REPORT REPRINT

Coverage Initiation: Reservoir Labs aims to accelerate network threat hunting

MAY 05 2020

By Eric Hanselman

Network security continues to become more complex, with greater context required to reliably weed out unhealthy activity at ever-higher data rates. Reservoir Labs is putting advanced analytics to work with a turbocharged packaging of the Zeek sensor to create greater levels of awareness and accelerate threat hunting.

Introduction

Networks offer a unique viewpoint from which to detect threats and priorities have been refocused on network security in recent times as the options for data collection from endpoints have become more complicated. Reservoir Labs' R-Scope network sensors address the need for greater performance in analytics and traffic capacity to raise the impact that network viewpoints provide. Better tools can make threat hunters more effective and keep security analysts on top of attackers and attack tools.

451 TAKE

Increases in network speed and traffic complexity continue to make it more challenging to sort through it all to find an elusive attack. Open source tools like Zeek provide a common platform that security analysts can depend on, but they can take a lot of care to be effective. R-Scope addresses the difficult task of making Zeek performant and expanding its capabilities to become a threat-hunting power tool. It's a tool that retains an important role in security operations, despite the intrusion of cloudy and metadata-fueled telemetry.

Context

Reservoir Labs was founded in 1990 and has headquarters in New York City. It started as a research and development lab and covers both government and commercial interests in high-performance computing and analytics. It indicates that about half of its roughly 40 employees have a doctoral degree in either software engineering or computer science. About a decade ago, Reservoir Labs began to turn some of its research projects into full-fledged products, while continuing its research operations. The company is privately held and has taken no external capital.

Reservoir Labs also offers professional services in support of its products and their integration into customer environments. These range from high-performance packet path adaptations to custom protocol analyzers for vertical specialties.

The company's research efforts extend into several different areas, including hypergraph analytics, advanced sensor and signal processing mathematics, and network flow optimization.

Technology

Network security use cases are varied. Isolation is the most direct, with firewalls of various sorts and network access controls being the most common methods to implement blocking for specific actions. Intrusion detection and prevention systems (IDS/IPS) are built to let traffic flow but detect and potentially dynamically block conversations that could be attacks. Next-gen firewalls (NGFW) blend a bit of both techniques. All these protections are meant to be put in place in fairly static roles. Their configurations are updated as environments change, but security admins use their event streams in a more reactive mode, investigating when alerts are triggered.

Threat hunting is a separate use case and involves a more hands-on operating mode. While reactive protections expect to see suspicious behaviors that they already understand, threat hunting looks to find suspicious activity that may fall below the radar of reactive techniques. It requires more complicated analysis and forensic capture of situations and data. While the output of reactive systems is often leveraged in threat hunting, more specialized tools can amplify the efforts of threat-hunting teams. There are three open source sensor projects targeted at network visibility for security: Snort, Suricata and Zeek (formerly named Bro). Snort and Suricata are traditional IDS systems, driven

primarily by detection signatures that identify traffic. Zeek uses a scripting language to accomplish the more complicated tasks needed for threat hunting. Reservoir Labs' R-Scope is built with Zeek and adds its high-performance data path as well as an on-box development environment for honing Zeek scripts.

The analytics that Reservoir Labs is putting to work drive more intelligent traffic identification and its implementation offers a triggered packet capture functionality (the Selective Packet Capture feature). It has developed a set of queue management techniques that both speed processing and ensure that all the data of interest in the capture environment is successfully captured and available for analysis. At multi-gigabit network rates, optimizations like this can ensure that richer datasets are available for threat hunting.

Products

Reservoir Labs' network security capabilities are packaged into R-Scope, which is available as both a physical and virtual implementation. Both offer a hardened software image with encrypted storage. The physical system is a 1U, rack-mountable device that offers 10Gbps throughput and four SFP+ interfaces. The virtual machine version of R-Scope can handle upwards of 2Gbps of throughput, depending on VM configuration. The company stated that it's planning on offering a container version of the product as well.

For management, the system is configured and controlled through Ansible playbooks, after initial CLI configuration. This can work well in larger deployments, where multiple sensors are deployed with segment-specific Zeek scripts running in each. The expectation is that customers will already be running an Ansible Tower environment, which is reasonably common in most enterprises.

Reservoir Labs offers a Nagios-based monitoring application that keeps track of the health of a collection of R-Scope systems. In the high-performance arena in which they're typically used, it's useful to keep an eye on device capacity to ensure that it's not reaching the limits of its capacity. As greater levels of analytics are applied to higher levels of traffic, tuning the distribution of traffic and processing loads can optimize the capabilities of a deployment.

R-Scope systems support event stream integration with a number of SIEMs, including Splunk and ELK, the latter in keeping with its threat-hunting focus. It can export file captures for sandboxing and investigation on other platforms such as FireEye.

Competition

The most direct competition for R-Scope is the set of vendors providing Zeek-derived products and the DIY network security teams willing to deploy and manage Zeek themselves. Corelight offers a pure-play Zeek product and Jask, now part of Sumo Logic, offers Zeek-based probes as part of its ASOC product. Corelight's web-based sensor configuration and multi-sensor management software might win some fans, but Reservoir Labs indicates that its customers prefer its greater analytical capabilities.

In the larger market of network visibility detection and response (NVDR), there are range of potential competitors with varying capabilities. Many fall into the class of protection products whose output can be used in threat hunting. Awake Security, Darktrace and Vectra AI (originally Vectra Networks) are examples of detection and response approaches. ExtraHop Networks comes out of a network visibility background and has pivoted to focus on security and straddles the detection and threat-hunting realms. Gigamon's acquisition of ICEBRG gives it threat-hunting capabilities as well.

Cisco, FireEye, Palo Alto Networks and VMware are all network security stalwarts that come from a traditional network security background. While they may compete for budget with Reservoir Labs, their products are going to different jobs in security operations.

In the longer term, as more traffic flows within cloudy environments, the most relevant telemetry will continue its nascent shift from raw packet analysis to flow records and event logs. That takes the network part of NVDR and turns it into the integration with cloud platform data streams that deliver more high-level information. Reservoir Labs can play there with its virtual product. More analysis will wind up being done on the metadata that's generated and some of that will be done in the likes of AWS Detective (from the Sqrrl acquisition) or Google Chronicle. We won't ever fully rise above the need to evaluate low-level bit streams, but analyst eyes are going to go more frequently to richer datasets.

SWOT Analysis

STRENGTHS

Powerful analytics are required to extract the subtle signals in high-speed network traffic and deliver reliable detection of advanced attack techniques. Performance and intelligence are both required.

WEAKNESSES

Reservoir Labs' device management approach is geared to larger customers with skill in automation. This could be challenging for smaller installations.

OPPORTUNITIES

The ability to extend a well-known platform like Zeek with additional analytics and customized capabilities will have appeal to threat hunters whose needs are more specialized.

THREATS

Network visibility through physical access is becoming more challenging as more traffic is dispersed across and within cloud systems. Cloud and SaaS providers are taking a larger position in owning that telemetry.