Cybersecurity in 2025 and Beyond: Top Predictions

Posted on January 29, 2025

Change is the only constant in this world, and cybersecurity is no exception to that rule. While no one can know for sure what will happen in 2025 and the years to come, one thing is certain: organizations must adapt to new cybersecurity trends to keep pace with peers and adversaries alike.

For one, organizations will need to employ a proactive and integrated approach to cybersecurity this year due to the forecasted growth of high-impact artificial intelligence (AI)-enabled threats. While this strategy has been peeking around the corner in the past few years, it will take the frontline in 2025.

WhoisXML API presents this and other cybersecurity predictions, covering both emerging cyber threats and the strategies required to address them, to help organizations prepare for future challenges.

Prediction #1 – Organizations Will Increasingly Struggle with Malinformation and Fake Online Personalities

Among Gartner's top cybersecurity predictions is that organizations will spend US$500 billion fighting against malinformation, which it defines as “algorithmically groomed and targeted facts, misinformation, and disinformation designed to undermine mental models and cause consumers to make decisions they otherwise wouldn’t.”

A significant share of cybersecurity and marketing budgets are expected to be allocated to this threat that manifests as social engineering, spearphishing, and other highly targeted attacks.

Malinformation can be exacerbated by the ease at which people can create seemingly credible personalities with an online presence, such as through social media and websites. In some cases, threat actors may not even need to fabricate fake personalities. They can just imitate well-known

and reputable individuals.

As the 2024 U.S. presidential elections approached, for example, our researchers detected more than 2,500 election-related domains and subdomains that could not be publicly attributed to the supposedly imitated personalities. These web properties contained the candidates' names and some could figure in impersonation and malinformation campaigns.

Prediction #2 – Organizations Will Focus on Cybersecurity Vendors that Can Address Multiple Use Cases

Another Gartner prediction that stood out as it has been a recurring theme since the 2024 RSA Conference was platformization. Specifically, Gartner says, "70% of organizations will combine data loss prevention (DLP) and insider risk management disciplines with identity and access management (IAM) context to identify suspicious behavior more effectively."

But, it looks like this unification is not limited to DLP and IAM. Palo Alto further predicts that "the cybersecurity landscape will undergo a transformative shift toward a unified data platform encompassing everything from code development to cloud environments and security operations centers (SOCs)."

In 2025 and the years to come, organizations will increasingly look for cybersecurity platforms that can help them mitigate several risks at once, ideally with the help of GenAI technology.

For security solutions providers, this trend means incorporating more security capabilities into a single platform, which consequently demands high-quality and comprehensive data sources to ensure the cohesive solution can do its jobs well. Palo Alto calls it the "data advantage," where organizations with massive datastores are likely to have an edge, specifically in AI-driven development.

Prediction #3 – AI Will Supersize Old Security Threats

While it's true that AI is a game changer, it's not always good news. In cybersecurity, we saw AI leading to more potent and evasive threats, such as the polymorphic malware Emotet. Malicious

actors will continue to leverage AI to power up old threats, such as phishing, insider threats, and ransomware.

For example, threat actors can use AI to craft hyper-personalized phishing messages and accelerate campaign deployment. Just as we thought we had a handle on phishing by looking out for grammatical errors, too-good-to-be-true offers, and other common signs of maliciousness, AI comes in curating highly targeted and believable phishing emails.

However, organizations can still effectively combat threats by using AI to their advantage. This tactic means leveraging AI-powered security solutions for threat detection and content anomaly detection.

AI can also ease the load off security teams through automation, enabling them to focus on more strategic tasks. Security teams can use it to automate specific security responses, such as isolating infected systems or blocking malicious traffic. Training on the right dataset will allow AI to analyze websites, emails, documents, and other content for signs of malicious activity, such as phishing attempts or malware distribution.

Prediction #4 – Zero-Day Attacks Will Increase

Because threat actors will increasingly leverage AI to detect vulnerabilities in target systems faster, zero-day attacks will increase. Think Log4Shell (CVE-2021-44228). This critical vulnerability in the Log4j library could likely have been discovered even faster with today's AI capabilities, potentially leading to widespread exploitation sooner.

Even worse, AI can also automate the development of exploits, allowing threat actors to launch attacks more quickly and efficiently.

Organizations will have to keep their eyes open for real-world exploits by integrating multiple threat intelligence sources. Proactive vulnerability management will also be crucial, entailing constant vulnerability scanning and patching.

