Sentry ND

Cyber-Defense based on Unsupervised Machine Learning

INTRODUCTION

Modern network traffic is approaching biological complexity with unprecedented data rates and flow varieties. The growth of application software with persistent cloud-to-edge interaction creates unusual traffic patterns, and the proliferation of new software outstrips the ability of traditional cybersecurity products to detect misuse across all of the software that might be installed within an organization. Traffic is further differentiated by where it is observed in a network, whether at endpoints, subnets, or inside or outside of firewalls. Most importantly, malicious actors continue to develop intrusion vectors that are hand-crafted to evade statically defined, network security measures.

PRODUCT OVERVIEW

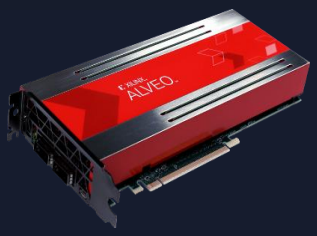
Sentry ND is a network monitoring and cyber-defense tool designed to autonomously learn normal traffic patterns wherever it is deployed and automatically detect and report anomalies. Combining Boon Logic's real-time, unsupervised machine learning technologies with the networking and compute acceleration of the Xilinx® Alveo™, the Sentry ND builds high-dimensional, detailed segmentations of all incoming ethernet traffic based on numerous packet and flow characteristics including geolocation, interpacket bursting patterns, packet flags and fields, and many more features. These segmentations allow instantaneous detection of abnormal incoming and outgoing traffic which may indicate malicious activity, network component failure, or misconfigured subnets. Detailed information about anomalous packets and flows is logged (via ELK stack) to the Alveo host machine in standard formats for consumption by existing customer SIEM tools or using our standard monitoring dashboard.

SOLUTION OVERVIEW

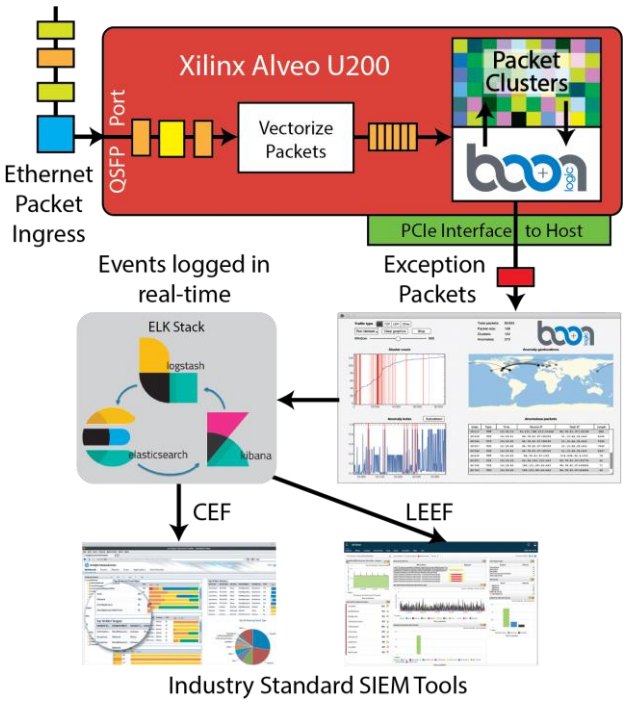
- Ethernet ingress via integrated Alveo QSFP ports
- Direct transfer of packets into FPGA fabric
- Each packet is vectorized into an *n*-space vector including length, protocol flags, geolocation, ports, TTL, select flow statistics, and more
- Vectorized packets are clustered using Boon Logic's real-time clustering technology
- Packets (or flows) representing atypical traffic are detected while still in the processing pipeline and exceptioned to the host for logging and consumption by standard SIEM packages.
- Network topology as an ML-clustered vector space can be viewed in our standard dashboard or in software such as Matlab, Mathematica, Python, etc.

