MONTHLY NEWSLETTER

Consortium Networks

October 2023

Welcome to the October edition of the Consortium Networks Monthly Newsletter. This month was an incredibly exciting one with Consortium Networks being honored as a member of the Philadelphia100®, Fal.Con in Las Vegas and Consortium Networks receiving the Champion Partner of the Year (North Americas) award, and more.

In this edition of the newsletter, we are featuring an interview with Col. Candice Frost (Ret.), an “everything you need to know” about Penetration Testing, and a Consortium Networks “Ask an Expert” on PenTesting.

Did you recieve this newsletter via forward or email? Make sure to sign up here so you never miss an edition.

Story Behind the Story with Col. Candice Frost (Ret.)

Candice Frost’s commitment to national security includes three decades of public service. Her career in intelligence and cyber, includes operational tours of duty in the Balkans, multiple deployments to Afghanistan. Candice was instrumental in the

integration of women into combat arms and served close to half of her career in infantry divisions. She retired on September 1st as a Colonel from her last position as the commander of the Joint Operations Intelligence Command at the US Cyber Command. She currently works at Raytheon. A graduate of the United States Military Academy at West Point, Colonel (R) Frost holds masters degrees from Central Michigan University and the United States Army School of Advanced Military Studies. Her awards and decorations include the Bronze Star, Legion of Merit, and Combat Action Badge. She is also the recipient of the Billington Cybersecurity Workforce Development Award, Business Council for Peace Lifetime Mentorship Award, and the Lifetime Achievement Award in Muscatine, Iowa. She is a member of the Executive Advisory Council for AFCEA DC. Candice is an adjunct professor at Georgetown University teaching masters students in the Security Studies Program.

Read the Full Interview

Everything You Need to Know About Penetration Testing

In today's digital landscape, where cyber threats are becoming increasingly sophisticated and prevalent, safeguarding your network has never been more crucial. One of the most effective ways to further the security of your systems and protect your valuable data is through penetration testing.

This proactive approach to cybersecurity involves simulating various attack scenarios to identify vulnerabilities and weaknesses in your infrastructure. By conducting regular penetration tests, businesses can stay one step ahead of potential hackers and strengthen their defenses.

In this article, we will delve into the importance of penetration testing and how it can help fortify your digital fortress. From identifying vulnerabilities to prioritizing remediation efforts, we will explore the key benefits of penetration testing and why it should be an integral part of your cybersecurity strategy. So, let's dive in and discover how this vital practice can protect your organization from the ever-evolving threats in the digital world.

Continue Reading

Consortium Networks Honored with Philadelphia100® Award

Consortium Networks is honored to be recognized as one of the fastest growing companies in the greater Philadelphia region as part of the 2023 Philadelphia100®.
The Philadelphia100® is a merit-based award run by the Philadelphia100® Forum honoring the top 100 fastest growing, privately held companies in the region. The integrity of the process and the resulting list make the Philadelphia100® one of the most sought awards in the region.

Continue Reading

Why does Pen Testing matter?
You don't know what you don't know and, in this case, you can't fix what you're unaware of. If you are not aware of vulnerabilities in your environment, there is zero way for you to fix them. Penetration testing finds these vulnerabilities and prioritizes them for your team according to those gaps that are the most dangerous for your organization.

What kinds of organizations should invest in this kind of testing?
Everyone should do it. From small businesses to large companies, it is always a good idea to test your systems and environment. Not investing in penetration testing is something that you will regret at the end of the day.

What is the most useful part of testing?
In comparison to vulnerability scanning, pen testing shows in-depth the critical issues that can impact you and your business.

How should organizations go about choosing a provider for penetration testing or should they do it in house?
I would always recommend doing it through a third party. If you do it in house, you've already got a sense of the environment and will skip over things assuming that they are secure. Going through a third party eliminates anything related to familiarity or insider knowledge. This method is much better, in my opinion.
When choosing a third party provider, it is important that the organization has the appropriate credentials and former client recommendations. Affordability is also an important factor to consider.

In Other News

Chaes Malware can now access Chrome Devtools to steal data: Chaes Malware can now use Chrome DevTools to steal data from users' browser functions. The Chaes Malware first came on the scene in November of 2020 when it targeted e-commerce clients throughout Latin America. It escalated when they used 800 different WordPress sites to disseminate their malware. This malware is known to capture screenshots of user activity, capture passwords and credit card numbers, and steal online banking information.

Hackers are now using Help Desks to access Okta Accounts: Social engineering at its finest- Malicious actors have begun to use information technology employees by getting them to reset any MFA settings for highly exclusive Okta enterprise accounts. This allows them to move laterally within the network.

GhostSec Hacker group leaked an alleged Iranian tool: Hacker Group 'GhostSec' leaked the code of the Alleged Iranian surveillance tool. GhostSec claims to have the source code from FANAP, an alleged Iranian hacker group. So far, various components of the code have been released on Telegram.

Ukraine's computer emergency response team bested a cyber attack aimed at their energy sector: The computer emergency response team of Ukraine beat out the cyber attackers who tried to hit one of the critical energy infrastructure facilities. This attack started with a phishing email with malicious attachments and then was followed by an exfiltration of the data but the attack was ultimately blocked.

Las Vegas' MGM resort hit with potential ransomware attack: The infamous MGM resort was hit with a cyber attack on September 10th that destroyed its hotel operations. Experts believe it may be a ransomware attack and suspect the use of insider threat.

California Enacts Bill Targeting Data Brokers: California becomes one of the first to put a bill that targets data brokers into circulation.
In an unprecedented legislation California lawmakers passed the DELETE Act. This law allows California residents to visit a single website and delete their personal data from over 500 hundred or more data brokers. This could lead to this kind of law being passed all over the country.

