



WHITE PAPER

# Natural Network Threat Hunting Emerging as One Key to Modern Cybersecurity

# CONTENTS

## Table of Contents

---

Overview.....	03
Defensive Shortfalls .....	04
Hackers Moving Laterally Keep Ahead of Beleaguered Defenders.....	04
How Can We Shore Up Defense?.....	05
The Perfect Solution for a Modern Cybersecurity Defense .....	06
The Complete Defensive Package with Bricata .....	07
Bricata Versus Real World Threats .....	09
The Big Picture.....	10
About Bricata .....	11



## Overview

Its signature format, called Snort Rules, is a defacto From a very high-level overview, it seems like today's computer networks are more protected than at any other time in history. Almost every organization protects itself with multiple defenses, with larger organizations spending millions of dollars on the latest and greatest protection devices, programs and technology schemes.

There are anti-virus and anti-malware programs embedded on just about every endpoint, sandboxing tools examining incoming programs for malicious intent, intrusion detection or prevention systems watching over data packets, firewalls and next-generation firewalls segregating all parts of a network from the outside world, and Security Information and Event Managers (SIEMs) monitoring every little blip that hits their radar. Some organizations have even invested in full-scale Network Operations Centers (NOCs) or Security Operations Centers (SOCs) to try and get a handle on security, even though it's likely not their company's primary focus.

Still, cyber-attacks are getting through,  
and doing so in increasingly large numbers.

The latest Verizon Breach Investigations Report [hit another high](#) in 2017, tracking 42,068 cyber incidents that resulted in 1,935 breaches at monitored organizations.

The same was true of the annual Identity Theft Resource Center Year End Data Breach Review, [which saw an uptick](#) of 44.7 percent in the number of tracked breaches over the 2016 numbers.

Clearly, there are problems with the way IT defenses are managed and deployed today. Those problems range from not having enough cybersecurity professionals, to a deluge of highly sophisticated threats from motivated attackers. In addition, many of the advanced tools and tactics needed to defend networks like data analysis techniques, or building investigative processes into workflows, are mostly non-existent. Those processes are the foundation of threat hunting, and are sorely needed in many organizations, yet seemingly unobtainable.



## Defensive Shortfalls

One of the biggest problems is not one of technology, but one of training. This decidedly human problem is at the core of many, but not all, cybersecurity woes. There simply aren't enough trained IT professionals to go around. It really doesn't matter how many tools are employed, or how good they are, if there aren't trained staff to use them. What good are 1,000 hammers if you only have two or three people to swing them?

The scope of the manpower problem is huge. According to CyberSeek, a program of the National Institute of Standards and Technology (NIST) designed to combat the cyber talent gap, in the U.S. alone there are [112,000 unfilled openings](#) for information security analysts, plus another 200,000 additional openings seeking cybersecurity-related skills. And the problem is growing. Estimates put the shortfall at anywhere between 1.8 million to 3.5 million open cybersecurity positions in the next five years.

Even governments are desperate to employ more IT professionals. According to a [recent report](#) by The Pew Charitable Trusts, both federal and state governments are turning to retired military personnel, students and other non-traditional workers to fill cybersecurity seats, then spending a lot of money on training them how to respond to threats.

Couple that with the fact that networking isn't getting any simpler. Every time a new application, technology, client, server, cloud, device or almost anything else is added to a network, the number of potential vulnerabilities that an adversary could use to successfully attack it grows. And most of the time, each additional item added brings with it multiple vulnerabilities, so the attack footprint grows much faster than the network itself. Reactive incident response often exacerbates the problems, only addressing serious issues after the damage has been done. Organizations must use proactive techniques like threat hunting to uncover hidden threats before they do serious and ongoing damage.

One of the biggest problems is not one of technology, but one of training. There simply aren't enough trained IT professionals to go around.

## Hackers Moving Laterally Keep Ahead of Beleaguered Defenders

One only needs to look as far back as March 2018 to see the dangers of lateral movement, where a new strain

of ransomware [brought the entire city of Atlanta](#) to its knees. The initial infection was eventually detected and cleaned, but not before it was able to jump to many other clients in Atlanta's municipal network. Entire city divisions, like its district courts, were knocked offline, and unable to process warrants or try cases.

The same thing happened in Europe last year, where a variant of the Petrwrap / Petya ransomware brought [business to a halt](#) at banks, airports, government offices, service providers and more. There too, each of the initial infections were eventually caught, but not before the malware secretly spread using lateral movement to other systems on the same network, which was undetectable to most security programs.

