qomodo Unveils Research on Shielding XIoT's Critical Infrastructure from Escalating Cyber Threats

LONDON, UNITED KINGDOM, April 1, 2024 /EINPresswire.com/ -- qomodo is pleased to announce the release of its research paper, "Stopping the Bad: Navigating the Expanding Attack Surface in a World of XIoT." The publication presents an in-depth exploration of the XIoT's integration into daily processes and critical infrastructure, driving unparalleled efficiency and innovation across numerous sectors. However, this interconnectivity also magnifies the increasing cyberattack surface, exposing essential services and physical safety to unprecedented risks.

Spearheaded by a seasoned team with roots in BAE Systems and NATO's cybersecurity teams, this research aims to demystify the complex ecosystem of XIoT. It highlights the need for sophisticated security measures to shield these technologies from the advancing strategies of global adversaries. qomodo sheds light on the real and present danger posed by nation-states and cybercriminal groups, which increasingly exploit XIoT vulnerabilities to launch sophisticated cyber-attacks, targeting everything from our power grids to healthcare systems. The potential fallout from these attacks is stark, risking financial ruin, operational paralysis, and even physical harm.

Toby Wilmington, CEO of qomodo, underscores the urgency: “The threat landscape is evolving at an alarming rate, with nation-states leveraging the XIoT as a battlefield for geopolitical dominance. This reality calls for a proactive stance to safeguard our interconnected world against potential disruptions, from hacking in transit autonomous vehicles or halting production of critical products to nationwide blackouts.”

“We believe there is a shift coming where devices currently in situ (in sensitive environments) are going to have to be ripped out because they no longer meet regulations for the environment they are in,” says Wilmington. “We also believe that new devices will need to have a tolerance built in and be future-proofed for the evolving security requirements that will be rolled out over the next 5+ years.”

Furthermore, the research paper not only outlines the vulnerabilities and threats facing XIoT but also sets out for robust defence strategies. It details qomodo's novel approach, utilising embedded detection and prevention capabilities with machine learning to deliver swift, context-sensitive countermeasures against cyber threats. Currently, there are 15bn IoT devices

connected to the internet, with that number set to hit 30bn by 2030 (Statistica 2024 - https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/)'.

As part of its mission to bolster global XIoT security, qomodo invites partners to join its 2024 pilot program, aimed at reducing the attack surface for companies navigating the complex XIoT landscape.

For more insight into qomodo's research and services, please visit https://www.qomodo.io or access the white paper at https://research.qomodo.io/stopping-the-bad.

About qomodo

Founded by a team of ex-BAE Systems and NATO cybersecurity experts, qomodo is pioneering advanced IoT observability and threat prevention systems. Its technology-agnostic software agents, part of a suite of sophisticated solutions, offer machine learning-powered detection and response to threats within embedded systems. qomodo's leadership team brings over three decades of collective cybersecurity experience to the forefront, having worked with top global enterprises to safeguard national defenses and critical infrastructures.

Toby Wilmington
qomodo
contact-us@qomodo.io
