A New Perspective on Protecting Critical Networks from Attack:
Why the DoD Uses Advanced Network-traffic Analytics to Secure its Network

2014: A Year of Mega Breaches
A Ponemon Study published January 2015
# Table of Content

Introduction .....................................................................................................3  
Current Security Solutions are Limited ............................................................4  
Advanced Network-traffic Analytics Reduces Risks.........................................4  
Case Studies: How the Department of Defense Protects its Network from Threats ..........................................................................................................................5  
  Detecting Threats in Near Real Time  
  Discovering Ongoing Threats Other Systems Missed  
The Architecture of an Advanced Network-traffic Analytics Solution ..........6  
  Core Architectural Concepts........................................................................7  
    Centralized Metadata Store  
    Petabyte Scale  
    Pre-built Query Templates  
    Infrastructure Integration  
    Collaboration Tools  
Advanced Network-traffic Analytics in Action..............................................8  
  Low and slow port scanning  
  Network access from remote geographies  
  Protocol Abuse  
  Unknown services  
  Abnormal server connections  
  Data exfiltration  
Breaking New Security Ground.......................................................................9  
About Novetta .................................................................................................10  
About Novetta Cyber Analytics .....................................................................10
Introduction

According to the Ponemon study, “2014: A Year of Mega Breaches” published in January 2015:

- More than half of the most serious data breaches are not discovered until one year after the incident, and most of these are discovered accidentally.
- In nearly two-thirds of organizations, IT departments fail to stop the most serious breaches because attackers “evaded existing preventive security controls.”
- More than half of all senior management are now “extremely concerned” about data breaches compared to only 13 percent in 2013.
- More than half of all companies have increased security budgets by one-third, and most of their additional spending was on security incident and event management (SIEM), endpoint security and intrusion detection and prevention tools.

Security teams face increasing pressure from management to prevent breaches, discover attacks faster, and become more efficient. Most will not succeed because the security infrastructures they have in place do not work against most of the advanced persistent threats organizations face today.

Advanced attacks are conducted by malicious actors with the highest levels of skill, resources, and patience, while most organizations have deployed a collection of “automatic” tools designed to counter relatively unsophisticated attacks. Current solutions, including SIEMs, cannot provide an enterprise’s analysts, their most effective counter weapon, with all the information they need to be more efficient and effective. Security teams spend most of their time reacting to alerts, producing reports and piecing together information from many systems, instead of proactively investigating and hunting the stealthy attackers already on their network – the ones who do the most damage. Chief security officers and other senior management are disillusioned and tired of listening to software vendors tell them how their latest and greatest product or upgrade is finally going to solve the problem.

Given the current state of cyber security, what can enterprises do to protect themselves from data theft and other malicious activities? How can organizations increase their likelihood of detecting attackers and reducing dwell times? Many leading edge organizations and those with the most critical assets, such as the Department of Defense, understand these issues and are taking steps to compensate for them using advanced network-based analytics.

In this white paper, we will provide important information about how an enterprise can significantly reduce damages caused by sophisticated attackers, including:

- Description of the limitations of today’s security solutions and how advanced analytics can help improve enterprise security.
- Two case studies about how the Department of Defense benefits today from advanced analytics.
- High-level review of the technical architecture of an advanced network analytics solution and how it can be used to thwart attacks.
- Discussion of how enterprises and their security teams will benefit from a network-traffic analytics approach to enterprise security.
Current Security Solutions are Limited

Security analysts spend much of their time investigating alerts and producing reports. In a typical security organization, when suspicious activities need to be investigated, analysts gather what data they can from multiple systems and search for more data that isn’t being provided by existing tools. This piecemeal approach is used because most security solutions deployed today produce a lot of data, but the results they deliver are limited. A determined attacker will almost always find a way around perimeter defenses, and today’s analytic tools simply don’t provide the timely and complete data analysts need to counter attacks as they occur. Some specific limitations include:

- Perimeter defense tools use a signature-based approach that leaves them vulnerable to even the slightest malware modification, while a legitimate username and password obtained from phishing is something that must be let through.
- SIEM tools usually overwhelm analysts with alerts, and worse, the logs and events used to create alerts can be modified or subverted by a sophisticated attacker.
- NetFlow-based analytics tools provide good behavioral information, but only capture a very top-level summary of network traffic data, and can’t provide enough information for a complete investigation.
- Network forensics tools work well for forensics and other historical analysis, but analyze too much data far too slowly for immediate action on enterprise-scale networks.

Many senior network analysts, incident responders, and cyber hunters working today are experts in their field and have the skills necessary to detect and interrupt advanced persistent threats. When presented with complete information, these professionals can quickly evaluate it, respond, and avert malicious attacks, but they can only do this if they have the right information at the right time.