SOLUTION BRIEF

XILINX ALVEO™



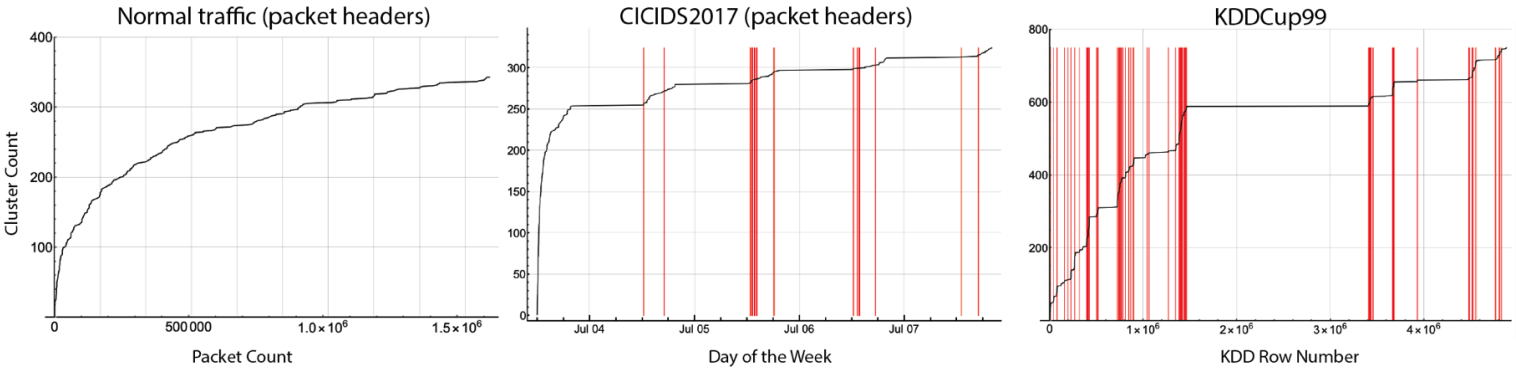
- Unparalleled, line rate, detection of both known and unknown threats
- Automatic configuration and autonomous learning of normal network activity wherever it is installed
- Non-invasive, passive network monitoring



Sentry ND

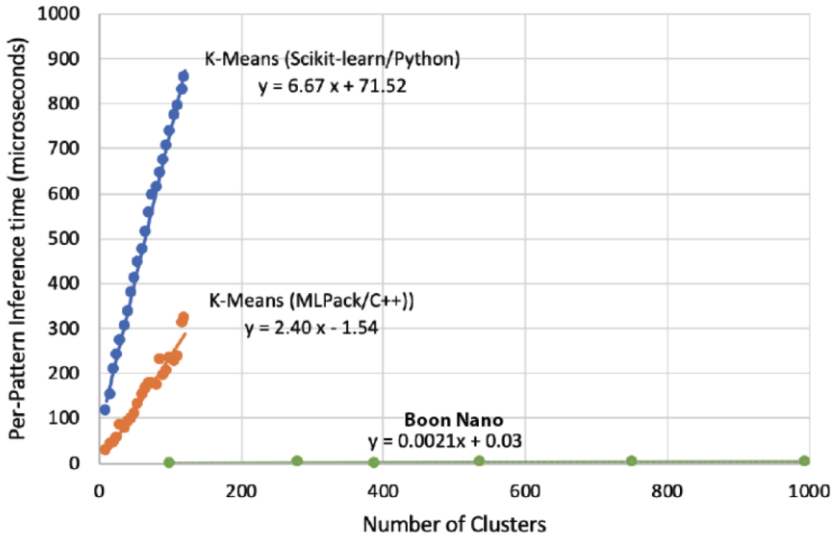
Cyber-Defense based on Unsupervised Machine Learning

ACCURACY



- CIC Attacks Detected**:** FTP-Patator, SSH-Patator, DoS slowloris, DoS Slowhttptest, DoS Hulk, DoS GoldenEye, Heartbleed Port 444, Web Attack – (Brute Force, XSS, Sql Injection), Infiltration (Dropbox, Cool disk), Botnet (ARES), Port Scan, DDoS LOIT
- KDDCup99 Attacks Detected: Unauthorized access from a remote machine, guessing passwords, unauthorized access to local superuser (root) privileges, various buffer overflow attacks, surveillance, probing and port scanning
- 99% detection with very few false positives

SPEED



- 300x faster than MLPack C++ K-means (K-Means on x86 vs. Boon Nano on Alveo U200)
- 850x faster than SciKit Python K-means (K-Means on x86 vs. Boon Nano on Alveo U200)
- Constant inference rate as input vector dimensionality grows
- Reduce by more than 99.9% the data sent to cloud-based SIEM and analytic tools

TAKE THE NEXT STEP

Learn more about Alveo accelerators
Contact www.boonlogic.com