CASE STUDY

ThreatEye Offers New Twist on Suricata with Accolade

SUMMARY

Emerging network detection company utilizes unique CPU offload techniques from Accolade Technology to enhance the efficacy of its security appliance

KEY CHALLENGES

- Provide 100% reliable packet recording and flow shunting capability for Suricata in an industry-standard server appliance

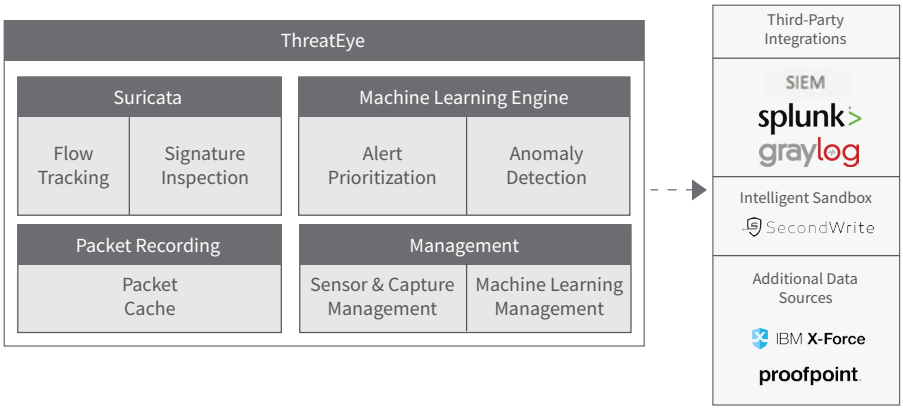
WHY ACCOLADE?

- Reliable technology partner with established track record in the marketplace for 1- 100G CPU offload adapters
- Unique flow shunting capability that works seamlessly with Suricata

ANIC FEATURES USED

- 100% packet capture
- Flow Classification
- Flow Shunting
- Nanosecond Precision Timestamping

Suricata is a well known, open-source network threat detection engine developed and maintained by the Open Information Security Foundation (OISF). While Suricata has been deployed extensively, security professionals recognize that its signature-based mechanism for intrusion detection can be augmented. ThreatEye—a network detection platform that enhances Suricata via machine-learning (ML) and hardware-based host CPU offload—is designed to improve the efficacy of network security. ThreatEye is developed and sold by Counterflow AI with essential host CPU offload capability provided by Accolade Technology.



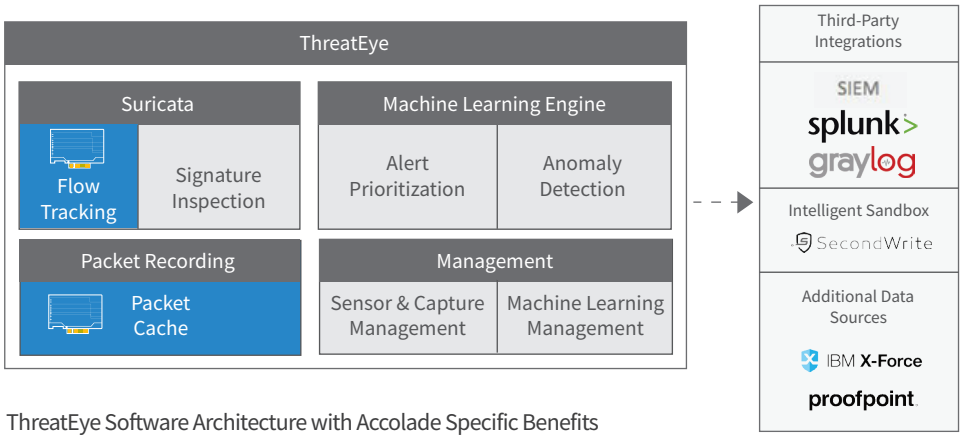
THE PRODUCT

ThreatEye is a network detection platform delivered as an appliance utilizing industry-standard hardware. The diagram above illustrates the high-level software architecture of a ThreatEye solution. There are four major components of the software: 1) A sophisticated machine learning engine is the most significant innovation in ThreatEye because it applies the latest data science techniques to manage the flood of network alerts which can overwhelm even the best security operations center (SOC) teams. 2) The latest release of open-source Suricata security software is packaged with the solution. 3) Packet cache is a packet recording mechanism that delivers 100% accurate, continuous packet caching. The data is stored in PCAP format so that an analyst can pivot directly from an alert to the full packet recording. 4) A web based GUI is provided for sensor management and updating of rules and ML models. An open REST API is also provided for easy integration with third-party tools that provide analytics support or input data such as the latest security signatures.

ThreatEye Offers New Twist on Suricata with Accolade

THREATEYE

ThreatEye is a network detection platform offered by Counterflow AI corporation. The platform is an industry-standard server with advanced security analytics capabilities. ThreatEye comes pre-bundled with an Accolade CPU offload adapter or SmartNIC for scalability from 10 to 40Gbps. The Accolade adapter offers several key benefits to the SOC team as depicted in the modified ThreatEye software diagram below. The blocks in blue (Flow Tracking and Packet Cache) are significantly augmented with the help of an Accolade adapter.



ThreatEye Software Architecture with Accolade Specific Benefits

FLOW TRACKING & FLOW SHUNTING

Each Accolade ANIC adapter can classify or track up to 32 million unique IP flows (based on 3 or 5-tuple) in hardware. With information about each flow in place, the ANIC adapter is then in position to take specific actions on an individual flow such as forward, drop or re-direct the flow. Control over which action to take is completely in the hands of the host application and can be programatically changed. We call this ability to dynamically cast away uninteresting flows: "Flow Shunting". There are many reasons for an application to shunt away specific flows, for example if they are encrypted; pose no security threat (e.g. NetFlix); or appear on a predetermined IP blacklist.

Flow Shunting is a generally useful capability, but it is particularly useful in conjunction with Suricata because Accolade has natively integrated hardware-based flow shunting with the software flow bypass feature that has been available since Suricata release 3.2 (December, 2016). Details about this integration can be found in the following technology brief: "Shunt Away Unwanted Suricata Traffic with Accolade Adapters".

PACKET RECORDING

Any packet loss for a security appliance is unacceptable because without a complete picture of all traffic flows you can never be sure that you didn't miss the crucial moment an attack began, spread or accelerated. Lossless or 100% packet capture is guaranteed with each ANIC adapter irrespective of packet size (i.e. 64 byte vs. jumbo frames). Furthermore, line rate packet capture is performed by the ANIC adapter no matter which packet processing functions (e.g. flow shunting) are enabled. Abundant onboard buffer memory is also available to temporarily absorb abnormally large bursts of traffic; all in an effort to ensure that the security appliance performs at maximum efficacy.

ID:191202

Accolade Technology

Headquarters:
124 Grove Street, Suite 315
Franklin, MA 02038

phone: 877 653 1261
email: inquire@accoladetechnology.com
www.accoladetechnology.com