Advanced Network-traffic Analytics Reduces Risks

Since networks are built to transmit information, they will always be vulnerable to break-ins from anyone with enough skill and patience. To thwart these inevitable attacks, enterprises need additional measures to detect prevention failures: they need to focus on network-traffic analytics because attackers cannot hide while traveling across a network. To detect sophisticated attackers, enterprises need to provide security experts with:

- Complete, security-specific battleground views of network traffic in near real time.
- Automated notifications on activities advanced attackers use to infiltrate networks and exfiltrate data.
- Analytical tools to immediately query data and dive deeper into analysis.
- Collaborative tools that allow security teams to tag and share information for better team intelligence and action.

Advanced network traffic solutions that provide these capabilities are in place today within agencies at the Department of Defense and elsewhere. These agencies use advanced solutions to detect new threats in near real time and pivot from detection, to triage, to remediation in seconds or minutes.

The network traffic data needed to stop sophisticated attackers is readily available today to all enterprises. What isn’t available are the powerful, near real-time analytics needed to help analysts think better and respond faster. Truly advanced analytics solutions gather a complete, centralized picture of the network ground truth, then make the entire network picture available rapidly to analysts, so that human intelligence can counter human attackers in real time.
Case Studies

How the Department of Defense Protects its Network from Threats

In 2007 the Department of Defense (DoD) wanted to find a better way to detect malicious attacks as they happened, and identify previously undetected ongoing attacks.

DoD agencies deployed advanced network-traffic analytics technologies to solve these problems. The new technologies provided security analysts with near real-time access to all network activity. The results were dramatic:

- An estimated 30x improvement in the number of incidents each agency could investigate.
- Near real-time detection of new threats.
- Huge increases in detection of ongoing and even past breaches.

Below are more details on how two agencies within the DoD use network traffic analytics to protect their networks.

Detecting Threats in Near Real Time

One agency in the DoD, with more than 1,000 physical locations and millions of users, was the victim of multiple cyber attacks and could not determine how attacks were occurring. Once they learned of an attack, usually from external sources, it could take them months or years to uncover the details. Their globally dispersed network included hundreds of entry and exit points along multiple 40Gbps network channels.

The agency wanted a system that could provide its analysts with a complete view of all network traffic and the ability to immediately determine context from information collected from more than 100 sensors. The agency’s goal was to enable incident responders to detect, triage and remediate incidents in minutes to hours, not days or months or never.

With advanced network-traffic analytics in place, the agency:

- Has a battleground view of its network.
- Uncovers malicious behavior in near real time.
- Pivots rapidly from detection to remediation.
- Chooses which breaches to stop and which to simply observe.

Advanced, scalable network analytics is now the cornerstone tool used by this agency’s 300+ analysts.

Discovering Ongoing Threats Other Systems Missed

Another DoD agency knew it had been hit by multiple attacks in the past. To attempt to better understand these attackers, the agency had deployed packet capture (PCAP) sensors and network analytics tools, but the tools it deployed to analyze 13TB of sensor data could not execute queries and analysis fast enough. The agency was left with more questions than answers.

With a highly scalable, advanced network-traffic analytics solution in place, the agency now detects the critical who, what, when, where, why, and how of attacks that had been eluding it. With access to these key insights, security analysts were able to:

- Design data-driven processes to thwart new attacks.
- Shore up perimeter defenses to make penetration more difficult and detection easier.
- Dramatically reduce investigation and triage time.
- Understand the capabilities, limitations, and motivations of their adversaries.

Advanced, scalable network analytics is now the cornerstone tool used by this agency’s 75+ analysts.
Architecture of an Advanced Network-traffic Analytics Solution

Advanced network-traffic analytics solutions capture all PCAP data as it happens, preprocess data up front and store it in a local repository, then transfer analyst-friendly metadata to a centralized hub where it is enriched with additional data. When new metadata is received, analytics are automatically applied and results are immediately provided to analysts, who can then apply their own queries to dive as deep as needed to rapidly complete their analysis.

An explanation of how advanced network-traffic analytics solutions work is as follows:

Sensors, deployed at key strategic points within the network:
1. Collect network traffic out-of-band from a tap
2. Preprocess traffic to extract important attributes (e.g. protocol decoding, header instrumentation, and key fields useful in analytical searches)
3. Index and link PCAP data to extracted metadata and store it persistently to enable reachback
4. Send extracted metadata to the analytics hub

Analytics hub:
1. Ingests and preprocesses metadata
2. Identifies duplicate sessions from multiple sensors
3. Provides clean, consolidated views by converting network conversations between hosts into information intelligible by humans
4. Enriches metadata with external contextual data (e.g. geolocation data, subscription DNS, blacklists, whitelists, threat lists, domain owners, etc.) and analyst tags, which include details or suspicions about sessions and IP addresses
5. Sends enriched metadata to a large scale analytical engine
6. Answers queries to glean important actionable information
7. Presents information to analysts in a web interface or external tools such as SIEMs
8. Interacts with custom workflows or log aggregators using multiple application programming interfaces

* PCAP is stored at sensors and is instantly retrievable when needed for deeper inspection
Core Architectural Components

Advanced network-traffic analytics solutions are able to perform the operations discussed above by leveraging core architectural components, including a centralized metadata store, petabyte scale capacity, pre-built queries, integrated infrastructure and collaboration tools. Below are more details on each of these architectural components.

