THE CYBER INFORMER

A Connect I.T. Solutions Quarterly Newsletter - Q1 2024

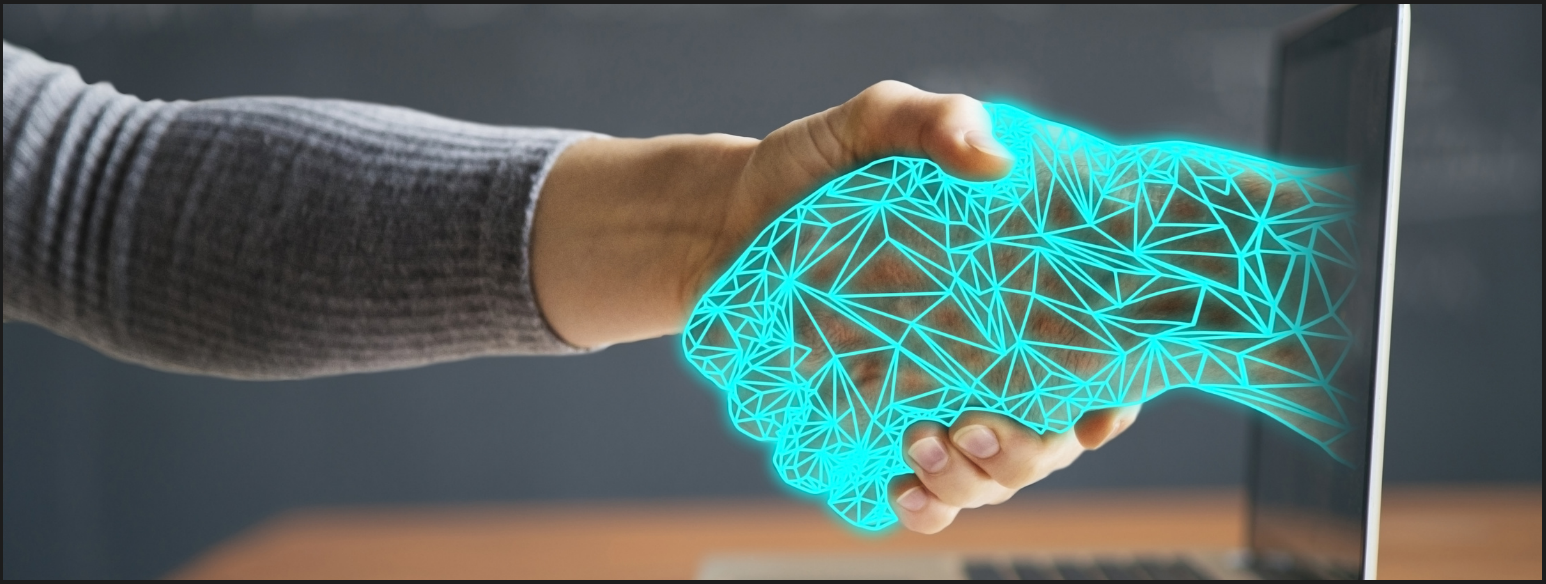


TABLE OF CONTENT

WWW.CITSUS.COM

FROM THE CEO'S DESK:

Hello to all and may your 2024 be filled with joy and prosperity.

Last year was an interesting year in cybersecurity. With the onslaught of AI and Machine learning, we at Connect I.T. Solutions have taken significant steps in order to keep our clients out of the headlines. As bad actors continue to use the same technologies to defeat us as we use to defend, "Defense in Depth" will become all the more critical.

Global politics and economics are still reaping havoc on supply chain cost and delivery as we've seen longer lead times and increasing prices to I.T. infrastructure solutions. Trends toward hardware agnostics solutions are on the rise in order to capitalize on existing fixed-expense spend. Keep an eye out for "enterprise-ready" open-source solutions.

One of the key functions we perform for our clients at Connect I.T. Solutions is to keep ahead of the learning curve in cybersecurity and networking. As bad actors know how to defeat many existing enterprise solutions, we spend a significant amount of our time researching and evaluating leading-edge products to stay ahead of these perpetrators. As trusted advisors, this saves our clients a significant amount of time when deciding to expand, layer or refresh critical cyber and I.T. assets, we return "time", one of the most expensive resources, back to the bottom line of our clients.

