**INTELLIGENCE
That Matters**

AVALON and SentryWire

When a data breach is detected, security analysts have limited time to investigate and actively respond. Important questions require immediate answers - What happened? When did it happen? What can be done to stop it? Quickly followed by: Who is responsible? How did it happen? How can it be prevented in the future?

Urgency escalates with each passing minute. Laser focus is needed to stop the threat.

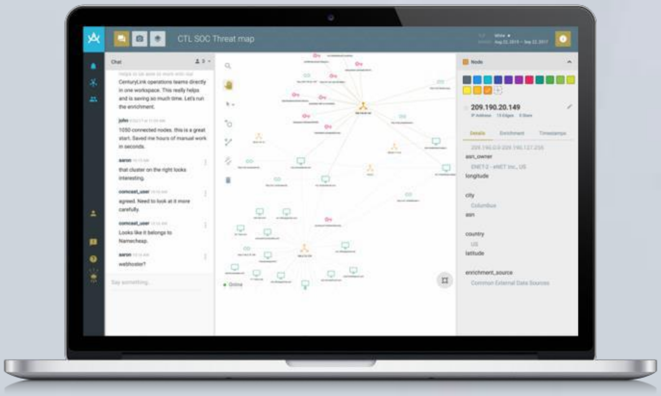
The question is…how?

Understanding the flow of data in, out, and within the network is crucial to identifying unauthorized, illicit, or criminal activity.

With data breaches now an endemic part of doing business, Security Operations Centers (SOCs) and Managed Security Services Providers (MSSPs) need a way to merge the detail found in full network packet capture with state of the art analytics to proactively focus SOC analysts on relevant data and allow real-time collaboration on threat detection, analysis, and action.

Avalon + SentryWire Joint Solution

By combining the forces of the King & Union's Avalon platform with the SentryWire full network packet capture platform, security analysts and incident responders now have a way to complete in-depth, focused analysis in a fraction of the time. Armed with SentryWire and Avalon, incident responders have visibility to specific communications between network endpoints presented with network relationship context for simultaneous team collaboration and information sharing in near real-time.



CTL SOC Threat map

Chat

CenturyLink operations teams directly in one workspace. This really helps and is saving so much time. Let's run the enrichment.

john
1050 connected nodes, this is a great start. Saved me hours of manual work in seconds.

aaron
that cluster on the right looks interesting.

comcast_user
agreed. Need to look at it more carefully.

comcast_user
Looks like it belongs to Namecheap.

aaron
webhoster?

Say something...

Node
209.190.20.149
asn_owner
longitude
city
Columbus
asn
country
US
latitude
enrichment_source
Common External Data Sources

How Avalon Works Together with SentryWire

Process

SentryWire captures the PCAP files and prepares them for ingestion into Avalon.

Normalize

Unstructured PCAP data complicates forensic analysis. SentryWire captures, filters, and structures this data for Avalon.

Categorize

Avalon uses the SentryWire data to reveal the network relationships of the traffic and associated endpoint relationships across the broader network for analysts to review and act. The Avalon artificial intelligence engine automatically adds what it knows from the SentryWire data to the visualization, revealing the network relationships of the traffic and associated endpoint relationships across the broader network so even the most seasoned analysts can understand threats more quickly. Investigative tasks are automated to return results in seconds with the click of a button.

Take Action

Understanding data is the key to properly defending networks. SentryWire and Avalon give you access to truly unique and exclusive data sources with unparalleled visibility of the network. Customers receive intelligence tailored to their needs and export output to their enterprise security architecture, ticketing system, or knowledge capture system. As a result, business leaders and security analysts can properly assess risk and allocate resources to the right activities.

When to deploy Avalon with SentryWire

- “Cut and paste” workflow, unwieldy spreadsheets, and awkward email chains used by many security analysts draw them further away from actual analysis. These problems are more than an inconvenience: they’re a weakness.
- When analysts devote more time updating spreadsheets and waiting for replies to emails, investigations slow to a crawl and remediation is delayed.

About SentryWire

SentryWire, a Division of Alliance Technology Group, is engineered and architected to be the most efficient packet capture solution on the planet. The system supports capture rates up to 100Gbps and retains network traffic for months and even years at 20% the cost of other systems. Learn more at www.sentrywire.com

About King & Union’s Avalon Platform:

King & Union’s Avalon platform enables cyber security operations and threat analyst and hunting teams to collaborate both within their teams and with other companies using automated correlation, enhancement, and graphical tools, dramatically improving their analysis and incident response in real time.

Avalon saves time, increases operational awareness, and reduces exposure and costs.
Learn more at www.kingandunion.com or contact us at info@kingandunion.com