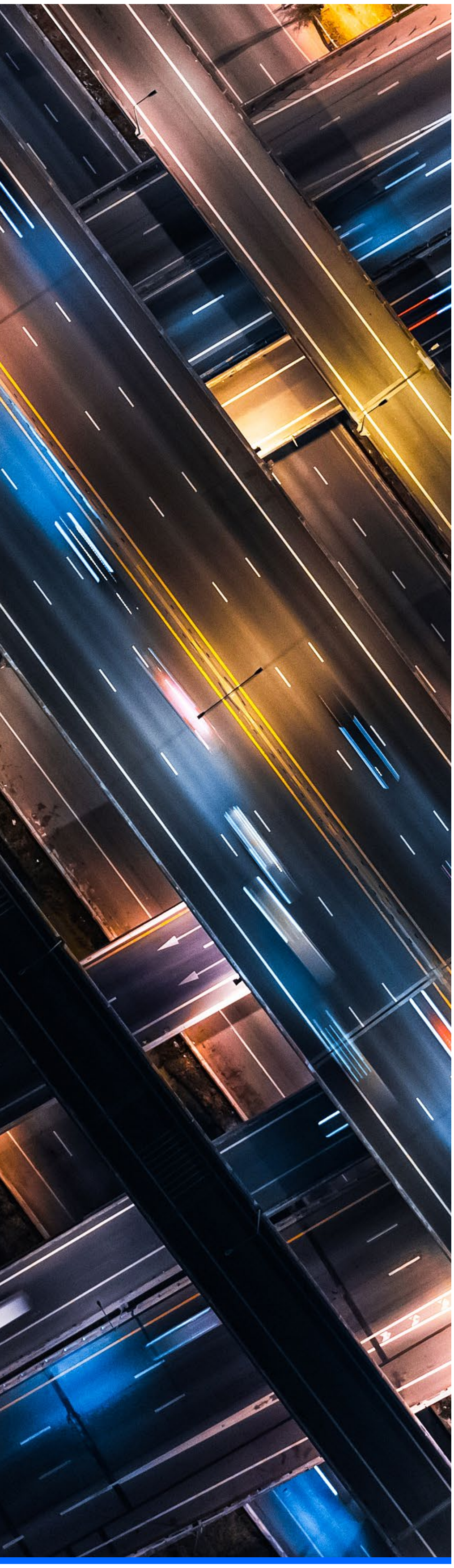
opentext™

Natural network threat hunting emerging as key to modern cyber resilience

Contents



Executive summary

Today's computer networks may seem to be 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.

Anti-virus and anti-malware programs are embedded on just about every endpoint, sandboxing tools examine incoming programs for malicious intent, intrusion detection or prevention systems watch over data packets, firewalls and next-generation firewalls segregate all parts of a network from the outside world and security information and event management solutions (SIEMs) monitor every 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 is likely not their company's primary focus.

Yet, cyber-attacks still get through and are happening in increasingly large numbers.

The Verizon Breach Investigations Report hit another high in 2021, tracking 23,896 security incidents that resulted in 5,212 confirmed breaches. Year over year, ransomware attacks increased by 13 percent, a jump greater than the past five years combined.[1]

Clearly there are problems with the way IT defenses are managed and deployed today. Highly sophisticated threats from motivated attackers are on the rise, while many organizations aren't able to field enough skilled cybersecurity professionals to combat them. Many of the advanced tools and tactics needed to defend networks, such as data analysis techniques or building investigative processes into workflows, aren't in place.

[1] Verizon, 2022 Data Breach Investigations Report. (2022)

Defensive shortfalls

One of the most serious challenges is not one of technology, but one of training. There simply are not enough trained IT professionals to go around. It does not matter how many tools are employed, or how good they are, if there are no trained staff to use 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, the U.S. alone has 180,000 unfilled openings for information security analysts, plus another 534,548 openings seeking cybersecurity-related skills. The problem is getting worse, not better. Estimates put the shortfall globally at anywhere between 1.8 million to 3.5 million open cybersecurity positions in the next five years.[2]

Even governments are desperate to employ more IT professionals. According to a 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, spending a lot of money to train them.

Networking is not getting any simpler. Every time a new application, technology, client, server, cloud or device is added to a network, the number of potential vulnerabilities grows. Additional items often introduce multiple vulnerabilities, so the attack footprint grows much faster than the network itself.

Reactive incident response often exacerbates the problems by 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 most serious challenges is not one of technology, but one of training. There simply are not enough trained IT professionals to go around.

