# Coreflow: Enriching security events for improved attack analysis.

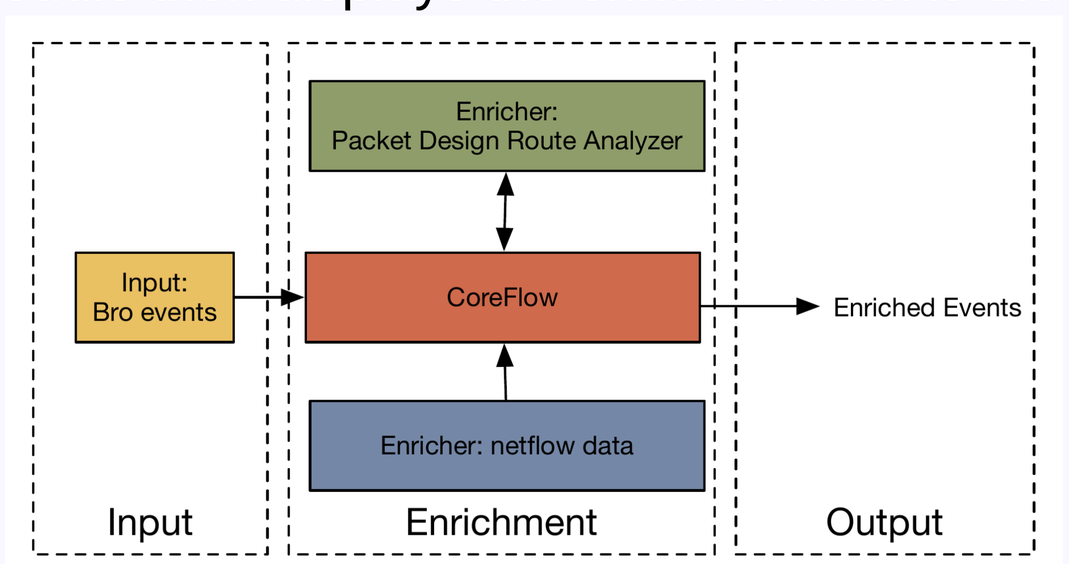
Ralph Koning, Nick Buraglio, Paola Grosso, Cees de Laat

## CoreFlow

CoreFlow is an enrichment tool for cyber security events developed by ESnet and the University of Amsterdam. Based on security events generated by an Intrusion Detection System (IDS), CoreFlow looks up contextual information from other information services (syslog, netflow, network management systems) and uses this information to augment the security event. The enriched event allows a more detailed attack classification, improved decision making and ultimately advanced responses.

## Processing

In the input phase, CoreFlow ingests events from an IDS (Bro). In the enrichment phase, the framework correlates the information with other data sources, detecting similarities in patterns and traffic behavior. The output module then displays the enriched data to the console, to a log file or into elastic search.
Events that are not correlated will pass throuth Coreflow unaltered so no information will be lost during this process.




**Components**
The input module reads bro events and translates them to the internal data format.
The netflow data enricher correlates the flow tuples from the bro event with netflow data.
The Packet design Enricher uses the source router and the possible ingress router to get a path estimation
Output sends the enriched events to elastic search.

## Application: Route estimation

When Bro reports an event, CoreFlow searches through the available netflow data of all the routers. This process gives information about which routers the malicious flow is reported on. With that information the path can be estimated using available topology information, and attacks can be blocked at the edge to unburden the network.

**Supported formats**
CoreFlow is work in progress and support for input formats is increasing and improving. The table below shows the formats CoreFlow currently supports for the different phases.

| Inputs | Enrichment | Output |
|---|---|---|
| • raw bro notice log<br>• raw bro notice log via stdin<br>• bro notice log via splunk | • raw bro connection log<br>• nfdump formated netflow data via NFS<br>• bro connection logs via splunk<br>• Palo Alto logs via splunk (under development)<br>• Netflow from splunk<br>• Syslog from splunk | • stdout (json)<br>• log file (json)<br>• elasticsearch |

## Conclusion

Automatically correlating IDS events with various data sources provides a more comprehensive view of the event that can be used for automated classification and defence actions.

## Additional information:

CoreFlow: Enriching bro security events using traffic monitoring data (**https://doi.org/10.1016/j.future.2017.04.017)**
Enriching network and security events for event detection **(https://tnc17.geant.org/core/presentation/30)**
SARNET, Secure Autonomous Response NETworks **(https://sarnet.uvalight.net)**

Ralph Koning <R.Koning@uva.nl>, Nick Buraglio <buraglio@es.net>, Paola Grosso <P.Grosso@uva.nl>, Cees de Laat <delaat@uva.nl>
http://sne.science.uva.nl | http://www.delaat.net/ | http://sarnet.uvalight.net

University of Amsterdam · SNE · NWO Netherlands Organisation for Scientific Research · ESnet Energy Sciences Network · Berkeley Lab