- **Centralized Metadata Store**
  A centralized metadata hub is what enables near real-time analysis. When metadata is centralized, analysts can quickly and easily combine different data elements and perform analytical queries without having to spend hours querying or manually gathering data from various locations throughout the enterprise.

- **Petabyte Scale**
  Since most enterprises have massive amounts of data running across their network, advanced analytic solutions must scale to handle extremely large data volumes while querying billions of records in seconds. Stored PCAP data volumes are usually about 100x larger than metadata stored in the centralized hub. The system must also be able to provide analysts with near-instant reachback access to PCAP data stored at the sensor as needed for further analysis.

- **Pre-built Query Templates**
  Advanced analytic solutions also need to provide pre-built analytical query templates created by experienced experts that can be scheduled to automatically run. These scheduled queries look for trends and patterns of behavior such as malware beaconing, protocol abuse, and internal scanning activity, and ensure the most up-to-date information is always available. If suspicious or malicious traffic is detected, the queries notify analysts via email or syslog, so analysts can quickly view the traffic’s metadata and underlying PCAP data. To investigate further, analysts can drill down, pivot, and run additional custom queries in seconds to gain better visibility.

- **Infrastructure Integration**
  Advanced network-traffic analytics also integrate with existing network security and incident response systems. Integration enables organizations to better leverage investments by combining information from many sources and providing analysts with superior intelligence. For example, they have the ability to:
  - Integrate with SIEM tools and firewalls to allow analysts to review raw PCAP data alongside the high-level log and summary reports produced by SIEM and firewall consoles.
  - Quickly export critical pieces of network traffic data to traffic analysis and forensics tools to help analysts deliver faster and more complete forensics.
  - Import third-party threat information and customer-specific blacklists and whitelists, and automatically tag IP addresses and domains that are part of known threat lists, to provide analysts with enhanced contextual analytics to better detect specific behaviors or traffic patterns.

- **Collaboration Tools**
  Advanced analytics tools have built-in collaboration tools that allow analysts to share contextual intelligence across security teams. In addition to sharing pre-built queries and results of scheduled queries, collaboration tools allow analysts to add tags to network traffic data and share attributes that help them associate specific sessions or hosts with internal infrastructure, active investigations, or ongoing attacker campaigns. By marking up network data with contextual tags over time, analysts and operations teams can more easily and efficiently detect patterns and other actionable intelligence.
Advanced Network-traffic Analytics in Action

Below is a description of some of the activities employed by advanced attackers today that can be detected and acted upon in near real time with advanced network-traffic analytics.

**Low and slow port scanning**
Attackers don’t usually know exactly how to gain access to a network, so they use port scanning techniques to perform reconnaissance and determine which access points are available. Many automated tools detect active brute-force port scanning, but can’t identify low and slow scanning activities used by more sophisticated attackers. Advanced attackers are patient: they spread out their activity over weeks or months and randomize it to avoid detection.

Advanced network-traffic analytics identify low and slow port scanning conducted over days, weeks or months. They collect large amounts of network traffic and run automated queries designed to look for scanning activities that occur over time. Once scanning or fingerprinting is detected, the software can automatically tag it as suspicious or malicious and notify analysts to investigate further. Detecting low and slow scanning as soon as possible helps enterprises close open channels quickly and pinpoint suspicious activities for further investigation.

**Network access from remote geographies**
Attackers use the authorized user names and passwords they obtain from phishing or other means to login to networks. However, most log in from a suspicious physical location (often China or Russia if a U.S. company is the target).

Advanced network-traffic analytics can use geolocation analysis to determine the locations of end users and their distance from the server. If a user logs in from a location where there are no remote offices, or no managers or administrators are traveling, the software can tag that activity as suspicious or directly notify an analyst. The software can detect remote activity at a country or city level, so activities can be monitored at the level of precision an enterprise requires.

**Protocol abuse**
Once they gain user-level access, attackers normally dump and crack password files using brute-force methods. They then use those passwords to move laterally across the network in search of administrator-level access on sensitive machines (e.g. database servers).

