CYBERSECURITY AWARENESS MONTH: WHY WE'RE TAKING A NEW ROUTE

RETHINKING CYBERSECURITY FOR A NEW ERA

Why We're Going Off Script

Every October, you've probably seen the same cybersecurity advice: "Use strong passwords." "Think before you click." "Update your software." All good tips, but let's be honest, you already know them.
This year, we're shifting gears.

Cyber threats are evolving fast and so are the ways we work: Remote teams, AI assistants, VIP impersonation, ransomware-as-a-service. The risks of today require more than yearly reminders; they need a deeper look and a more modern conversation.

That is why we've developed our own set of themes for Cybersecurity Awareness Month. Each week focuses on a real-world risk tied to how we live and work today. It's not just about avoiding mistakes. It is about becoming an active part of a secure culture.

What to Expect This Month

Week 2: Agentic AI & Your Digital Twin
AI is acting on your behalf, sometimes without your knowledge. Learn how to use it safely, avoid overexposure, and protect your digital identity.

Week 3: Securing Wizards and Whales
Admins, engineers, and executives are top targets. We'll show you how to protect privileged users and high-profile leaders, maybe even yourself.

Week 4: Crisis Mode: Ready or Ruined?
When a breach happens, chaos isn't a plan. This week is about incident response, your role during a cyber crisis, and how to stay cool under pressure.

Week 5: Secure Culture Ambassadors
Security isn't just IT's job. Find out how everyday employees can be agents of change, role models, and protectors of company culture.

Let's stop just "raising awareness" and start building real security habits and let's do it together.

WHY WE'RE DITCHING THE STANDARD CSAM PLAYBOOK

A STRATEGIC PIVOT TOWARD MODERN CYBER RISK

Elevating the Conversation

Every year, October rolls around with the same talking points: password hygiene, software updates, and suspicious links. While essential, these messages underserve our technical teams and fail to reflect the complexity that defines cybersecurity.

We're not following that script this year.

Instead, we're introducing a modernized set of CSAM themes, designed to engage technical professionals and raise the bar across the entire organization. These weekly spotlights are grounded in threat intelligence, human behavior, and operational realities. They are as much about culture and resilience as they are about controls and compliance.

Let's move beyond compliance checklists. This CSAM, we're aiming for impact, not repetition.

A Glimpse at the Road Ahead

Week 2: Agentic AI & Digital Twins
AI agents and digital twins are expanding the attack surface. We'll explore responsible use, shadow AI risks, and how to establish AI security guardrails in your enterprise.

Week 3: Privileged Access: Wizards & Whales
From system administrators to senior executives, certain users have disproportionate risk. This week focuses on lateral movement, social engineering, and securing human infrastructure.

Week 4: Cyber Crisis Readiness
True resilience means cross-functional response. We'll dive into tabletop exercises, communications under duress, and aligning SOC playbooks with business continuity.

Week 5: Building a Secure Culture with Ambassadors
Your best line of defense may be cultural. Learn how to activate technical and non-technical ambassadors to scale secure behaviors and reduce organizational blind spots.