CISA suggests a National Cyber Alert System: This would provide "actional information on threats and risks" and would be available to the public. CISA already provides a large amount of information and alerts if you are signed up for their services but this would be a much larger endeavor.

Organization Tasked with Protecting the Lakes and Rivers Along the Border of the US and Canada was Hacked: The IJC or the International Joint Commission experienced a cyberattack that hackers claim resulted in reams of stolen data. The NoEscape ransomware gang has claimed the attack but has not shown any proof of stolen data. They have given the IJC 10 days to respond to their requests.

USB Malware Infects Dozens of Networks: UNC53 a cyber group backed by the Chinese government is responsible for a new influx of USB drive based malware. This group is known to engage in espionage-centered cybercrime and is taking advantage of countries who are technologically behind.

After 10 days of Outages - MGM is Back and Ready for Business: Almost all operations including gaming, room bookings, and online reservations were shut down at MGM for 10 days. They are now back in operation, but the amount of revenue lost between the gambling and reservations remains unknown. The attack involved an AlphaV encryptor and social engineering.

'Sandman' targeting Telecommunication Services Around the World: The 'Sandman' threat actor group has been targeting telecom providers throughout the Middle East, Western Europe, and South Asia. They are using a modular info-stealing malware named 'LuaDream.' Their malicious activity was discovered by SentinelLabs and the full extent of the attacks is currently unknown.

Apple Fixes Three Additional Zero-Day Vulnerabilities in Emergency Security Update: After discovering three new zero-day vulnerabilities in iPhones and Apple computers, Apple released an emergency update to patch the actively exploited vulnerabilities. All of these vulnerabilities were found in much newer apple products than would be expected and can allow outsider access with escalated privileges.

New threat actor 'AtlasCross' Deploying new Red Cross Phishing Attacks: The AtlasCross, an up and coming threat actor, has begun using Red Cross themed phishing attacks to deploy two previously unknown backdoors called DangerAds and AtlasAgent. One of the ways that they are trying to get past traditional phishing blockers is by posing as a blood drive donation for the Red Cross.

Windows Targeted by new ZenRAT Malware through Fake Password Manager: Installation packages of the Bitwarden password manager are the root of the new ZenRAT malware attacks. Customers are downloading the Bitwarden password manager and later finding themselves with the remote access trojan installed on their device.

Blacktech Group Hacking Cisco Firmware; Targeting US, Japan: Chinese-linked hacking group Blacktech was covertly using Cisco routers to attack US and Japanese companies. Attackers are currently targeting small companies attached to large multinational businesses based in the United States and Japan.

The FBI, NSA, CISA, and the Japanese Police Released an Advisory on Chinese Actors: The advisory is based around threats from Blacktech. BlackTech is a People's Republic of China backed Advanced Persistent Threat Group. The advisory details the specifics around the hacking group.

ABOUT CONSORTIUM NETWORKS

Your Trusted Cyber Concierge

WHO WE ARE

Consortium Networks is a cybersecurity risk, technology, and networking organization on a joint mission to connect and educate the community. We founded Consortium to change the “game” and help our clients make sense of the spaghetti labyrinth they call cybersecurity. By mapping our clients’ controls to industry standards and risk, we help them reduce complexity and risk to their organization and people.

The outcome: clients will quickly understand their gaps and realize the impacts of their investment decisions, strengthening their cyber hygiene, and, ultimately, protecting the business.

Our Concierge way sets us apart and follows four timeless principles of customer service: attitude, consistency, service, and teamwork. We are devoted to helping others selflessly in both our work and personal communities.

WHO WE HELP

CISOs & IT Professionals

We save you time and keep you up-to-date by providing the latest technology content, expertise, and product information and reviews.

IT Vendors

Emerging and established vendors can present their products to a group of CISOs to obtain feedback and exposure and learn how their products are being used.

Our Community

Consortium is committed to recognizing and helping others in our both our work and personal communities.

OUR MISSION

Our mission is to be the most trusted partner in reducing cyber complexity and mitigating risk to promote a safe, secure, and resilient environment for companies and people.

OUR VALUES

We are a veteran-owned business built on Trust, Integrity, Collaboration, and Altruism. We have high ethical standards and infuse thse values into every aspect of our company.

www.consortium.net 800-530-8350 contact@consortium.net

HOW WE HELP

CONSORTIUM NETWORKS

OUR TECHNOLOGY PARTNERS

corelight, tenable, VERACODE, expel, HYPR, ExtraHop, Recorded Future, VARONIS, SALT, FLASHPOINT, zscaler, splunk>, Abnormal Security, CROWDSTRIKE, okta, WIZ, sumo logic, SUREFIRECYBER, Island, AXONIUS, paloalto NETWORKS

OUR SERVICES

- Cybersecurity Incident Response Preparedness
- Cybersecurity Policy Library Development
- Cybersecurity Risk Assessments
- Penetration Testing Services
- Request for Proposals (RFP) and Procurement Advisory

The Consortium Networks professional services team works with our clients to tailor our services to best fit your organization's needs while preparing you to combat cyber threats, mitigate risk, and build resilience.

THOUGHT LEADERSHIP

WASHINGTON WATCH

Our semi-annual publication "Washington Watch" provides a birds-eye view of all conversations around cybersecurity happening in the nation's capital.

VENDOR SPOTLIGHTS

Every month the Consortium Networks team brings together our analysis of the latest cyber technology offerings brought into our network.

MONTHLY NEWSLETTERS

Our Monthly Newsletter brings the most relevant trends, news, and policy changes directly to your inbox every month.

EXPERT INSIGHTS

From our expert-driven blog to insightful interviews with impressive figures in cybersecurity, Consortium Networks provides a wide variety of resources for your organization

www.consortium.net 800-530-8350 contact@consortium.net