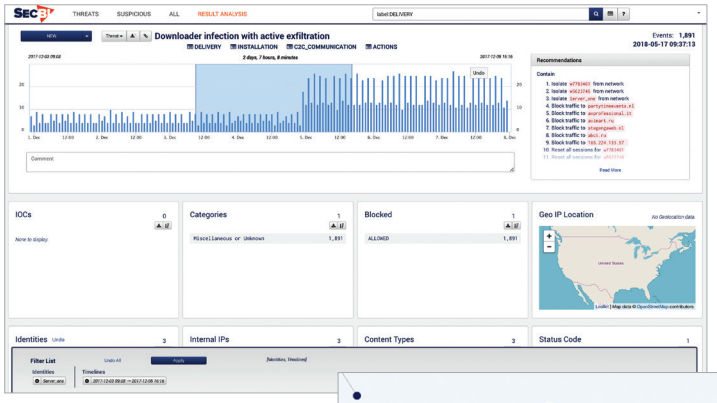
Cyberthreat analysis and intelligence

The very topic of cyber threat analysis conjures visions of security analysts pouring through terabytes of data to identify a specific threat, the virtual equivalent of picking though a pile of sand with tweezers to locate a speck of gold.

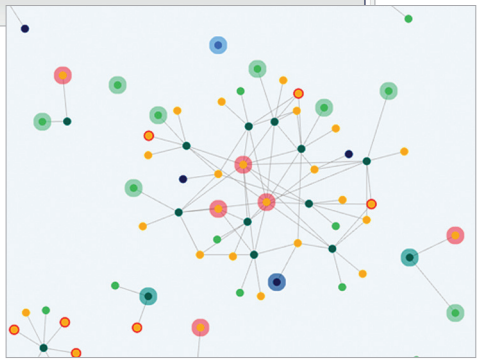
Cyberattacks are no longer a single event and may span many months, using a combination of exploits ranging from social engineering to network probes. The diverse and disparate data events generated during these events, combined with the elongated timelines over which they occur, further complicates the process of identifying and stopping active threats.

Fortunately, automation has improved the world of cyber threat analysis, and manual efforts have been supplemented with AI learning technologies. Applying AI to parse data, establish patterns, and identify anomalies eliminates (or dramatically reduces) the mundane tasks typically associated with threat hunting, allowing SOC analysts to do what they do best: connect the virtual "dots" to target evolving threats. A secondary benefit of this approach is that analysts can stay focused and avoid data saturation fatigue. For 2018 there are two Innovators that fit into the cyber threat analysis category: Uplevel Security and SecBi. Uplevel Security uses a rich graphic interface to visually link entities related to threats identified by its AI engine. The interface visually clusters data to make it easier to interpret and more actionable. SecBi also leverages AI technology to consume and analyze large volumes of network and log data at high speed. And it uses a hybrid Network Traffic Analysis (NTA) technology that leverages existing network traffic logs generated by proxy, firewall and other networked assets.

Both solutions offer great insights into evolving threats while delivering great efficiencies that help security analysts provide more coverage with fewer resources.

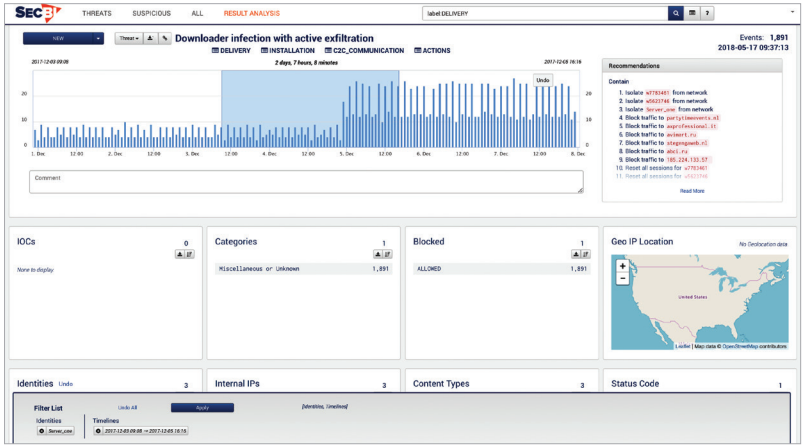


Page 10



Page 11

SecBi



When considering the many challenges to effective threat hunting and one item consistently stands out – the sheer volume of data to parse. Many have described it as the challenge of finding a needle in a stack of needles. Unfortunately, the more assets an organization has, the bigger the challenge. So how can analysts reduce the time and resources required to find threats in the enterprise?

The genesis of the Autonomous Investigation platform from SecBi came at the end of a large breach investigation that forced the team to wade through large volumes of data in a predominately manual fashion. SecBi developed Autonomous Investigation as an AI engine that makes detection and response quick, accurate, and simple by mimicking.

An artificial intelligence engine that mimics expert analysts operating at machine speed. The proprietary technology interrogates existing logs in a manner not done before. Since there is a big market shortage of talented individuals, the technology helps address resource gaps.

Surprisingly, the technology operates without the use of probes or network capture equipment. Executives refer to this capability as the "simple" in their equation. Autonomous Investigation focuses on network traffic because it is a MUST in any attack scenario. It uses a hybrid Network Traffic Analysis (NTA) that leverages existing network traffic logs generated by proxy, firewall and other networked assets. The platform creates a comprehensive view of each cyber incident by combining disparate alerts, events, and logs into one narrative. This process eliminates unnecessary noise, allowing the security analyst to focus on the critical information needed for cyber investigations.

DETAILS

Vendor SecBi, secbi.com

Flagship Product: Autonomous Investigation

Price: Annual subscription based on the daily volume of log data starting at $25,000 per year.

Innovation: An AI framework that ingests network traffic to parse though volumes of data and automatically flag suspicious behavior.

Greatest Strength: Simplicity of the solution translates into a rapid implementation that delivers high value for analyst teams.

secbi.com