In the United States, critical infrastructure in the form of power plants were recently breached by suspected Russian hacker groups. Instead of using ransomware to try and exploit money, the power plant attackers "conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems" according to a [report](#) from the United States Computer Emergency Readiness Team (US-CERT).

# DEFENSES

In response to the attacks against power plants and other utilities, US-CERT issued [Alert TA18-074A](#), entitled “Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.” The report details how the attackers gained access to internal energy sector networks, including indicators of compromise and the vulnerabilities that were exploited.

IT teams at power plants could shore up their defenses based on the US-CERT report, which would protect their networks from future attacks using the same vectors. However, most security programs don’t have the ability to look back in time, so those same plants may never know if they were breached before the report was released.

And beyond the obvious security problems, or any ransom demanded by an attacker, is the fact that every breach costs organizations a lot of money. One recent study by the Ponemon Institute puts the average cost of a security breach in 2017 [at well over](#) a million dollars for many large enterprises, and a hundred thousand or more for small and medium sized businesses. That estimate does not include all the many intangible costs such as damage to brand reputation and loss of confidence, or the long-term impact on customers from the theft of personally identifiable information, or the risk of identity theft, financial fraud and other secondary crimes.

## How Can We Shore Up Defenses?

Clearly, the myriad examples show a set of common flaws in cybersecurity defenses today. At the highest level, there are too many defensive tools reporting into too few people. The tools are not normally integrated, requiring the few IT people that an organization can deploy undertake multiple training sessions to simply learn their complex interfaces.

The process that most cybersecurity teams use to handle security alerts is inadequate against advanced threats capable of lateral movement.

At a deeper level, the process that most cybersecurity teams use to handle security alerts is inadequate against advanced threats capable of lateral movement. Cleaning one infected endpoint is no longer enough, because the threat actor has likely already moved laterally within the network, elevated their privileges and secured a foothold in many other systems. Most cybersecurity programs are blind to this type of lateral movement, and weren’t designed to perform threat hunting processes needed to uncover the most advanced attacks.

Finally, even if threat hunting or other techniques could be employed to expose advanced threats, most organizations have no ability to look back at historic traffic patterns. Stopping one threat and learning its indicators of compromise can help protect a network from future incursions, but does little good if the network was already compromised by other threat actors before the vulnerability was closed.

## The Perfect Solution for a Modern Cybersecurity Defense

Talking about a perfect security toolset is difficult because the idealistic concept of perfect is the enemy of the more realistic good. Not every cybersecurity solution will be optimal for every environment. However, looked at through traditional IT manpower constraints, the amount of data that needs to be processed, the level of training that cybersecurity personnel generally require, and the sophistication of today's threats, we can form a picture of what a very good defensive tool would encompass for most environments.


Without a doubt, networks can't abandon their baseline protections. Firewalls, endpoint protection software and even traditional anti-virus tools can all work to eliminate known or less advanced threats, sometimes automatically, so there is no reason not to employ them. Slightly more advanced defenses can center around NDR systems, which can make an IT worker's daily cybersecurity tasks a lot more effective.

It should also be a very easy-to-use platform, enabling both junior and senior analysts to work from the same


toolset. Clearly it needs to be able to detect lateral movement within a network, and not be stuck simply looking outward when today's modern threats are so adept at finding ways to move laterally inside a secure perimeter. The tool should collect historic traffic data so that administrators can be sure that no similar threats were able to sneak inside prior to new threat mitigation rules being written and put in place.

Into that picture, we must then inject the concept of threat hunting, enabling network data analysis techniques, and building investigative processes into everyday workflows. For most organizations, the concept of threat hunting is purely aspirational, something they know would be ideal, but also seemingly impossible to obtain without expensive, hard-to-find cybersecurity professionals and advanced tools for them to employ.

To that end, the perfect tool would help to bring threat hunting to every IT worker with minimal training. The interface needs to be simplified so that network data analysis can begin with any frontline cybersecurity worker regardless of their skill level. Ideally, it should work right from the same toolset that they use every day, such as their NDR console.



Creating the perfect tool is a pretty tall order but is the exact reason behind the creation of the Bricata platform.





## The Complete Defensive Package with Bricata

Deployed as a physical, virtual or cloud appliance, Bricata offers the leading Network Detection and Response (NDR) capability. By fusing real-time visibility, advanced detection, analysis, forensics, incident response and threat hunting into a single platform, Bricata provides organizations with end-to-end visibility and full context for direct answers and powerful insight to take immediate action.