Below we have listed top trends in our industry that we have been tracking and researching. This will also be reflected in some of the new solutions we have onboarded for 2024 to address these trends.

Please feel free to reach out to me or anyone on our staff to discuss any of the trends or solutions you see in this newsletter. As always, your feedback is always welcome as are suggestions for upcoming newsletters or topics of research.

Best to all,

Bill Rubin

NEWSLETTER

3 MAJOR CYBERSECURITY TRENDS IN 2023 THAT HAVE HAD MAJOR IMPACT ON OUR CUSTOMERS

1. SOPHISTICATED MULT-VECTOR PHISHING ATTACKS

The most successful phishing compromises leverage a combination of deception tactics, psychology triggers, technology cloaking, surprise vectors outside email, and steady testing to determine what strategies work best on their targets. The tactics leveraged by threat actors continues to grow more personalized, stealthy, and technically savvy. As email security and end user awareness improves, hackers are shifting to blended techniques across platforms. Staying ahead of emerging exploitation strategies remains crucial for security teams seeking to keep their organizations safe. Proactive thinking is required as attacks escalate in complexity.

2. ENHANCED RANSOMWARE STRATEGIES

Cybersecurity experts expect ransomware attacks to become more sophisticated in their delivery in 2024. Threat actors may extort funds through gradual payment demands over an extended timeframe, rather than locking victims out of their systems immediately. These stealthier approaches aim to delay detection. Organizations will need to implement intelligent behavioral analysis solutions to identify risks early on, rather than rely solely on signatures.

3. CRITICAL INFRASTRUCTURE IN THE CROSSHAIRS

Hospitals, power facilities, water treatment plants, and other critical infrastructure sites are increasingly vulnerable targets for financially motivated hackers. By crippling healthcare access or energy availability, cyber-attacks now pose significant physical and economic damage potential. Bolstering the cyber resilience of hospitals, utilities, and other infrastructure providers against malware and denial-of-service tactics serves as an urgent priority for municipalities and governments alike in the coming year.

WWW.CITSUS.COM

NEWSLETTER

HIGHLIGHTED SOLUTIONS @ CONNECT I.T. SOLUTIONS ADDRESSING INDUSTRY TRENDS

HELPING YOUR SOC PROTECT CRITICAL INFRASTRUCTURE

Horizon3.ai leverages AI and machine learning to provide real-time threat protection. It uses behavioral analysis to detect attackers as they recon and attempt to compromise accounts and assets. What makes Horizon3 stand out is its integrated PEN testing engine to simulate real-world attacks. The PEN testing continuously tests your entire environment for vulnerabilities that a hacker could exploit, without any impact on operations. It launches over 30,000 breach methods to uncover gaps across Web, API, mobile, network, host and OT environments.

These full-scale simulations are like handing your environment over to a team of ethical hackers. Horizon3 does this safely and smartly using attack intelligence to create missions that are relevant to your infrastructure. Any vulnerabilities uncovered are prioritized by risk level for efficient remediation to get your security posture where it needs to be. By continuously validating defenses with PEN testing, Horizon3 stops attacks in their tracks within seconds before they have a chance to escalate or cause damage.

TO DISCUSS HOW AUTONOMOUS PEN TESTING CAN ELEVATE YOU SECURITY POSTURE CONTACT US AT CONNECT I.T. FOR MORE INFORMATION 888-246-6350 OR INFO@CITSUS.COM

PUT A SECURITY BUBBLE AROUND YOUR EMPLOYEE'S COMMUNICATION CHANNELS

SlashNext helps protect your users from targeted phishing attacks using AI and machine learning. It detects and mitigates brute force, social engineering, and credential harvesting attempts across email, network and cloud in real time.

Specifically, SlashNext has leading protection against Business Email Compromise (BEC) and mobile-based phishing. SlashNext analyzes inbound email content and sender patterns to uncover targeted spear phishing attempts, the most common vector for BEC schemes. This prevents employees from mistakenly wiring funds or sending sensitive data to criminals posing as trusted contacts.

