Black Hat 2024: Key Takeaways and Trends

Posted on August 28, 2024

WhoisXML API representatives were among the more than 20,000 security professionals from 117 countries who gathered at Black Hat 2024 held at the Mandalay Bay Convention Center in Las Vegas on 3–8 August 2024.

The annual conference once again delivered on its promise of showcasing the latest security advancements and exposing emerging threats. As our team continues to absorb the valuable insights gained from Black Hat 2024, we put into writing this recap to capture the key themes and highlights of the conference.

Third-Party Risk Management

Supply chain security was a major talking point at Black Hat 2024, and for good reason. These risks keep security professionals up at night, including ThreatLocker CEO and Co-Founder Danny Jenkins. During his mainstage session, "Understanding and Reducing Supply Chain and Software Vulnerability Risks," Jenkins emphasized the importance of identifying backdoors and unintended vulnerabilities in IT environments.

Attendees extensively discussed the need for effective third-party risk management strategies. These strategies include integrating security into the software development process, improving supply chain resilience, and continuously tracking the security posture of the supply chain.

Conducting thorough vendor risk assessments is crucial to building supply chain resilience. These assessments typically involve asking questions like, "Can their Internet infrastructure be trusted?" To answer that, organizations may check the reputation of the domains and IP addresses associated with vendor software products. This type of due diligence is critical in light of Verizon's Data Breach Investigation Report (DBIR) finding that 15% of data breaches involved third parties.

Artificial Intelligence in Security

Artificial intelligence (AI) was a prominent theme at the conference, with many vendorsshowcasing AI-powered security products and solutions. Several sessions also explored thepotential benefits and risks of utilizing AI in security.

For one, Swimlane CISO Mike Lyborg and Security Weekly's Mandy Logan talked about how AI can streamline security operations (SecOps) by summarizing, categorizing, and prioritizing information. This tactic enables security teams to respond faster and more effectively with risk remediation and mitigation strategies.

AI and automation in security are likely game changers, considering the massive volume of data SecOps teams process every day. In fact, they receive an average of 50 security alerts per day. Additionally, they may need to sift through billions of historical DNS, IP, and domain data points to obtain much-needed context and cyber intelligence. AI can make data analysis easier and quicker, giving security teams more time for other crucial tasks.

Convergence of Cybersecurity and Fraud Prevention

Another session that specifically caught our attention was that of Allison Miller, faculty member at IANS Research, who discussed the growing overlap between cybersecurity and fraud prevention. Her studies revealed that both fields are increasingly using similar technologies to address different aspects of the same problem. We couldn't agree more since we've seen clients from both sectors leverage the same sets of cyber intelligence sources.

What does the merging of cybersecurity and fraud prevention look like? Here's an example. While cybersecurity teams may detect the presence of botnets or signs of a brute force attack, fraud prevention specialists are looking at the same issue as an account takeover waiting to happen. In essence, "both teams are dealing with different manifestations of the same problem."

This convergence highlights the need for a unified approach to security that encompasses both cybersecurity and fraud prevention. Sharing information and collaborating allows organizations to better protect themselves from a wide range of threats.

Universal Zero Trust Network Access

Another recurring theme at Black Hat 2024 was the rising adoption of zero-trust architecture across all facets of an organization's network infrastructure, encompassing cloud environments, enterprise applications, and on-premises networks.

Universal zero trust network access (ZTNA) ensures that only authorized users who have been verified and authenticated can access specific applications and data, regardless of location or device. It aligns with the growing trend of organizations embracing hybrid work models and the need for secure access to both cloud-based and on-premises resources.

For a security solution to align with ZTNA, it must be able to identify all users, implement policy controls, and update policies instantly. This technique may require integrating extensive DNS data to aid with user identity verification and device posture assessment, among others.

About WhoisXML API

WhoisXML API is a leading provider of cyber intelligence solutions that can significantly enrich AI models with valuable domain, IP, and DNS data.

Our Know Who You're Talking To (KWYTT) Intelligence empowers enterprises to implement zero trust strategies through in-depth third-party assessment, accurate fraud detection, and continuous cyber risk monitoring.

We maintain strong collaborative relationships with major data providers worldwide, including domain registries and registrars, ISPs, and security agencies. Our network of data aggregators enables us to provide comprehensive, accurate, and up-to-date domain, IP, and DNS information.

For several years now, WhoisXML API has been recognized as an Inc. 5000 honoree and one of the Financial Times Top Fastest-Growing Companies. Our solutions are trusted by more than 52,000 users, including Fortune 500 companies, leading security firms, and organizations across various industries.