Traditional monitoring tools can easily identify lateral movements over standard communication channels. To avoid detection advanced attackers use non-standard channels. A common approach is to execute shell-level commands using applications such as Secure Shell or Telnet over ports that are non-standard for those types of applications. Advanced analytics automatically search for this type of protocol abuse in near real time to identify lateral movements that use a mismatch of services and ports. A customized analytic can also be tuned to whitelist or blacklist particular protocols or ports to better meet an enterprise’s specific security requirements.

**Unknown services**
Attackers often launch services unknown to an enterprise as they attempt to move laterally between backend servers and database servers. Since unknown services should never occur between servers, if one is detected it should be investigated immediately. This type of activity is most likely an attacker interacting between two machines to perform remote administration, conduct automated command and control with malware, or create a tunnel into a server using custom protocols or communication channels.

By performing automated searches for unrecognized services occurring between internal, or even internal and external, servers or devices, advanced network-traffic analytics provide analysts with detailed information about the devices, communications channels and standards involved.
Abnormal server connections
Once attackers are able to move laterally, they often attempt to communicate with database and application servers to access sensitive records and move them to staging servers for exfiltration. Each enterprise has normal, established communication channels between clients and servers. For example, it probably isn’t normal for a laptop or server in human resources to have a connection with a database server in the development organization, or for an internal, sensitive database server to have a connection with a public FTP server.

Advanced network-traffic analytics examine traffic summary information in near real time and identify suspicious connections between servers, or servers and clients. Analysts can then investigate these connections further and shut down malicious access or staging activities. Although a NetFlow analysis tool could issue an alert about direct communication between a database server and an FTP server, if a large amount of data was transferred, analysts could not use that tool to quickly review PCAP data or other related information.

Data exfiltration
Attackers who have successfully staged information on internal servers usually encrypt it into a large file or many small files, and then transfer it to an external location. These locations are usually anonymous, Internet sharing sites that can be easily accessed from another location at a later time.

Advanced network-traffic analytics detect this type of data transfer in near real time by automatically analyzing data traffic and identifying any data, or specified thresholds of data volumes, moving from an internal server to an external site. Once suspicious data transfers are identified, analysts can immediately investigate and stop further exfiltration.

The examples above represent only a few of the common types of behavior an advanced network-traffic analytics solution can identify. The real power of this type of solution is its ability to enable analysts to fine-tune the queries above to adapt to their attackers as attackers adapt to the enterprise’s defenses.

Breaking New Security Ground
Advanced network-traffic analytics solutions enable better enterprise security because they approach it in an entirely new way—by focusing on near real-time network-traffic data to dramatically improve visibility and awareness. These powerful analytics are designed to identify the behaviors of advanced attackers and give enterprises an edge by automatically detecting advanced threats and allowing lower level analysts to intelligently monitor activities. Rapid querying capabilities enable high level analysts and cyber hunters to fully investigate suspicious activities by diving deeper and exploring all possibilities in seconds, not hours or days. The software also allows intelligence to be shared across teams using built-in tagging and collaboration tools.

With advanced network-traffic analytics in place:

- CISOs and other senior security executives are far more confident in the reports their security teams provide.
- Security personnel are more efficient and effective because they spend more time finding and stopping malicious activities and less time responding to false positive alerts.
- Enterprises retain more talent, and more easily recruit new talent, because security team members actually enjoy their jobs: they no long spend the majority of their time doing the tedious work of wrangling data from multiple systems.

Enterprises that want to find a better way to detect new threats as they happen, identify undetected ongoing threats, and increase employee efficiency and job satisfaction, should add advanced network-traffic analytics to their security infrastructures. With these solutions in place, enterprises can achieve the same type of results DoD agencies are already realizing.
About Novetta
Novetta has been solving problems of national significance through advanced analytics for government and commercial enterprises worldwide for more than two decades. Novetta’s Cyber Analytics, Entity Analytics and Multi-INT Analytics capabilities enable customers to find clarity from the complexity of ‘big data’ at the scale and speed needed to drive enterprise and mission success. The company is headquartered in McLean, VA with more than 600 employees across the U.S.,

About Novetta Cyber Analytics
Novetta Cyber Analytics is an advanced network-traffic analytics solution that provides complete, truthful, near real-time network security visibility and awareness for security analysts, incident responders and network hunters. Now available for commercial enterprises, the solution dramatically increases the efficiency and effectiveness of an enterprise’s security team and its current infrastructure by enabling analysts to receive ground truth, PCAP-based answers to subtle queries almost instantly - with immediate reachback to the exact PCAP needed. Customers using Novetta Cyber Analytics can usually handle 5-10X times the number of triaged alerts and incidents (even with a Security Analytics solution already in place), and detect an immeasurable number of previously unknown intrusions. Learn more at www.novetta.com/cyber-analytics.

(Endnotes)