cpacket NETWORKS VISIBILITY YOU CAN TRUST | corelight

Solution Brief

Proactive Cybersecurity using Network Detection and Response

Integrated Network Observability, Security Monitoring, and Intrusion Detection

Organizations are constantly under attack by cybercriminals who are clever, stealthy, and well-armed. They use many methods and vectors to attack to commit fraud, steal digital assets, and demand ransoms. Preventing attacks and their consequences begins with monitoring network traffic and observing behaviors. Prevention is ideal, however when events occur, causation, containment, response, and recovery must proceed quickly and effectively. Network-based visibility must provide information to security tools, analysts, and the security operations (SecOps) team. For maximum effectiveness of your NDR solution such as using Corelight's implementation of Zeek and Suricata, visibility from network packet data must:

- Be reliable and lossless so you have thorough visibility without blind spots
- Be an amalgamation of network data acquired from many vantage points
- Include detailed high-resolution visibility into behaviors, patterns, and trends

THE SOLUTION

The cPacket Intelligent Observability Platform and the KPIs and security delivery it provides is an ideal fit for Corelight's Open Network Detection and Response (NDR) stack. The field-proven joint solution is applicable for hybrid-cloud and multi-cloud environments. Security analysts can easily drilldown and replay events (including before and after) because alerts generated by Suricata are sent via an API call to cPacket cStor® packet capture appliances to tag the data enabling fast data queries and analysis of specific events. Evidence from Zeek, alerts from Suricata, and captured network packet data from cStor appliances empower analysts to quickly and thoroughly understand network activity linked to a specific alert so that an agile and accurate response can be initiated.

Corelight Network Security Monitoring and Intrusion Detection:

Corelight's platform performs security monitoring by analyzing primarily network data directly ingested from cPacket cVu® packet broker appliances. Zeek creates security evidence for diagnosing threat and attack types, threat hunting, finding rogue applications, and determining the scope of an attack. The evidence dramatically helps SecOps to reduce the time to respond, resolve, and recover. Zeek generates logs that contain rich security information that are used by many other vendor's Security Information and Event Management (SIEM) solutions. Complementing the evidence generated by Zeek is Corelight's tight integration with Suricata, primarily an Intrusion Detection Solution (IDS). Suricata uses binary pattern matching to raise alerts that are incorporated into the output generated by Zeek, adding helpful context to event alerts.

What our customers say:

"Our NetOps and SecOps teams use Zeek, Suricata, and the visibility and insights from the cPacket Intelligent Observability Platform for our security assurance strategy. We sleep well at night."

– Security Architect
Fortune 1000 Retail/Etail Company

The cPacket Intelligent Observability Platform includes:

- Network packet acquisition using TAPs and virtualized packet acquisition for cloud and other virtualized infrastructure
- Physical and virtualized network packet brokering (NPB)
- Physical and virtualized packet capture, storage, and analytics
- Unified management of the cPacket monitoring fabric in a single-pane-of-glass

cPacket Networks + Corelight
A Winning Combination for Effective NDR

Key Benefits

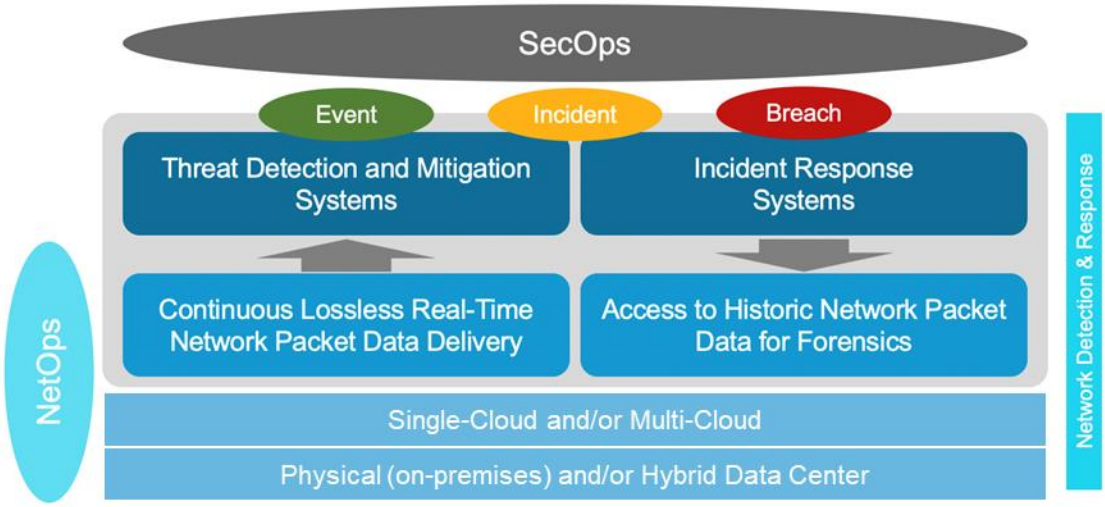
- **Strong Cybersecurity Posture**
  Tightly integrated network observability, security monitoring, intrusion detection with alerts, forensic analysis, and threat hunting.
- **Seamlessly Secure All IT Environments**
  Detect attacks, breaches, fraud, cybercrime, and malicious activity across physical, public cloud, multi-cloud, and hybrid environments.
- **Fast and Easy Deployment**
  Field-proven interoperability with standard interfaces and open APIs make deployment and bring-up easy and fast.

Real-Time Cybersecurity Alerts and Intelligence with Rich Forensic Evidence

Zeek and Suricata were developed in the open-source community, refined by Corelight, and are widely used by many organizations. Using these solutions fueled by dependable delivery of network packets, the SecOps team has the best available network evidence to understand and respond to security events. Corelight offers physical sensors that enable organizations to easily deploy the combined solution in minutes. Corelight offers virtualized instances of its sensors and appliances for use in public cloud and virtualized IT environments. Learn more about Zeek and Suricata.

Security Begins with High-Fidelity Network Visibility

Monitoring to acquire network packet data and observing behaviors, patterns, and trends enriches the visibility provided to security analysts and the tools they use is the foundation for effective NDR. Prevention, threat hunting, forensic analysis, and incident responses all rely on the information derived from network packet data. Gapless and lossless visibility is especially important for distributed hybrid environments because visibility and data gaps due to dropped packets during peak network activity are vulnerabilities that attackers will exploit. Learn more about the cVu Network Packet Broker+ and cStor Packet Capture physical and virtual appliances from cPacket Networks.



cPacket Networks de-risks IT I&O through network-aware service and security assurance across hybrid and multi-cloud environments. Our AIOps-ready Intelligent Observability Platform provides single-pane-of-glass analytics and provides the deep network visibility required for today's complex IT environments. The result: increased service agility, enhanced experience assurance, and faster transactional velocity. Learn more at www.cpacket.com