RSA Conference 2024: Cybersecurity Trends and Takeaways

Posted on June 14, 2024

WhoisXML API representatives joined more than 40,000 people who attended the recent RSA Conference held in San Francisco, USA, on 6–9 May 2024. The event brings together cybersecurity professionals from around the world every year.

Our team was impressed by the thought-provoking discussions, cutting-edge innovations, and brilliant people we encountered, familiar faces and new acquaintances alike. To provide a glimpse of our experience, here is a recap that dives into some of the key themes and insights that emerged from this premier event.

Cybersecurity Needs AI, and AI Needs Security

If there's one glaring trend made evident during the conference, it's that cybersecurity vendors are increasingly leveraging artificial intelligence (AI) by tapping into its ability to analyze massive amounts of data for advanced threat detection and protection. This trend aligns with recent statistics that say the market for AI in cybersecurity is expected to significantly grow from US$24 billion in 2023 to US$134 billion by 2030.

Predictive analytics is one of the strongest applications of AI in cybersecurity. It can analyze past security incidents and historical attack data to identify trends and predict future threats. For example, AI algorithms can detect the types of domains threat actors may use in phishing, fraud, and other malicious campaigns.

Undoubtedly, AI plays a crucial role in enabling cybersecurity vendors to catch up with, and perhaps even overtake, the increasing sophistication of cyber threats.

However, security solutions should also concurrently apply security frameworks to generative AI strategies. IBM executive Kevin Skapinetz aptly describes this urgent need in his keynote, Securing New Limits: Protecting the Pathway for AI Innovation, where he said, "And while AI is aggregating and integrating crown jewels, it is also uniquely capable of actually creating new crown jewels. In some ways, like prompts and responses, become sort of the printing press of high-value data, massively expanding what we now need to protect. So, as we push toward these new limits, we also must secure them."

Secure by Design

The need to secure AI-powered cybersecurity solutions leads us to the next highlight of the RSA Conference—the momentous signing of the Secure by Design pledge by more than 60 organizations.

Secure by Design is a cybersecurity philosophy that emphasizes building security into enterprise software and services from the very beginning instead of bolting it on as an afterthought. While the pledge is voluntary, participating cybersecurity vendors are committed to working toward seven goals within one year of signing, namely:

- Increase the use of multifactor authentication (MFA) across their products
- Reduce the use of default passwords
- Reduce the number of vulnerability classes
- Increase their customers' application of security patches
- Publish a vulnerability disclosure policy (VDP) authorizing the public to test their products
- Become transparent and timely in vulnerability reporting
- Enable customers to gather evidence of intrusions affecting the vendor's products

Future-Proofing SOCs

The keynote by Splunk's Gary Steele, Revolutionizing the SOC for the Future Threat Landscape, shed light on another critical issue—the immense pressure security operations centers (SOCs) face in keeping pace with the current and evolving threat landscape. This pressure can take a toll on SOCs and entire organizations. In fact, 83% of security professionals say that burnout has ledto mistakes that eventually caused security breaches.

With cybercrime becoming more sophisticated and aggressive, SOCs need future-proofing. Steele states this initiative involves automation, data federation, and consolidation to streamline operations.

Automation

AI-powered automation enables security analysts to focus on critical aspects, such as investigating complex threats and developing strategic security plans. It can help SOCs tackle overwhelming amounts of security data, freeing analysts from time-consuming tasks like log analysis, incident triage, and threat hunting. Automating repetitive tasks can significantly reduce analyst workload and improve overall SOC efficiency.

Data Federation

The need for "security at scale" was another key takeaway from the conference. A recurring theme in presentations was the challenge of detecting threats across complex data environments, especially considering the vast amount of data organizations generate today. One solution that emerged as a game-changer for SOCs is data federation.

Data federation allows security teams to access data from various sources—databases, applications, and cloud storage—without physically copying or moving the data.

Platform Consolidation

Keynote speaker Gary Steele also talked about the "need to have a single integrated environment that delivers context, insights, and AI-delivered actions. Not a plethora of tools." He emphasized

how organizations may end up with fewer tools integrated into an open and extensible SOC environment. As a result, the SOC becomes a place where analysts obtain insights and rapidly take action.

Therefore, platformization was one of the buzzwords at the conference. It aims to streamline security operations by creating a cohesive security system instead of using various solutions from different companies.

Platformization is similar to vendor consolidation, where organizations reduce the number of security tools and vendors they manage. Either way, security teams have to ensure that all newly adopted technologies work seamlessly with existing systems.

About WhoisXML API

As a leading provider of cyber intelligence solutions specializing in domain, IP, and DNS data, the key trends and takeaways we encountered at the RSA Conference resonate deeply. We deliver our intelligence sources notably through secure RESTful APIs, simplifying data access and facilitating data federation.

Our predictive threat intelligence data feeds leverage AI predictive analytics capabilities, giving security teams the ability to detect potential phishing and malware domains at the time of registration. Since we understand the need for seamless integration, our data sources are well-parsed and unified to work well with existing security solutions.

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.

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