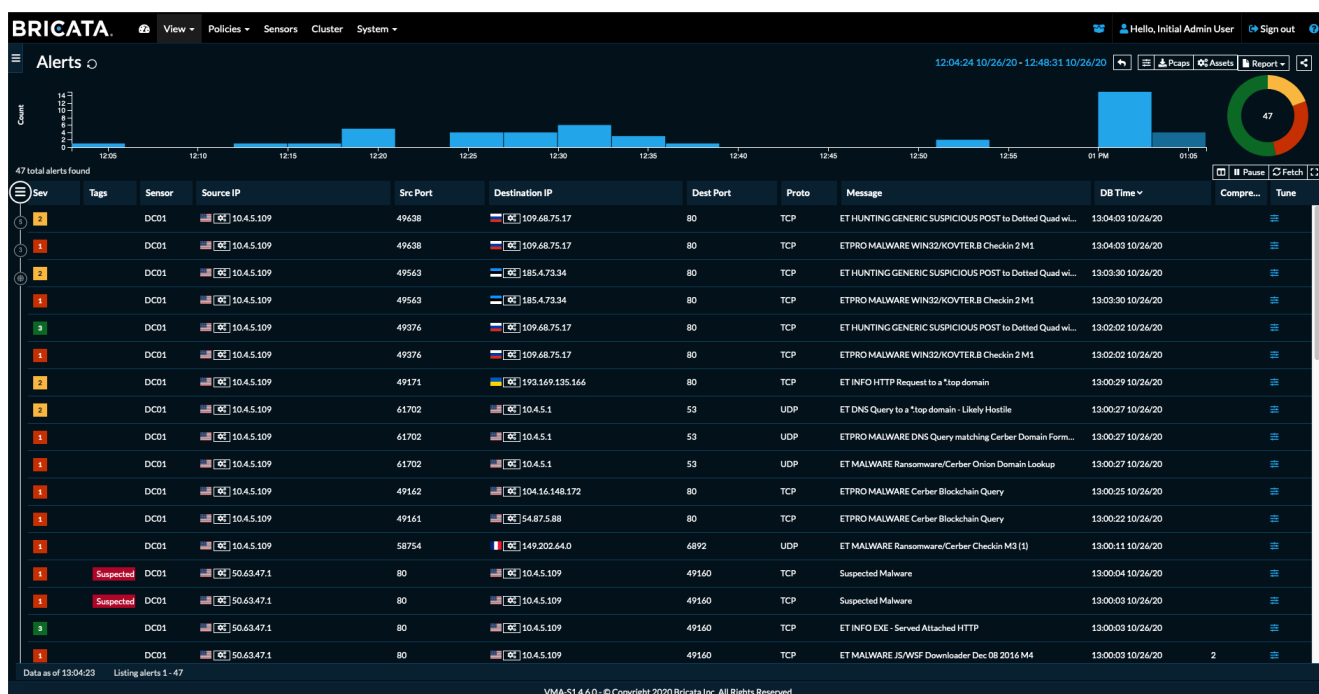
Bricata's software based solution in conjunction with its cost effective consumption based pricing allow organizations to eliminate network blind-spots and monitor traffic flows in every direction "north-south" or "east-west" without compromise.

By default Bricata analyzes, extracts and captures critical information on every network transaction good or bad providing security teams with long-term information to not only react to an incident but retrospectively apply today's intelligence to historical data to ensure there aren't any gaps in protection.

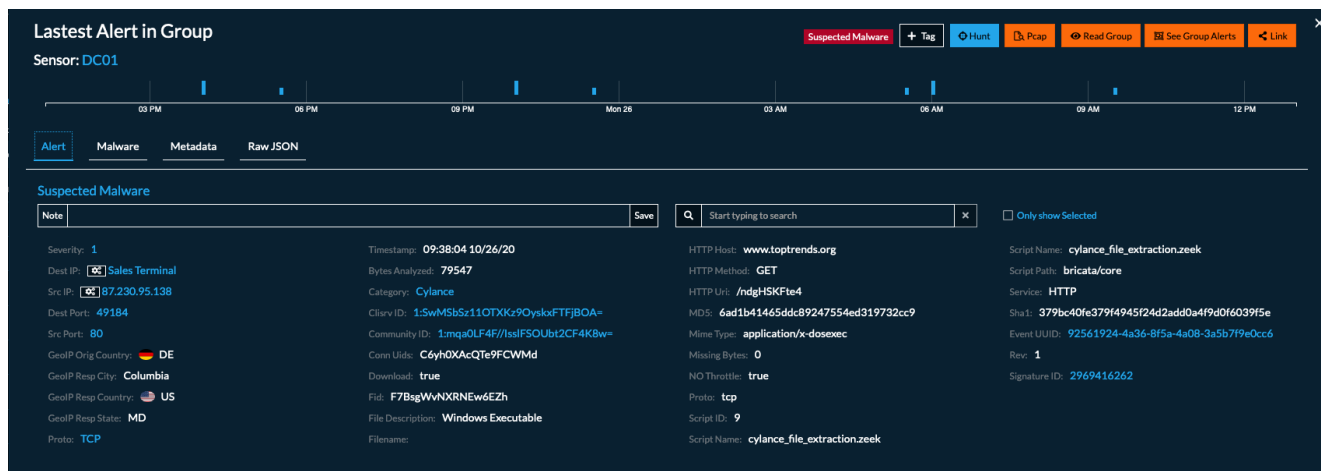
Bricata offers advanced NDR protection with multiple detection engines and threat feeds to defend network traffic and core assets.



