NOVETTA

Novetta Cyber Analytics

Infrastructure and Workflow Integration

Know your network. Arm your analysts.

Introduction

Novetta Cyber Analytics is an advanced network-traffic analytics solution that empowers analysts with comprehensive, near real-time cyber security visibility and awareness, filling a critical gap in today's enterprise cyber security toolset. With queries that take only seconds - even at Petabyte scale - the solution enables analysts to receive comprehensive answers to complex questions "at the speed of thought," then instantly access the ground truth network traffic needed for alert triage, incident response and hunting. The solution dramatically increases the efficiency and effectiveness of IT security staff and threat responders by providing them with the right information when they need it.

In modern day networks no security solution should be designed as a standalone capability, incapable of communicating, coordinating, and sharing with other solutions. Security systems must integrate to share and receive information that will help all systems detect and block threats that mean to harm and steal from the organization. This holds true across firewalls, routers, web proxies, Security Information and Event Management (SIEM) systems, Security Analytics solutions, other critical network infrastructure components, and even the security team itself. If a system, including its team members, is not exchanging information it is not fully protecting its network. As an advanced network-traffic analytics solution, Novetta Cyber Analytics must exchange information with, and provide access to, other systems as well as facilitate the exchange of information amongst security team members. To support these workflows, Novetta Cyber Analytics provides multiple capabilities that enable integration into existing network security and incident response activities. These capabilities include the following:

- Tagging of IP addresses and sessions for rapid investigations
- Ingestion of threat intelligence for enhanced contextual analysis
- Third-party console integration for rapid and confident alert review
- Network traffic export for fast and complete incident response and forensics

Tagging of IP Addresses and Sessions for Rapid Investigations

Throughout their daily exploratory and investigative activities, incident responders and security analysts review a lot of data. While reviewing network traffic data, it is very helpful to both have available and to be able to add organization-specific context to help the analyst generate actionable intelligence and to share knowledge with their co-workers — this is especially powerful when Tier 3 analysts can share their thoughts and suspicions with Tier 1 and 2 analysts. The Tagging feature in Novetta Cyber Analytics does just this — it adds analyst-defined labels as attributes of network traffic for the purpose of associating specific sessions and/or hosts with internal infrastructure, active investigations, or ongoing attacker campaigns. In Novetta Cyber Analytics, tags can be applied to network traffic attributes manually, in bulk, or automatically.

Manual Tagging

When analysts find interesting traffic within result sets they are able to manually apply existing tags and create new free-text tags. Using this feature, analysts can quickly add new context and categorization to the observed network traffic. An example of a manually added tag is the labeling of a newly-discovered external attacker's IP address as also being part of a separate attack campaign investigation. By marking up network data over time with contextual tags, analysts and operations teams can more easily and efficiently create and share actionable intelligence for their organization. This shared intelligence creates analysts that find never-before-seen — or even suspected — attacks while saving them an immeasurable amount of time by providing the single screen contextual information needed for investigations.

Bulk Tagging

When analysts have a large number of IP addresses or IP ranges that they'd like to tag, they can bulk upload tags and have them instantly applied to the observed network traffic. An example of bulk tagging is the labeling of known bad IP addresses that are known to target organizations in their industry. An analyst can upload the list of IP addresses and associate various tags with them. The analyst will then be able to view the tags in the network traffic and search for those specific tags from within analytic queries.

Automated Tagging

When analysts want tags to be applied automatically instead of as a one-time bulk upload, they can simply select criteria for adding tags to data and Novetta Cyber Analytics will apply tags during data ingestion and pre-processing. An example of automated tagging is the labeling of internal infrastructure based on rules defining how the organization has defined its subnets and VLANs (e.g. 'Web Servers'). No interaction is required by the analyst for automated tagging — the tags will be seamlessly applied and available for use in queries such as, "Show me all Sessions during XYZ time period related to 'Web Servers'," saving the analyst the tedious work of inputting individual IP addresses.

Ingestion of Threat Intelligence for Enhanced Contextual Analysis

Nearly all enterprise security teams maintain lists of, or even complete dossiers on, external attackers who are trying to breach their defenses. Threats found on these internal intelligence lists include hosts that have actively launched scanning or attack campaigns against the enterprise, command-and-control botnet servers, known spam servers, known compromised hosts, known Tor entry and exit nodes, and members of public blacklists. Maintaining this list is good for awareness, but ideally it should be automatically pushed to and used by network security systems for threat detection and prevention.

Novetta Cyber Analytics imports (via spreadsheets and tab-separated-value files) third-party threat information and customer-specific threat lists to provide the maximum amount of context to security analysts reviewing traffic. These threat lists are collections of IP addresses and CIDR blocks that can be ingested and used by the analytics engine for searching and results presentation.

