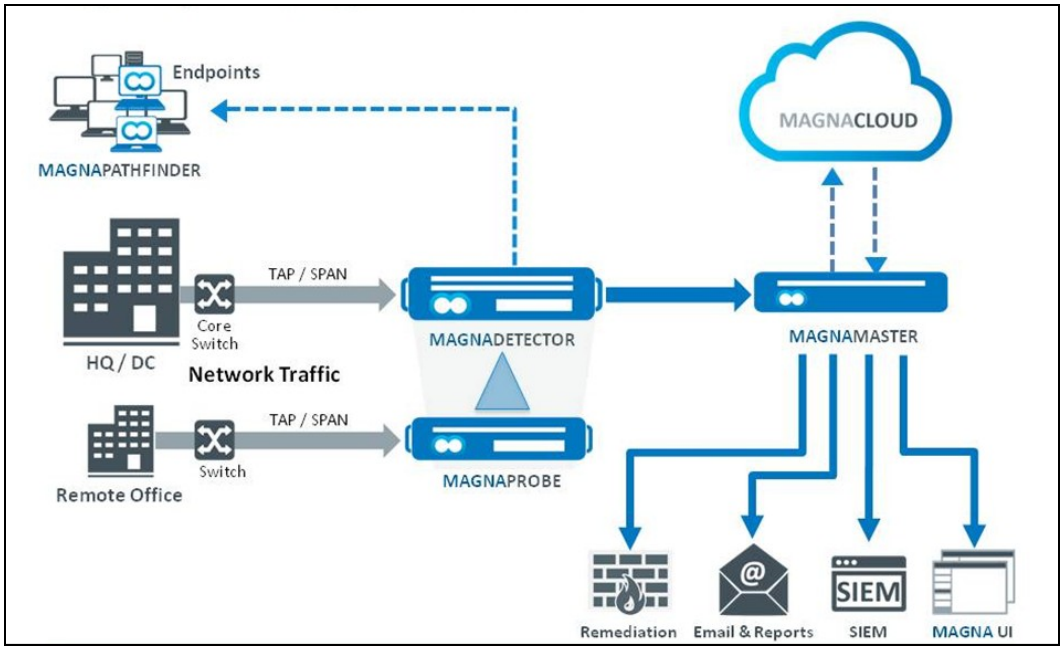
NETWORKWORLD
The Leader In Network Knowledge
www.networkworld.com May 20, 2016

LightCyber's attack detection platform distills alerts and generates actionable information

By Linda Musthaler, Principal Analyst with Essential Solutions Corp.

The Ponemon Institute published a report called *The Cost of Malware Containment* that reveals some interesting statistics—none of which will surprise the people in the trenches who work hard every day to protect their organizations' networks.

Ponemon surveyed 630 IT and IT security practitioners who have responsibility for detecting, evaluating and/or containing malware infections within their organization. According to the research, organizations receive an average of nearly 17,000 malware alerts a week. Of these, fewer than 20% (3,218) are considered reliable, meaning the malware poses a genuine threat and should be investigated. And even though more than 3,200 alerts are worthy of investigation, only 4% (705) actually do get investigated.



Organizations point to resource constraints and lack of in-house expertise as the reasons why so many important alerts are simply ignored.

Ponemon also reports that the time to respond to these alerts is a severe drain on an organization's financial resources and IT security personnel. The average cost of time wasted responding to inaccurate and erroneous intelligence can average $1.27 million annually. Of course, not responding to an alert can be even more costly. The 2013 Target breach is traced back to an alert that was ignored, and so far this single event has cost hundreds of millions of dollars.

There are plenty of cyber security tools on the market that generate alerts for anomalies, signatures or blacklisted domains. The lack of notification of suspicious events is not the problem; knowing where to focus and having accurate visibility to the artifacts that truly matter is the real challenge. Security analysts need intelligent tools that cut through the clutter and lay out the entire story behind a relevant alert so that they can respond quickly and efficiently.