FIGURE 1: CONSOLIDATED ALERT VIEW SHOWS WHICH ENGINE IS USED IN RIGHT COLUMN

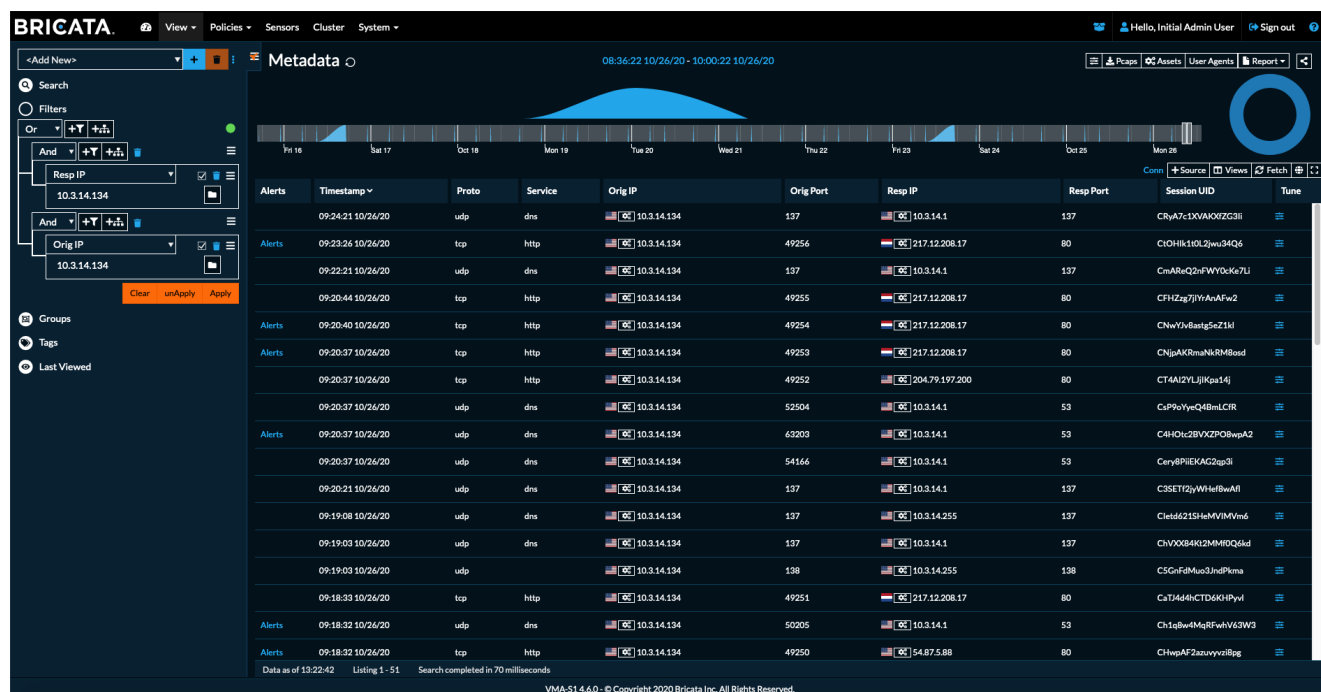


**FIGURE 2: ALERT DETAIL OF KNOWN MALWARE IDENTIFIED BY CYLANCE ENGINE**



The historic data is searchable, allowing IT staff to confirm that no similar variant of any captured malware previously snuck past defenses. All data is collected using an on-prem system, so organizations never lose control of their intellectual property, and no third-party infrastructure is required to use it.

