Use Case

Enhancing SOC Capabilities with Streaming Defense

The **only** Solution to Provide Full Attack Visibility combines with the ability to stop it at wire speed.

STREAMING DEFENSE

a new dimension in cybersecurity

Transforming SOC Environments: How Streaming Defense Empowers Security Operations Centers

In the ever-evolving landscape of cybersecurity threats, Security Operations Centers (SOCs) play a crucial role in safeguarding organizations' digital assets. However, with the increasing volume and complexity of cyber threats, SOC teams are facing mounting challenges in detecting and responding to incidents effectively.

This is where innovative solutions like Streaming Defense come into play, revolutionizing SOC environments and empowering security teams to stay ahead of emerging threats.

Streaming Defense combines cutting-edge technologies, including wire-speed processing, in-memory analytics, and AI-driven threat detection, to deliver unparalleled capabilities to SOC environments.

By processing network traffic in real-time and analyzing vast amounts of data with lightning speed, Streaming Defense enables SOC analysts to identify and respond to threats promptly and decisively.

The Problem

Current cybersecurity tooling relies on time consuming “Log Analytics" and ”Query" for a response to enable critical decision making. And require complex configuration and intrusive tooling.

- Lack of attack visibility leaves organizations with blind spots and vulnerabilities to compromise
- Growing Frustration of cybersecurity defense teams leading to errors and high staff burnout – As an industry we are already under resourced.
- Latency in identifying, containing and responding to attacks (mean time to respond (MTTR)).

The Solution is Streaming Defense

Streaming Defense operates at wire speed, swiftly processing code operations to assess connection integrity in circa ~ 100 milliseconds. This agility enables it to provide instant threat intelligence, empowering SOC operators to respond rapidly and effectively to potential security incidents. By harnessing the power of AI algorithms, Streaming Defense detects and exposes network threats in real-time, allowing SOC teams to take immediate action to mitigate risks and safeguard critical assets.

Moreover, Streaming Defense equips SOC analysts with the capability to terminate threats promptly, ensuring decisive action when needed most. This feature not only enhances response times but also minimizes the impact of cyberattacks, reducing downtime and potential financial losses for organizations.

In addition to its real-time threat detection capabilities, Streaming Defense offers comprehensive visibility into network activities. By providing detailed analytics and actionable insights, it empowers SOC analysts to gain deeper insights into potential security risks and vulnerabilities, enabling proactive defense against evolving cyber threats.

Wire Speed: In computer networking, wire speed or wirespeed refers to the hypothetical peak physical layer net bit rate (useful information rate) of a cable (consisting of fiber-optical wires or copper wires) combined with a certain digital communication device, interface, or port.

How Streaming Defense Helps SOC Analyst

- Provides a consolidated, simple, wire speed visualization of your entire estate.
- Enables analyst to perform visual inspections of entity interconnections with no need for query or drill down.
- Captures asset criticality and geospatial data into a single view.
- Advanced analytics combined with efficient hot storage provides rich context for forensics and threat hunting.
- A unified platform for threat detection, investigation, and response across entire IT and OT environment.
- Integrates with tools across EDR, SIEM, SOAR and ITSM.

Security Operations Center Use Cases

- Wire Speed Inspection: Indicators of Compromise (IOCs)
- + AI-driven detection is performed on each packet.
- Reduce "Mean Time to Detection": Improved defense effectiveness and reduced SOC workloads.
- Automated Ticketing: Integrated Threat Intelligence Platform enabling an ISAC, out-of-the-box, with advanced analytics.
- Enhanced Scalability: Scales to accommodate growing network traffic volumes without sacrificing security.
- Protection of Sensitive Data: Security controls are applied consistently and effectively across the network, reducing the risk of data interception and exfiltration.
- Audit EDR Effectiveness: Perimeter flows at wire speed detect weaknesses and anomalies in endpoint interconnections.
- Ensure Firewall Integrity: Wire speed detection of rule gaps and unreconcilable persistent connections.
- Simplified IT and OT monitoring: A single probe at network ingress inspects a limitless number of devices and types.

See It: For the first time, organisations have full and immediate network visibility – *See the attack*.

Capture It: Significantly improved and automated user experience (UX/AX) results in faster and more robust productivity – *Ticket the attack*.

Stop It: Kill switch allows immediate termination of confirmed attacks – *Stop it before it propagates*.

Streaming Defense is a game-changer for SOC environments, empowering security teams to detect, respond to, and mitigate cyber threats with unparalleled speed and efficiency. By leveraging advanced technologies and delivering real-time threat intelligence, Streaming Defense enables SOC teams to stay ahead of emerging threats and protect organizations' digital assets more effectively than ever before.

With Streaming Defense, SOC environments can achieve greater resilience and readiness in the face of evolving cybersecurity challenges.

Contact us today

https://www.StreamingDefense.com info@StrDef.com Partners@StrDef.com