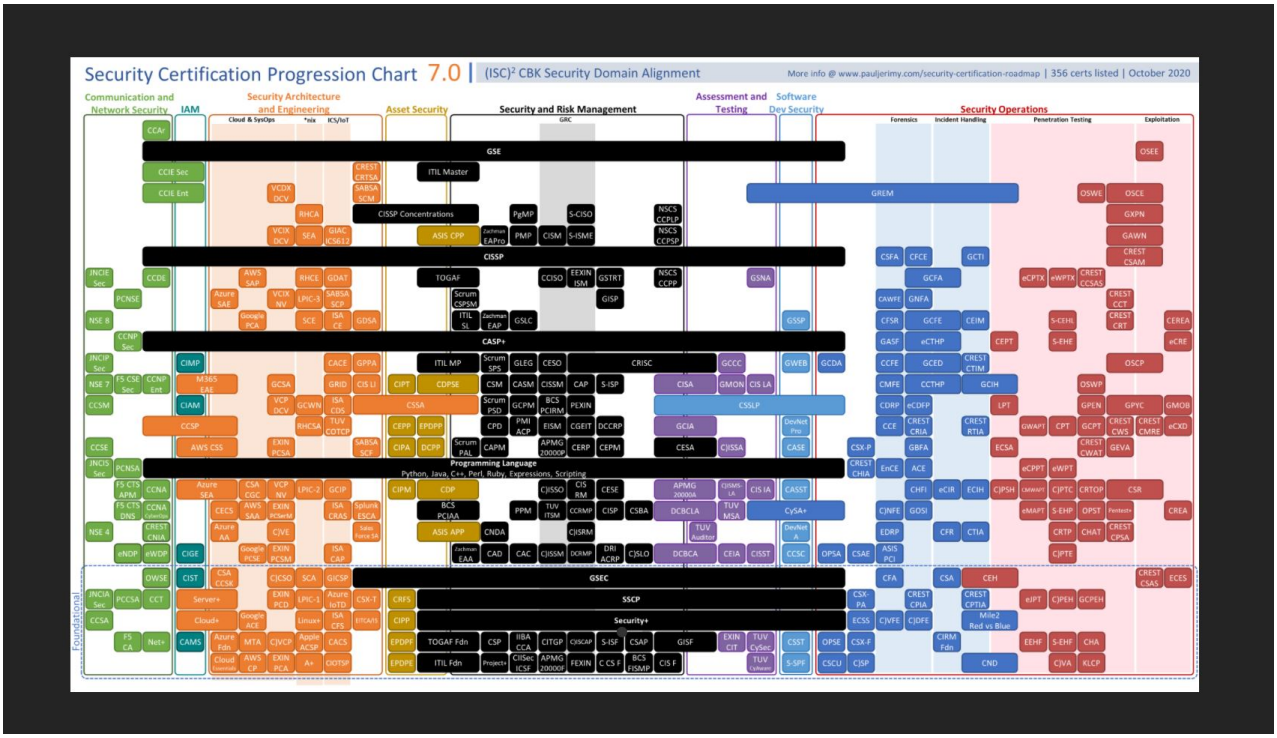
https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0PG?edition-redirect=uk

https://www.newsweek.com/alleged-russian-solarwinds-hack-probably-11-scale-1-10-cybersecurity-expert-warns-1554606

https://www.forbes.com/sites/kateoflahertyuk/2021/02/16/solarwinds-microsoft-reveals-new-details-about-sophisticated-mega-breach/?sh=69087b014879

Announcements and Resources

Interactive certification and career map: https://pauljerimy.com/



The Security Awareness Library Tool (SALT) has launched! This is a great resource for security concepts pulled from reliable sources like NIST and FireEye Intelligence Reports. Any student can access SALT at this website (https://securityapplearningtool-polyengineering.azurewebsites.net/).

YOUR VOICE WAS HEARD BY YOUR VOTE!

Pitchfork Award is a university-wide program that celebrates students, organizations and events that make an impact at ASU.

The Pitchfork Award winners are decided through a combination of live event votes and committee selection.

We will find out in April 2021!

slack

We have our own slack channel
#fso-cybersecuritydevils

Stay tuned for more awesome articles from our CyberSecurity Devils!

If you have questions, comments or would like to contribute content to your Newsletter.

Contact:

Jacob Harwood
CyberSecurity Devils President
jrharwo1@asu.edu

Dr. Tatiana Walsh
CyberSecurity Devils: NerdHerd Advisor
drtatiana.walsh@asu.edu

Sources

Fast-track your cybersecurity career for free, with scholarships to support your studies. Cyber FastTrack: Cybersecurity scholarships for U.S college students. (2021). https://cyber-fasttrack.org/.