**FIGURE 3: METADATA SHOWS HOW USER TRANSITIONED FROM NORMAL BROWSING, TO DOWNLOADING MALWARE, TO LATERAL SPREAD OF MALICIOUS CONTENT.**



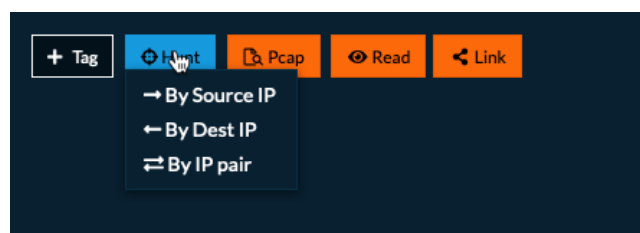


CSO Magazine recently reviewed the Bricata platform, finding it to be [among the best](#) in the industry in terms of complete NDR protection. During that trial, Bricata was able to detect both the presence of malware landing on a client system, and the fact that the malicious program beacons out and infected other hosts using lateral movement, something that would have been camouflaged to many other IDS systems.

In addition to great baseline NDR protection, Bricata incorporates the advanced defensive technique of threat hunting into the same console. Every tracked incident has a bright orange button in the corner that is used to initiate a threat hunt. Once started, Bricata collects all relevant information that a hunter would require for a successful investigation, including all indicators of compromise and detailed information about any other systems or clients, outside the network or within, where a suspected compromised host interacted.

The threat hunting interface is extremely easy to use, tapping into the same interface that cybersecurity teams use every day with the NDR part of the platform. Designed this way, it adds a highly effective threat hunting tool into the hands of less-skilled or junior IT staff, elevating the efficiency of the entire SOC team. This in turn reduces the need for more highly-paid and hard-to-find security analysts, or for expensive and lengthy training sessions to teach the nuances of overly-complex threat hunting tools. In fact, Bricata does such an excellent job at streamlining the threat hunting process, only minimal training is ever required.

**FIGURE 4: NETWORK THREAT HUNTING SIMPLIFIED**



Bricata cannot only catch the initial landing of malware, but can track its lateral movement to give defenders a complete picture of the threat, and the full scope of the problem.

There are also several advanced threat hunting features bundled into the interface that are normally only present in dedicated threat hunting programs. For example, traffic can be examined to look for anomalies manually, even ones that are not triggering alerts. This would be more of a pure threat hunting activity where users would form a hunch and do their own investigating.

## Bricata Versus Real World Threats

No cybersecurity program is always going to be perfect every time, but Bricata's unique blend of robust baseline protection and advanced threat hunting features fares well against the kind of threats making headlines today.

Take the example of the [city of Atlanta](#), or the ransomware that [swept through Europe](#) last year. In most of those cases, the initial infection on a client machine was caught and mitigated by alert security teams. But because they were blind to lateral movement and had limited or no threat hunting tools, the spread of the malware to other systems throughout the network was not discovered until many other clients started to go down. Bricata can not only catch the initial landing of malware, but can track its lateral movement to give defenders a complete picture of the threat, and the full scope of the problem.

In the case of US power plants [getting probed by](#) Russian hackers, US-CERT issued a warning complete with threat indicators and intelligence about a week later. This enabled power plant operators to close the door on the gaps attackers used. However, that only protected them against future incursions. They would still be vulnerable to anything the hackers previously left behind, and would have no way of knowing definitively if they had been breached in the first place.

That would not be the case with Bricata protecting their network. Users could easily go back at least 11 days, and longer if configured for it, to see if any threats bypassed the new access rules before they were solidly in place. It would give plant operators peace of mind, and like with the ransomware cases, a complete and total view into their situation.



## The Big Picture

In conclusion, the best form of network protection would have the following characteristics:

- Accurate baseline protection through NDR;
- Be able to look back and check for threats against historic traffic data;
- Add advanced protections such as network threat hunting;
- Use one interface for every element in the toolset to minimize training and skill level requirements;
- And be extremely easy to use.



The Bricata network detection and response platform offers all of this and more. It is one of the only security toolsets to incorporate a 360 degree approach to threat detection by combining signature, behavior and advance malware analysis with network visibility in a single solution.

Want to learn more about Bricata and how this innovative platform can help you defend your own network from the most insidious threats without negatively impacting productivity? Contact us at [info@bricata.com](mailto:info@bricata.com) or 888.468.0610.



# BRICATA®



## ABOUT BRICATA

Bricata is a cybersecurity solutions provider that combines a powerful network threat hunting platform into a comprehensive IDPS solution to help determine the true scope and severity threats. Bricata simplifies network threat hunting by identifying hidden threats using specifically designed hunting workflows that use detailed metadata provided clearly and eases your transition from the known to unknown malicious activities in conjunction with a modern IDPS platform which detects zero-day malware conviction.

## BRICATA HQ

9711 Washingtonian Blvd  
Gaithersburg, MD 20878



---

INFO@BRICATA.COM

[ 8 8 8 ] 4 6 8 - 0 6 1 0

BRICATA.COM

