



ENTERPRISE SECURITY GROUP AT BROADCOM

Reinventing the security operations center

AI-driven detection, automation and unified visibility are combating alert fatigue and accelerating cyberthreat response

Paul Miller | Enterprise Security Group at Broadcom



In today's cybersecurity landscape, we're seeing increased velocity in terms of threats, vulnerabilities and attacks. With the advent of artificial intelligence, some adversaries are using malware embedded with a large language model that can make decisions on its own, and others are starting to toy with fully automated attacks. Those attacks are not easy to do, and so far, they're using tactics and procedures we know how to detect and stop. But as those attacks mature, they will overrun a security operations center (SOC) that's playing by the rules of even a year ago.

Furthermore, as we have seen, AI is incredibly good at sniffing out software vulnerabilities. During last year's Black Hat Europe, I was asked for my threat prediction for 2026. I referred to my main concern as an "AI-enabled zero-day apocalypse cannon." Just a few months later, several models began detecting and quickly exploiting software vulnerabilities.

It's just a matter of time before attackers figure out how to do that in a more open-source way so they're not relying

on commercial AI tools. Attacks based on someone else's infrastructure are easily detected and stopped, and an attacker can usually be identified in some fashion. But it's reasonable to believe we'll see an increase in AI-driven vulnerability exploitations once adversaries can inexpensively run those models on their own.

Predicting an attacker's next move

At Broadcom, we are always looking for ways to move SOC analysts further left on the attack timeline and reduce the amount of time they spend on both sides of an attack. AI is playing a key role in those efforts.

Within Broadcom's Enterprise Security Group, Carbon Black embraced automation over a decade ago, and Symantec's founding documents from 1982 talk about the plan to be a leader in AI. Symantec started keeping track of cyberattacks that same year, and Broadcom has used that huge corpus of data to train a variety of AI models.

We recently released a new product called Symantec CBX, an extended detection and response solution that combines the best capabilities of Symantec and Carbon Black into a unified, cloud-based platform. It can be very effective at turning an incident into a singularity instead of a several-day timeline. CBX includes Symantec's Incident Prediction, an AI model that can predict the next several moves an attacker will make, with a likelihood rating for each of those steps.

The tool gives analysts an effective way to stop attacks earlier than standard state-of-the-art detection can occur.

Easing the cognitive load on analysts

Another component of CBX, the Carbon Black Threat Tracer interface, helps analysts visualize an attack. It enables them to drill down into each incident and see metadata and actual data in some cases about the attack and targets. Switching between tabs to evaluate information creates a cognitive load for analysts. Reducing those effects is critical



Repetitive work slows down SOC analysts and makes them less responsive at a time when threats and attacks are growing exponentially.”

for speeding analysts' ability to handle the more automated and sophisticated attacks we expect to see in the coming years.

Analysts also waste precious resources dealing with false positives. That's another area where AI can have an impact. Because Broadcom looks in aggregate across a large group of organizations, we can see patterns of known false positives and use automation to preemptively dismiss them. As a result, we dramatically reduce the number of alerts that require a SOC analyst's attention.

Repetitive work slows down SOC analysts and makes them less

responsive at a time when threats and attacks are growing exponentially. With Broadcom's solutions and expertise, analysts can use automation to enhance their ability to secure an increasingly complex environment.

Paul Miller is the security strategist in Broadcom's Enterprise Security Group.



**ADVANCED PROTECTION,
AUTOMATED DETECTION AND RESPONSE,
MAXIMUM SECURITY VALUE
SYMANTEC ENDPOINT SECURITY**