This is the mission LightCyber has espoused since its founding. The company claims to deliver value through the accuracy and efficiency of its attack alerts, and the proof of this claim is in real customers' results. In a first-of-its-kind disclosure, LightCyber publishes quarterly attack detection metrics that validate what the company's customers experience. The results for Q1 of 2016 show that LightCyber customers received, on average, 1.1 meaningful alerts per thousand endpoints per day. Obviously this is a much more manageable volume than what the security

professionals self-reported in the Ponemon study, which was approximately 172 per day.

More important than reducing the volume of alerts is receiving alerts that are really relevant. LightCyber reports that 62% of all its customers' alerts were dispositioned in a way that the security analysts objectively identified them to be useful. That is, the alerts weren't ignored, whitelisted, or automatically archived without any investigation. Instead they were escalated, resolved or closed as normal.

LightCyber's solution is in the category of behavioral attack detection. The vendor assumes that prevention technologies are porous, and that attacks will successfully get passed perimeter defenses. LightCyber offers an integrated profiling solution that brings together, in a single detection domain, multiple aspects of profiling. The solution looks across the full span of network events, endpoint activities and state, and user credentials to find attacks across the attack lifecycle. The graphic above illustrates the architecture of the solution, called the LightCyber Magna Platform.

The solution starts with a network-based appliance called the MagnaDetector. This device sits off a network tap in a passive fashion, ingesting packets and doing deep packet inspection (DPI) on both application and administrative protocol use, domain access, and more. It also looks at credential use associated with those network traffic flows, not only source and destination IP but also deep knowledge through DPI and identity services. This approach yields knowledge of the traffic and what user and what host is associated with each flow.

When the solution sees anomalous network traffic, it interrogates the associated endpoint host using MagnaPathfinder agentless technology. The idea is to learn where the anomalous traffic is coming from, what low prevalence process might be running on that host, what user account or credentials were used to spawn the process on the host, and so on. This helps to see how an attack manifests on the network and how it was sourced on the host, as well as the credentials that were used with it.

LightCyber defines an endpoint as anything that has an IP address on the network and that has activity. All devices are profiled—PCs, servers, routers, printers, IP phones, IoT devices, etc. Since there is no agent used to do the endpoint profiling, the interrogation is done through standard administrative and monitoring protocols.

As shown in the architecture graphic, the MagnaProbe is a way to scale this solution in a large distributed environment. It works in conjunction with a MagnaDetector. The Detector is a hardware appliance with significant storage and processing capabilities for doing the enterprise-wide profiling. A Probe is purely a data ingestion and parsing system. It forwards the metadata to the Detector where the real processing takes place. A lightweight and low cost Probe can be deployed in a virtual system.

The Magna platform has four basic functions: behavioral profiling, attack detection, automated investigation, and integrated remediation.

In behavioral profiling, Magna establishes a baseline using machine learning in order to aggregate and group devices, user credentials and peer groups based on the broadest set of inputs. It starts from the network through DPI and is augmented with the state of endpoints, including the processes that are running, the files that are installed, and the user credentials that are spawning the processes on the endpoints and the credentials that are associated to the traffic on the network.

From that baseline, Magna does attack detection based on anomalies that aren't merely statistical anomalies, such as reconnaissance activities that aren't simply network scans being performed by a legitimate system administrator, but actual attack activity.

The third piece is automated investigation. Since Magna can see across the endpoints and the network, the solution can investigate what artifacts are involved in the anomalies that are detected. For example, in the case of attack reconnaissance, the system detects the traffic came from a particular executable. Magna then goes out to LightCyber's cloud-based expert system, MagnaCloud, to ask what is known about this anomalous process. Magna automates the investigative process that would otherwise have to be done manually across different systems, and the results are brought together in one pane of glass.

The final piece of the solution is integrated remediation, which is done through integration with third party solutions such as firewalls, SIEMs, and identity and access management systems. Through such integrations, it’s possible to, say, enforce quarantine of a host or force a passive reset of a credential.

The broad visibility provided by this system makes it look like it could generate accurate and efficient alerts. Security analysts are presented with all the network, user and endpoint context they need to investigate and take action on an alert. What's more, they aren't wasting time (and money) delving into alerts that don't matter.