

ESET World 2025: In Pursuit of Zero False Positives

April 09, 2025

By: [Mike Jude](#), [Christopher Kissel](#), [Craig Robinson](#)

IDC'S QUICK TAKE

ESET's premier event, ESET World, as well as exploring the state of endpoint cybersecurity also provided a forum for discussing the impact of artificial intelligence (AI) on the detection and mitigation of cybersecurity threats. While ESET's aspirations for zero false positive threat detections using AI remain somewhat optimistic, the conference demonstrated that such an approach can yield much improved cybersecurity over time.

EVENT HIGHLIGHTS

From March 24 through March 27, ESET (www.eset.com) held its annual ESET World cybersecurity event in Las Vegas. ESET's mission statement, Progress Protected, served as a theme for the event, but the subtext of many of the presentations and discussion could have been: zero false positives and prevention-first approach. This reflects the fact that throughout many of the presentations from ESET's management and technical leadership, the problem of false positive threat detections and its impact on SOC personnel was a recurring theme and having the ability to focus on most critical alerts only is what ESET strives for.

In particular, Richard Marko, ESET's CEO, noted in the initial keynote that cyberattacks have evolved beyond simple extortion and anarchism to big business. He suggested that only by combining human oversight with AI-enabled automation can we reasonably achieve cyber-protection that delivers zero false positive where SOC personnel can concentrate on those threats that are truly impacting.

Later in the first day, Juraj Malcho, CTO for ESET, amplified that theme by noting that as threat actors increase their use of AI to refine their attacks, organizations need to adopt AI-enabled technologies to improve their response. Malcho also noted that a robust cyber-defense must address threats in a layered way that seeks to ameliorate the most impactful first. ESET believes that AI can assist in making these determinations.

Additional keynote presentations on the first day focused on the sophistication of tools available to spoof facial recognition technologies as well as the ways in which ESET is taking advantage of on-chip technologies to push cyber-detection to the endpoint.

Day 2 focused on the theme of implementing cybersecurity from an organizational as well as an architectural perspective. Henrique Bernard, strategic vendor manager from the

Dutch government, along with Bas Dekker, senior legal counsel Strategic Vendor Management for the Dutch government, joined Dave Maasland, CEO ESET Nederland, to discuss how organizations can successfully negotiate with large technology vendors. Bernard suggested that such negotiations must be based on constant communication and transparency of objectives.

Also on day 2, IDC's Craig Robinson, VP Security Services, and Chris Kissel, VP Security and Trust Products, discussed how threat intelligence can effectively amplify an organization's cybersecurity capabilities. They noted that managed detection and response (MDR) vendors bring not only a dedicated labor pool that can provide 24 x 7 coverage but can also leverage industry-leading capabilities that an organization might otherwise not be able to obtain.

In addition to the keynote speakers, ESET World ran technical tracks focused on such areas as consumer cybersecurity, bespoke solutions of the ESET Corporate Solutions division for large enterprises, ESET's own Threat Intelligence service (various data feeds and private APT reports), and technical aspects of cybersecurity with clear business outcomes.

IDC'S POINT OF VIEW

IDC believes that ESET World provides a valuable forum for information sharing as well as establishing networks of like-minded professionals to promote professionalism in cybersecurity. Although the event was heavily focused on ESET products and services, there was broad acknowledgement that ESET is one of many players attempting to improve the response to cyberthreats, moving from simple response to preemptive approaches. This will, in ESET's view, depend on the application of advanced analytical techniques including AI.

One aspect of the event that bears noting is the focus on reducing the load that false positive threat detections have on organizational security resources. Zero false positives tend to gum up SOC operations and take the focus off of legitimate threats: such threats increasing because of bad actors' adoption of new technologies such as AI. Using AI and MDR services, false positives can be greatly reduced; however, it may be optimistic to think that there will be no false positives even using the best analytic technology. Zero false positives, in IDC's opinion, remain an aspirational target rather than a totally realistic one.

Nevertheless, incremental improvements in threat detection can have a substantial impact on the cost of cybersecurity and can shift the battle taking place between bad actors and organizations in favor of the SOC. IDC views the pursuit of more capable cybersecurity tools as a worthwhile endeavor; one that can be measured in terms of ROI rather than TCO.

In addition, and this seems counterintuitive, the pursuit of zero false positives requires data refinement and access to more telemetry, not less. A flagship product for ESET is its antivirus (AV), and ESET has offered AV since 1989 and has a library of over 2 billion malware files. ESET also gathers telemetry from appliances that customers install and from managed detection and response. Those appliances give ESET visibility into how the adversary attacks businesses on their perimeter, but ESET threat intelligence aggregates this data in any of 13 global research and development centers and tests the data internally before presenting data through threat intelligence portals. The better the context, the more likely the potential to eliminate false positives.

ESET's statement that they have engineering in their veins has been an asset and a hinderance to their full potential. The asset is that they have a long legacy of solid cybersecurity-focused solutions. The hindrance is that engineers often do not make the best marketing decisions. Their move to launch ESET World 2025 in Las Vegas this year — from Bratislava, Slovakia, in 2024 — showcases their desire to elevate their presence in the North American market. Having a mix of cyber-focused practitioners from the United States, such as an engagement lead from the Cybersecurity Division of NIST, and two senior officials from the Dutch central government that offered up poignant advice and counsel to a receptive audience, is a key step forward to combining ESET's thought leadership with their engineering capabilities.

Subscriptions Covered:

[Cloud Native XDR and Artificial Intelligence Security Analytics](#), [Endpoint Security](#), [MDR and Managed Security Services](#)

Please contact the IDC Hotline at 800.343.4952, ext.7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC or Industry Insights service or for information on additional copies or Web rights. Visit us on the Web at www.idc.com. To view a list of IDC offices worldwide, visit www.idc.com/offices. Copyright 2025 IDC. Reproduction is forbidden unless authorized. All rights reserved.