

Neuromorphic Cyber Systems

Solution Brief: Accelerating Cyber Security with Neuromorphic Processors

Lewis Rhodes Labs (LRL) is the first company to deploy neuromorphic processors into a production environment. The LRL product is a cyber-optimized threat detection device that accelerates industry standard intrusion detection systems by over 100x. The extreme speed and precision of these devices enable them to function as cyber microscopes providing analysts with unprecedented coverage and resolution at a fraction of the cost of alternative solutions.

The Problem

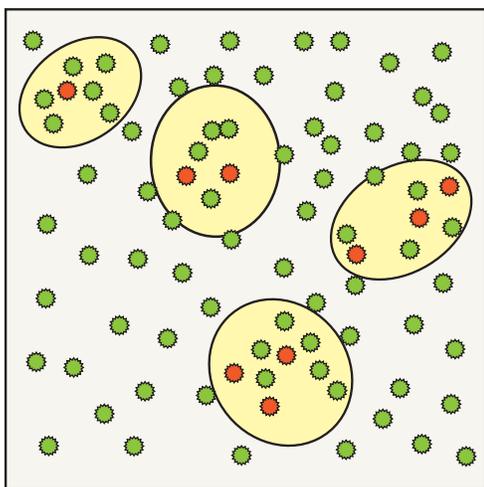
Cyber defense is a three-stage process. First, intrusion detection systems (IDS) monitor network and system activity for malicious events. IDSs use hardware and software sensors to execute security policies describing these events to generate alerts. Second, the alerts are consolidated into a security management system. Finally, highly trained security analysts evaluate the alerts using experience and a variety of analytic tools to identify and neutralize threats.

This model is increasingly compromised by the high cost of detection. Cost limits the number and fidelity of operational sensors that can be deployed, leading to a marked deterioration in the quality of alert data. In practice the vast majority of alerts consist of False Positive indicators placing a huge burden on the security analyst.

Consider detection like a microscope looking for malicious activity. Because of cost analysts must scan for potential threats at low resolution, Figure 1. Improving the cost of the sensors so they can be more widely deployed and deliver higher resolution is a top priority.

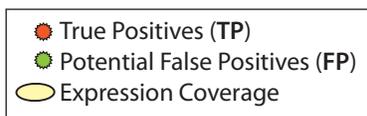
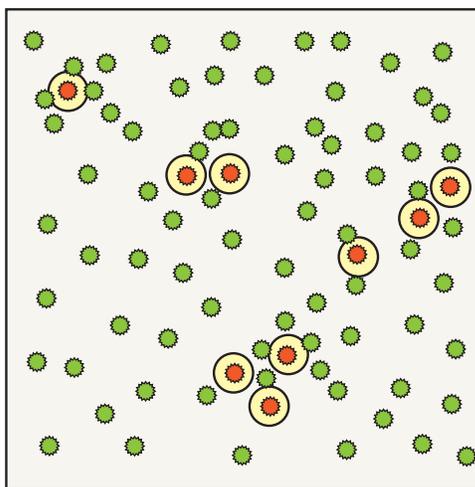
Low resolution
yields low fidelity alert data

Figure 1.



Neuromorphic processors
support high resolution analysis

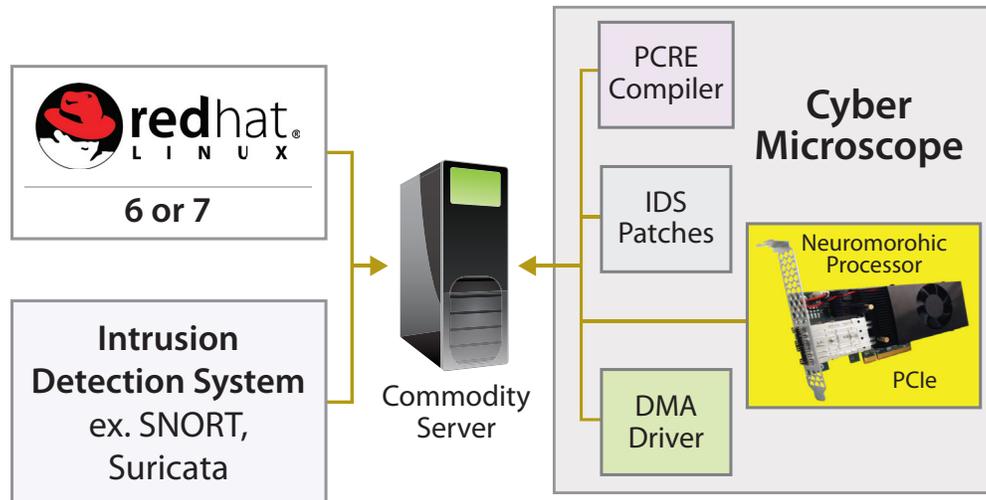
Figure 2.



The Solution

LRL is introducing a Cyber Microscope based upon a Neuromorphic processor optimized for computer security. The LRL Cyber Microscope is designed to execute standard security expressions while integrating transparently into existing security infrastructure. The Cyber Microscope improves sensor speed dramatically while lowering cost allowing for broader deployment and significantly higher resolution. In Figure 2, improved resolution means the False Positives are attenuated, improving the signal-to-noise ratio. The Cyber Microscope consists of a PCIe compatible interface card, driver and PCRE compiler integrated into a SNORT, Suricata or similar intrusion detection system as shown in Figure 3.

Figure 3.

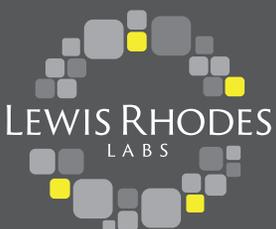


The Results

In collaboration with Sandia National Labs, the Cyber Microscope was benchmarked using production PCRE expressions and public PCAP files against a deployed state-of-the-art intrusion detection appliance. The Cyber Microscope pervasively analyzed 800+ complex PCRE expressions at a 2+Gb/s rate, delivering greater than a 100x performance gain. Future Cyber Microscopes will support 10,000x performance gains on a single ASIC, essentially making the cost of alert generation free. Critically, this scaling dramatically reduces False Positives while increasing True Positives, significantly improving accuracy and reducing the time and cost of threat detection.

Lewis Rhodes Labs

Lewis Rhodes Labs provides cyber-optimized systems with unparalleled precision at a disruptively low price. Based upon a unique understanding of how the sensory cortex of the brain processes streams of data, LRL has developed a Neuromorphic Architecture™ for implementation in PCIe based sensors. The result is state of the art anomaly detection with lower operational overhead, complexity, and cost.



Lewis Rhodes Labs
66 Commonwealth Ave., Suite 2
West Concord, MA 01742

cyberneuro@lewis-rhodes.com
978-795-4008