ENTERPRISE SECURITY GROUP AT BROADCOM

Public/private partnership boosts cyber defense



By sharing information and experiences with government, industry plays a key role in making systems more secure and resilient

Sunjeet Randhawa and Vikram Thakur | Symantec by Broadcom

When the government and private sector work together, we can make all our systems more resilient. Sharing our expertise leads to more widespread adoption of security innovations, including secure software and less vulnerable code. And when the government incentivizes the private sector to use proven solutions, it reduces the vulnerabilities in our networks.

As an example of the kinds of conversations government and industry can have, organizations often look for the cheapest way to respond to competitive pressure by quickly implementing artificial intelligence solutions, but they might overlook new attack surfaces being introduced in the bargain.

By working together, we can explore options and find ways to harness the tremendous potential of AI without sacrificing security.

Boosting collective defense in a complex threat environment

Broadcom has a long history of collaborating with the government on security concerns, and we have good relationships with many law enforcement and intelligence agencies. We often have the granular visibility into what threat actors are doing while the government has the channels to amplify the message and encourage people to protect themselves against these threats. When we share technical information with our government partners, they use that information to secure their own networks and then amplify the message across other critical sectors.

In particular, we've been sharing our threat intelligence and indicators of compromise with the FBI and the Cybersecurity and Infrastructure Security Agency for many years. CISA uses that information to warn other government agencies, businesses and critical infrastructure providers about security concerns, while our threat intelligence helps the FBI with its investigations and its efforts to reduce the number of bad actors. We also work with CISA's Joint Cyber Defense Collaborative (JCDC), which seeks to unify defensive capabilities from government, industry and international organizations.

The overall objective is to strengthen our collective defense in an increasingly complex threat environment.

Previewing frontier AI models and protecting infrastructure

AI has accelerated the threats we're seeing and is particularly adept at uncovering vulnerabilities in software, operating systems and web browsers.



Broadcom is previewing some of the frontier models and using those insights to protect our infrastructure, secure our software, and help our customers understand potential vulnerabilities and what needs to be patched, remediated or mitigated.

In another key area of public/private collaboration, we also share our experiences with other companies and the government. Those experiences are helping to shape federal policy related to previewing and potentially regulating AI models.

In addition, Broadcom participates in JCDC's Gold Eagle initiative, which is a disclosure platform for vulnerabilities discovered through AI. It is designed to prioritize vulnerabilities and coordinate remediation across critical infrastructure. We were the first company to share our experiences and what we're doing to protect our infrastructure and our customers. Furthermore, we've been sharing our expertise with the Office of the National Cyber Director, which is developing a framework for AI security policy.

Broadcom will continue to share both our threat intelligence and our experiences with the government for the benefit of our customers, other companies, government agencies and the country as a whole. The odds of success are much greater when the public and private sectors join forces toward our common goal of secure, resilient infrastructure.

Sunjeet Randhawa *is director for government affairs and policy counsel at Broadcom, and* ***Vikram Thakur*** *is a technical director at Symantec, a division of Broadcom.*

> **We often have the granular visibility into what threat actors are doing while the government has the channels to amplify the message."**