Additionally, SlashNext provides browser and mobile SDKs that protect your employees as they access content across devices. The mobile SDK scans each URL click in real time to classify threats. If a user clicks a phishing link on their phone, SlashNext will block the page from loading. This offers defense beyond traditional email filters. Employees can browse safely knowing SlashNext has their back across all phishing entry points.

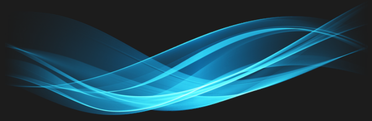
TO LEARN MORE ABOUT THE LATEST DEVELOPMENTS IN EMAIL AND MULTI-VECTOR CHANNEL PHISHING SECURITY CONTACT US AT 888-246-6350 OR INFO@CITSUS.COM

STOP PATCHING SECURITY HOLES IN APPLICATION. DEVELOP WITH SECURITY IN MIND.

Secure Code Warrior is a hands-on cybersecurity training platform to help developers write secure code. With a comprehensive curriculum including languages like Java and Python, developers can upgrade their skills through coding challenges and validation labs. Custom pathways allow you to tailor training to your software development lifecycle.

What makes Secure Code Warrior unique is how it helps organizations stay within compliance regulations around software security and privacy. The platform tracks all developer training activity and security competence development. This auditable progress trail helps you comply with directives like the EU Cybersecurity Act, which mandates evidence of cybersecurity skill development. Secure Code Warrior also incorporates security requirements from major standards like PCI DSS, HIPAA, and GDPR into its training. By completing pathways around these regulations, developers get verifiable education on building compliant code. This helps protect customer data and avoid significant fines due to violations.

TO LEARN MORE ABOUT TRAINING YOU APPLICATION DEVELOPMENT TEAM TO CODE WITH "SECURITY IN MIND" CONTACT US AT 888-246-6350 OR INFO@CITSUS.COM FOR A DISCUSSION



USE THE CLOUD AS YOUR NETWORK INFRASTRUCTURE

Alkira offers a revolutionary way to build networks called a cloud-delivered network. Instead of relying on legacy hardware, Alkira creates networks using the cloud itself. Their Network Cloud service builds, optimizes, operates, and secures networks globally through a single cloud interface.

This means you can leverage the power of the cloud for all of your connectivity and security needs. Alkira integrates natively with clouds like AWS, Azure, and Google Cloud so you have one common interface to manage multi-cloud networks. Their software-defined architecture allows businesses to scale connectivity on-demand without the hassle of configuring additional appliances or ACLs.

With Alkira's global backbone, you can achieve consistent security and performance between regions or cloud providers. Alkira also offers advanced services like cloud firewalls, routing, VPN, and analytics through their platform. Say goodbye to complex MPLS management across continents and achieve the promise of a simplified cloud experience.

TO LEARN MORE ABOUT HOW ALKIRA IS REVOLUTIONIZING NETWORKING, CONTACT THE CLOUD CONNECTIVITY EXPERTS AT CONNECT I.T. SOLUTIONS TODAY! 888-246-6350 OR INFO@CITSUS.COM

NEWSLETTER

JOIN US IN 2024 – HERE ARE UPCOMING EVENTS CONNECT I.T. SOLUTIONS WILL BE AT IN 2024. LET'S MEET UP!

- THURSDAY, JANUARY 18TH - FUTURECON LOS ANGELES CYBERSECURITY CONFERENCE– HILTON LAX
- THURSDAY, FEBRUARY 22ND - DATA CONNECTORS AUSTIN – SHERATON AUSTIN HOTEL AT THE CAPITAL
- MAY 6-9 – RSA CONFERENCE – MOSCONE CENTER – SAN FRANCISCO
- AUGUST 3-8, 2024 - BLACK HAT USA - MANDALAY BAY CONVENTION CENTER, LAS VEGAS

MORE TO COME . . .

FEATURED VENDORS

HORIZON3.ai

~~TRUST~~ ~~BUT~~ VERIFY

SECURE CODE WARRIOR

SLASHNEXT

alkira

About Us: Connect I.T. Solutions' mission is to supply innovative and objective solutions that help our customers meet their needs of having a secure, high-performing, reliable and manageable network. In doing this, we design systems so that our clients' investment will be preserved years down the line. We design, architect, build and supply systems that are future-proof and keep pace with the growth of your business.

WWW.CITSUS.COM