Broadcom Introduces Industry's First Incident Prediction Capability to Stop Living-Off-The-Land Attacks

April 15, 2025

Leveraging advanced AI, Symantec Endpoint Security can predict cybercriminals' moves in the attack chain, quickly stop them and return organizations to a state of cyber resilience

PALO ALTO, Calif., April 15, 2025 (GLOBE NEWSWIRE) -- Broadcom Inc. (NASDAQ:AVGO) today announced Incident Prediction, an industry-first security capability that extends Adaptive Protection, a unique feature of Symantec Endpoint Security Complete (SES-C), by leveraging AI to identify and disrupt living-off-the land (LOTL) attacks and other cyberthreats.

Trained on a catalog of over 500,000 real-world attack chains built by the world-class Symantec Threat Hunter Team, Incident Prediction puts the advantage back in defenders' hands by: predicting attackers' behaviors, preventing their next move in the attack chain even when they're using legitimate software, and then quickly returning the enterprise to its normal state. With Incident Prediction, SES-C delivers exceptional cyber resilience against motivated adversaries.

"The inspiration for Incident Prediction came from how GenAI can 'predict' the next word when generating text," said Eric Chien, Fellow, Symantec Threat Hunter Team, Broadcom. "By leveraging our extensive attack chain repository and threat intelligence using advanced AI and ML, Incident Prediction can predict the next four or five possible moves attackers will make in a customer's environment, disrupt them, and then revert to normalcy right away. As a result, security analysts no longer need to triage the event to figure out mitigation strategies; Incident Prediction does that automatically for them."

With Incident Prediction, SOC analysts and other security professionals can:

- **Automate mitigation and disrupt attackers**: Automatically identify the next steps that a specific attacker will most likely take based on past attack patterns. It then applies mitigation policies to block those predicted actions, disrupting most attacker's progress before they can reach their end goal of encrypting data or exfiltrating information.
- **Reduce burden on SOC analysts:** Eliminate the need for SOC analysts to manually triage alerts, analyze attack sequences and determine mitigation strategies. It handles this automatically, freeing up analysts to focus on other security priorities.
- **Avoid business impact:** Incident Prediction provides specific granular attacker behaviors to block limiting impact to normal business processes. Common day, but crude mitigation measures, which disrupt business such as quarantining machines, shutting down the network, removing user access, or reimaging machines are largely unnecessary.
- **Reduce attack surface:** Enhancing Symantec Adaptive Protection, which identifies and recommends blocking low-prevalence applications and behaviors to proactively shrink the attack surface. It helps close the "doors" to attackers and their common attack techniques.

The use of legitimate software by cybercriminals, the approach used in LOTL attacks, is on the rise. According to "*Ransomware 2025: A Resilient and Persistent Threat*," a new report by the Symantec Threat Hunter Team, LOTL attacks are used by nearly all ransomware actors. Nation-state actors also use them to conduct surveillance or exfiltrate data. And large organizations are not the only victims – mid-market businesses increasingly are targeted. Instead of re-imaging the whole machine or changing everyone's credentials when an attack is discovered, security professionals can use Incident Prediction to have more granular control over their security by blocking only the attacker's most likely behaviors to reduce the risk of business disruption and enable a streamlined incident response – as attacks happen – all without additional cost.

"Broadcom is focused on providing enterprise-grade security for all organizations, whether they have a mature SOC or a small security team. Incident Prediction delivers on this commitment – organizations can enhance SOC capabilities regardless of sophistication," said Jason Rolleston, Vice President and General Manager, Enterprise Security Group, Broadcom. "Today, every organization needs to empower their security teams to become faster, stronger and more resilient against highly sophisticated APT groups. With Incident Prediction, they now have an automated system that can flag, act and help protect against cyberattacks – as they happen – faster and more cost-effectively."

See Us At RSAC™ 2025 Conference

Broadcom is a Gold Sponsor of RSAC™ 2025 Conference which will take place April 28 – May 1, 2025 at the Moscone Center in San Francisco. Broadcom will be demonstrating innovations from Symantec and Carbon Black at booth N-5345 in the North Expo. In addition, Broadcom executives will be speaking at the event. Arnaud Taddei, Global Security Strategist, Broadcom, and Roelof du Toit Distinguished Engineer, Broadcom, will present, "*ECH: Hello to Enhanced Privacy or Goodbye to Visibility?*" on Monday, April 28th from 10:50 AM to 11:40 AM PT. In addition, Eric Chien, Fellow, Symantec Threat Hunter Team, Broadcom, and Jason Rolleston, Vice President & General Manager, Enterprise Security Group, Broadcom, will present, "*Under Siege: How APTs and Nation-States Are Coming for Everyone*," on Tuesday, April 29th from 2:25 PM to 3:15 PM PT.

Pricing and Availability

Incident Prediction is available now as a new feature for Adaptive Protection, which is part of Symantec Endpoint Security Complete (SES-C), at no additional cost to current SES-C customers. SES-C is one of the most integrated endpoint security platforms on the planet and delivers cloud-based protection with AI-guided security management, all on a single agent/console architecture.

About Broadcom

Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops, and supplies a broad range of semiconductor, enterprise software and security solutions. Broadcom's category-leading product portfolio serves critical markets including cloud, data center, networking, broadband, wireless, storage, industrial, and enterprise software. Our solutions include service provider and enterprise networking and storage, mobile device and broadband connectivity, mainframe, cybersecurity, and private and hybrid cloud infrastructure. Broadcom is a Delaware corporation headquartered in Palo Alto, CA. For more information, go to www.broadcom.com.

Press Contact:
Dan Mellinger
Enterprise Security Group Communications
daniel.mellinger@broadcom.com
Telephone: +1 415 572 0216

Source: Broadcom Inc.