Prediction #5 – Security Will Increasingly Shift toward a Predictive Model

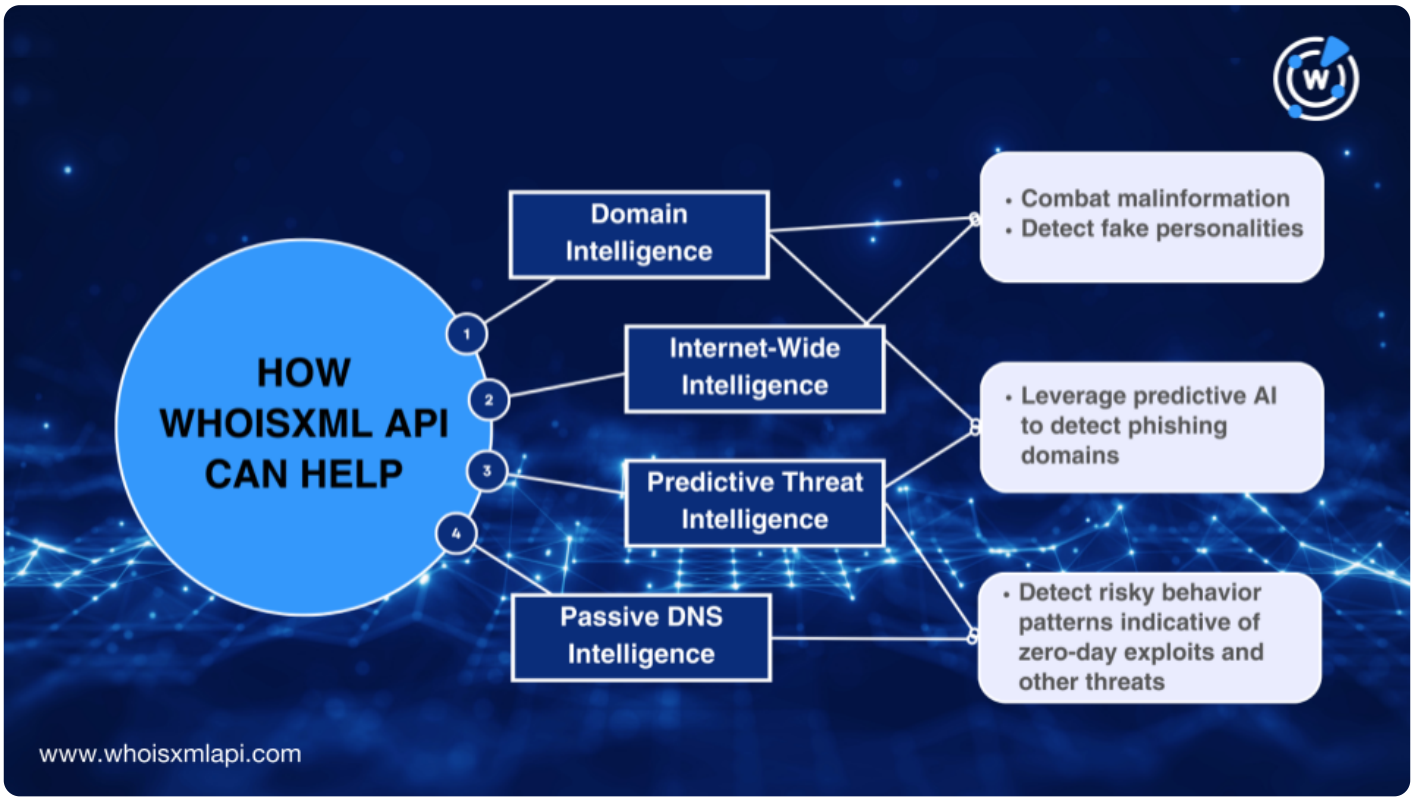
Traditional security is more reactive, focusing on incident detection and response. For example, a reactive approach to domain security involves blocking domains only after they have been identified as malicious, typically following their use in phishing campaigns or malware attacks. However, this reactive stance no longer suffices in today's threat environment.

In 2025 and the coming years, organizations will increasingly look for more proactive solutions that can analyze, detect, and predict risky behavior patterns. A predictive security model involves monitoring suspicious domain registrations by analyzing early indicators, such as domain naming patterns, WHOIS data, and DNS configurations. This allows organizations to anticipate and prevent potential threats before they escalate into significant incidents.

What does this trend mean for security solutions providers, though? It emphasizes the development of specialized predictive AI models trained on security-specific datasets, such as DNS logs, network traffic, user behaviors, and threat intelligence feeds. These models must be designed to recognize patterns and anomalies that traditional security systems and even general-purpose AI models trained on broader data may overlook.

WhoisXML API's Role in Cybersecurity in 2025 and Beyond

With over 15 years of providing a wide variety of cyber intelligence, WhoisXML API has witnessed security solution providers successfully meet their users' evolving security demands by integrating high-quality datasets with modern technology.



Timely domain intelligence sources such as Newly Registered Data Feeds and Typosquatting Data Feeds have been instrumental in identifying cybersquatting and other types of malicious domains. Using GenAI to combine domain intelligence with other Internet intelligence sources, such as website screenshots and categorization datasets, can play a vital role in enhancing the detection of malinformation vehicles.

AI-driven predictive threat intelligence sources can help organizations detect potential malicious domains before they are mobilized. First Watch Malicious Domains Data Feed, for instance, can identify newly registered domains likely to be used for phishing or command-and-control (C2), serving as a proactive defense against malware and phishing threats.

Meanwhile, incorporating passive DNS data into security solutions can significantly aid in detecting malicious activities and potential zero-day exploits. Sudden changes in name servers or IP addresses, for example, may indicate the repurposing of a domain for a phishing or malware campaign. Similarly, seemingly harmless domains with DNS records pointing to known malicious

infrastructure can also signal suspicious behavior patterns.

***Contact us* for more information about how our cyber intelligence sources can empower your proactive security strategy this 2025.**