Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider



VOL. 1 · ISSUE 59

Cyber Shield

November 09, 2026

Essential cybersecurity intelligence for small and mid-sized businesses — powered by AI, delivered by Intelligent Automation, LLC.

INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

This Week in Cybersecurity



Default 'admin:admin' Server Password Helps Researchers Hack Two Automakers, Unlock and Start Cars



Web3Auth Flaw Exploited to Steal Keplr Crypto, Provider Empties Other Wallets for Safety



LNbits Urges All Operators to Shut Down Their Bitcoin Lightning Wallet Servers Amid Attacks

INTEL

Cyber Threat Intelligence



Default 'admin:admin' Server Password Helps Researchers Hack Two Automakers, Unlock and Start Cars



Web3Auth Flaw Exploited to Steal Keplr Crypto, Provider Empties Other Wallets for Safety



LNbits Urges All Operators to Shut Down Their Bitcoin Lightning Wallet Servers Amid Attacks

INTEL

Threat Intelligence — Continued

Taiwan-Based Hacker Used BOSSAI AI Agents to Steal Taipei Emergency Dispatch Records

Former OpenAI Engineer Pleads Not Guilty to Planting Covert Device in Executive Meeting Room

U.S. Agencies Warn Refrigeration Controller Attacks Could Cause Fires and Inventory Losses

ISC Stormcast For Monday, November 9th, 2026 https://isc.sans.edu/podcastdetail/10170, (Mon, Nov 9th)

Scans for Sshole Vulnerability (CVE-2026-123158), (Sun, Nov 8th)

💡 WEEKLY TECH TIP

Change Default Credentials Immediately on All Systems

Default passwords like "admin:admin" remain shockingly common and give attackers trivial access to critical systems, from servers to IoT devices. This week, researchers exploited default credentials to remotely unlock and start vehicles from two major automakers.

Step 1: Inventory all devices, servers, applications, and network equipment in your environment.

Step 2: Change every default username and password to strong, unique credentials immediately.

Step 3: Document new credentials in a secure password manager, never spreadsheets.

Step 4: Schedule quarterly audits to catch newly deployed devices with default settings.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, November 9th, 2026 https://isc.sans.edu/podcastdetail/10170, (Mon, Nov 9th)

Scans for Sshole Vulnerability (CVE-2026-123158), (Sun, Nov 8th)

ISC Stormcast For Friday, November 6th, 2026 https://isc.sans.edu/podcastdetail/10168, (Fri, Nov 6th)

Vulnerability Scans for Older Cisco IOS Vulnerability / Opt-Out Headers, (Thu, Nov 5th)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, November 9th, 2026 https://isc.sans.edu/podcastdetail/10170, (Mon, Nov 9th)

Scans for Sshole Vulnerability (CVE-2026-123158), (Sun, Nov 8th)

ISC Stormcast For Friday, November 6th, 2026 https://isc.sans.edu/podcastdetail/10168, (Fri, Nov 6th)

🛡 NOVEMBER AWARENESS

Holiday Shopping Scams

Security Awareness Spotlight: Holiday Shopping Scams As your employees start their holiday shopping, scammers are counting on distraction and urgency to slip fake shipping notifications, too-good-to-be-true deals, and fraudulent gift card requests past your team's defenses. These scams don't just target personal inboxes—criminals often impersonate executives asking staff to "quickly grab some gift cards for clients" or send fake invoices that look like legitimate vendor charges during the year's busiest purchasing season. The financial damage from one employee falling for a business email compromise or approving a fake invoice can easily run into thousands of dollars, not to mention the time lost cleaning up the mess. **Do this today:** Send a quick company-wide message reminding your team that you will never ask them to purchase gift cards via email or text, and that any unusual payment requests—even if they appear to come from you—should be confirmed

ACTION ITEM

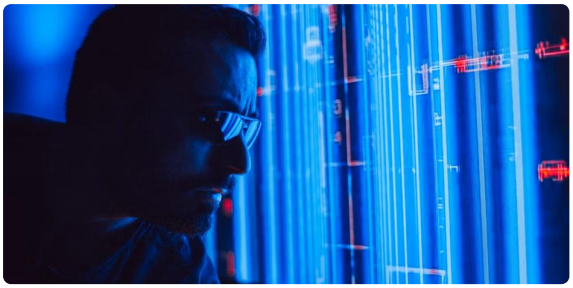
Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

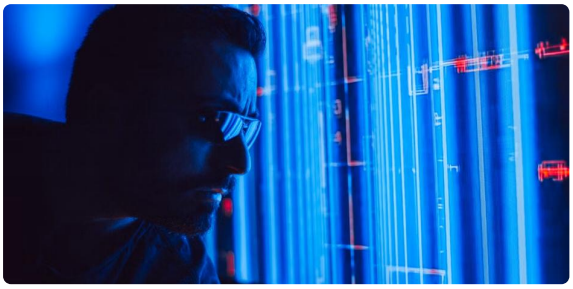
Protecting Your Business



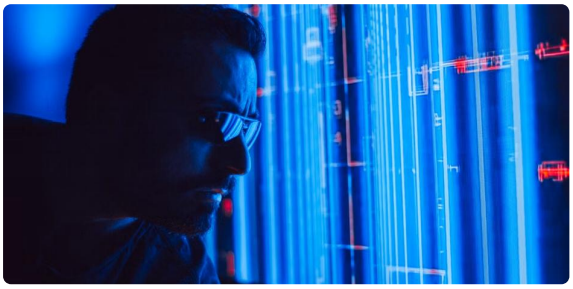
Cyber chief: UK facing AI-powered attacks on critical infrastructure within two years



Artificial intelligence and cyber intrusion



From industry concern to practical action: the value of working with regulators



Critical security issue affecting PHP

INNOVATION

Cybersecurity Advancements

Plex2Shell Exploited Against QNAP NAS Users

Iris Plaza Breach May Have Exposed Data of 7.7 Million Customers

Italy’s Meloni Blames Pro-Russian Hackers for Leak of Foreign Minister’s Data on the Dark Web

Hackers Exploiting ‘SSHole’ Authentication Bypass in OpenSSH

CTO'S DESK

From the Desk of Daniel Ramos



Daniel Ramos
Chief Technology Officer
Intelligent Automation, LLC | Fairfield, NJ
Managed Cybersecurity Service Provider

This week's headlines tell a troubling story that keeps me up at night: the fundamentals still matter more than the fancy threats. While everyone worries about sophisticated AI-powered attacks, two major automakers were compromised because someone left "admin:admin" as a server password. Let that sink in for a moment.

We're living in an era where AI agents can infiltrate government systems and exploit cutting-edge Web3 vulnerabilities, yet the most damaging breaches often trace back to elementary security hygiene. Default passwords, unpatched systems, and basic misconfigurations remain the unlocked doors that criminals walk through first.

Here's what I tell every client: before you invest in the latest threat detection platform, ensure your foundation is solid. Change those default credentials. Enable multi-factor authentication. Conduct regular access reviews. These aren't glamorous solutions, but they stop the majority of attacks dead in their tracks.

The good news? These fundamental protections are entirely within your control and budget. Start today by auditing just one system. You'll be amazed what you find—and how much safer you'll feel once you fix it.

CONNECT WITH DANIEL
linkedin.com/in/iamdanielramos · daniel.ramos@intelamation.com



Your Cybersecurity Partner for the Digital Age

Serving small and mid-sized businesses since 2013

336 US Highway 46, Fairfield, NJ 07004

(888) 711-4521 · intelamation.com

Read online: newsletters.intelamation.net

© 2026 Intelligent Automation, LLC · All rights reserved