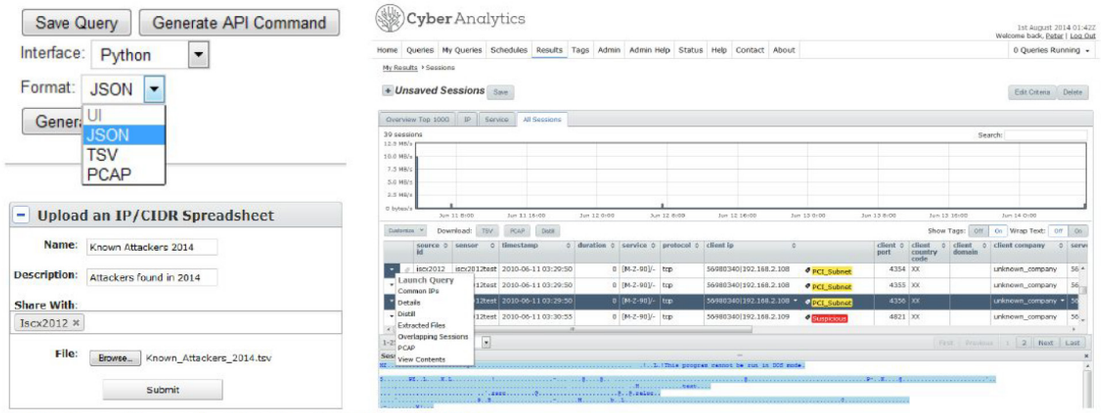
Once known attackers are imported, Novetta Cyber Analytics can use the lists in multiple ways:

- The system can continually scan network traffic for any activity from these sources. In this way the system serves as an early warning system that can alert analysts to suspicious traffic and enable them to immediately view the raw network traffic for the event
- The system can use these lists as an input to analytics in search of specific behavior or traffic patterns
- The system can automatically tag or label these IP addresses and sessions to tell analysts that they are part of a known threat list

Using these features as well as the built-in tagging capabilities, analysts have single pane access to the contextual information and ground truth network traffic needed for pinpointing and rapidly determining the full scope of a threat. For more advanced analysts — along with the solution's base capability of rapid search through intelligently selected metadata — they have everything they need to efficiently hunt for intruders starting even without an alert; perhaps with just a suspicion that something is wrong.

Third-Party Console Integration for Rapid and Confident Alert Review

Novetta Cyber Analytics integrates seamlessly with existing security solutions by providing a RESTful web API, a Python API, and a syslog message generation capability. The APIs give external systems direct and secure programmatic access to the analytics back-end engine with very minimal integration effort — an administrator simply adds a new menu item to launch an analytical search and analysts have direct access to Novetta Cyber Analytics from within their primary workstation interface. The syslog message generation capability enables the creation of syslog messages after the execution of an analytical search, which provides SIEM tools and other monitoring solutions with greater context around network events.



Integration options on Novetta Cyber Analytics web interface

A centralized hub with immediate PCAP access empowers workers with rapid, comprehensive answers

With strategically placed sensors providing a comprehensive network view, and with its core being a single columnar 'table' of observed network traffic, Novetta Cyber Analytics answers complex queries extremely rapidly and completely, allowing an analyst to, for example, quickly find all sessions and hosts related to a particular threat or alert — whether it be from a SIEM, firewall or security analytics console — immediately drill into the directly related PCAP, pivot and search through more remotely related PCAP, and then repeat. The rapidity of this iterative process provides an analyst with the ability to quickly come to a comprehensive and confident answer as to the criticality and scope of a particular alert.

The alert investigation process is very streamlined for any console that can access the Novetta Cyber Analytics APIs: Once the analyst receives a firewall or correlated SIEM alert, or perhaps even a signature-based DPI alert from their Security Analytics solution coming through to their SIEM console, they simply right-click on their menu to launch a Novetta Cyber Analytics query for information and traffic associated with the alert, and the query will be returned in seconds. The information and traffic provided to the analyst includes detailed information such as IP addresses, domain names, WHOIS details, blacklist membership, geography, and more. The analyst can then use the Novetta Cyber Analytics "View Contents" feature to instantly preview the first 10KB of the associated payload data in the packet capture. Should the analyst find malware or other interesting data they can instantly retrieve the full packet capture as seen on the wire. This enables them to perform traffic replay, session reconstruction, malware extraction, and other forensic activities — or pivot to other searches.

By combining the data associated with any alert with a comprehensive, rapidly searchable view of network traffic, analysts now have access to all the information they need to rapidly triage correlated, behavioral, and signature-based alerts.

Network Traffic Export for Fast and Complete Incident Response and Forensics

Security team investigations frequently require forensic analysis of traffic to retrace the steps of attackers, identify key activities, and reveal any other impacted internal hosts. Novetta Cyber Analytics is inserted into these security team workflows upstream of existing forensic capabilities to provide analysts and incident responders with rapid access to a broad, contextually enriched view of their network, empowering analysts to explore and investigate large volumes of network traffic at the speed of thought. With Novetta Cyber Analytics, an analyst can see a small clue, ask subtle questions with respect to their entire network, receive an almost immediate response, then drill down or pivot based on the information received.

Once an analyst has determined the full extent of a threat using Novetta Cyber Analytics, they can quickly export key packet capture to a traffic analysis or forensics tool for deeper analysis and traffic replay. In this fashion, the deep-dive forensics tool is leveraged for its key capability after a subset of network traffic has been identified. This enhanced workflow serves to accelerate the operational tempo of analysts. They can now quickly start at a console alert, attain situational awareness, identify threats, get visibility of raw packet capture, and perform deep dive analysis — all dramatically faster than without Novetta Cyber Analytics.

Conclusion

Organizations that make use of all these Novetta Cyber Analytics integration and workflow features can connect a powerful network traffic analytics and visibility platform to their existing security infrastructure and threat intelligence sources. This coordination empowers analysts and their entire teams to gain far greater visibility and awareness and substantially accelerate their operational tempo as they explore their networks, investigate specific alerts and incidents, and perform forensic activities. It also makes a security team's management chain far more confident when saying, "Yes, we're secure."