HYAS Comox

ATTRIBUTION INTELLIGENCE: ILLUMINATING THE SHADOWS

CEOs understand that cyber attacks are a threat. CIOs know that network visibility is crucial in detecting them. But in a world of rapidly-evolving cybersecurity threats, logging network event data is not enough.

To truly protect itself against an attack, an organization needs intelligence. It must understand not just what is happening on its network, but what the data means.

To do this, it must know its attackers. Where do they come from? What tools, tactics and procedures do they use? Looking behind the network data to understand the narrative of an attack helps us to know who is coming at us, why, and how.

Until now, though, the clues have been scarce. Filling in the gaps between them have been more art than science. Sifting through a sea of low-quality open source information has left even the best threat intelligence analysts shooting at shadows.

Every cyber security professional today is facing down this problem, and at HYAS we have dedicated ourselves to helping them solve it. We offer our customers more than data and general awareness. We offer them the chance to close the circle and zero in on attackers. We offer them attribution intelligence.

In an age of sophisticated attacks, attribution intelligence is a difficult job. Twenty years ago, attackers were happy to break into a network and wreak havoc, setting off alarms indiscriminately along the way. Today, they fly deliberately under the radar, lurking unseen on networks for months. They not only cover their tracks but even impersonate others.

HYAS Comox

TAKING ATTRIBUTION INTELLIGENCE TO THE NEXT LEVEL

Comox is HYAS' flagship online attribution intelligence platform, built for cybersecurity professionals including investigators in law enforcement and intelligence agencies, and forensic cybersecurity analysts in large corporations.

1B+

Data points processed everyday

Exclusive databases

The platform's investigation tools enable customers to query an exclusive, deep database of compromise indicators gathered from multiple proprietary sources extending years into the past.

100M+

DNS queries analyzed daily

Digital fingerprints

One of Comox's strengths is its ability to provide information and intersections that other investigative tools cannot. Its database indexes public, hard-to-find, and exclusive to HYAS datasets which allow investigators to better fingerprint events, actors, and infrastructure.

GEO IP

"to the doorstep accuracy."

The range of data types

Analysts can query a broad range of data types ranging from phone numbers through email and IP addresses. Comox searches and cross-references a vast array of information to return useful data for investigators to save into online case files.

Real-time event detection

Comox also features the ability to create alerts using a sophisticated set of rules, providing analysts with a rich set of real-time event detection and mitigation capabilities.