[2] Global Tech Council, Cybersecurity Jobs Report: 3.5 Million Openings Through 2025. (2021)

[3] The Pew Charitable Trusts, Cybersecurity Quest Sends States to Vets, Students and Women. (2017)

Hackers moving laterally stay ahead of beleaguered defenders

One only needs to look at recent ransomware attacks to see the dangers of lateral movement. The JBS ransomware attack in 2021 highlighted the need for earlier detection and rapid response.[4]

Modern ransomware campaigns, like those that affected JBS and Colonial Pipeline, build a presence inside the target network long before the actual ransomware is deployed. Typically, attackers are in the network moving laterally, stealing data and credentials, deploying additional tools and only then execute ransomware as the final stage.

A similar attack happened in Europe, where a variant of the Petrwrap/Petya ransomware brought business to a halt at banks, airports, government offices, service providers and more. While each of the initial infections was eventually caught, it was not before the malware secretly spread using lateral movement to other systems on the same network—undetectable to most security programs.

In the United States, critical infrastructure in the form of power plants was recently breached by a suspected Russian hacker group. 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).[5]

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 do not have the ability to look back in time, so those same plants may never know if they were breached before the report was released.

Beyond the obvious security problems, or any ransom demanded by an attacker, responding to every breach costs organizations a lot of money. According to a Ponemon Institute data breach study, the average cost of a data breach in 2021 was US $4.24 million, up 10 percent from the average cost of $3.86 million in 2019. In 2021, ransomware attacks cost companies worldwide well over $6 trillion.[6] That estimate does not include 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.

[4] OpenText, JBS Ransomware attack highlights need for early detection and rapid response. (2021)

[5] Cybersecurity & Infrastructure Security Agency, Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. (2018)

[6] Security Intelligence, What's New in the 2021 Cost of a Data Breach Report. (2021)

How can we shore up defenses?

These examples show 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 to take multiple training sessions to learn their complex interfaces.

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 were not 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.

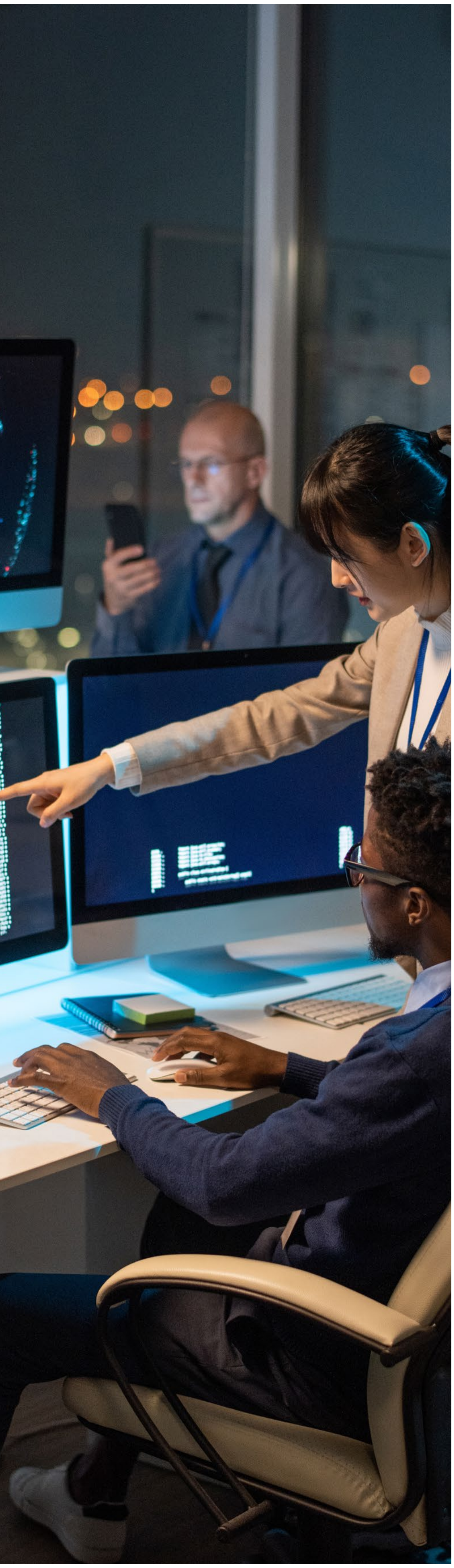
The process that most cybersecurity teams use to handle security alerts is inadequate against advanced threats capable of lateral movement.

The perfect solution for a modern cybersecurity defense

Talking about a perfect security toolset is difficult because fixating on the ideal can often get in the way of achieving 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.

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 network detection and response (NDR) systems, which can make an IT worker's daily cybersecurity tasks a lot more effective.

The ideal platform should be very easy to use, 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 within 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.

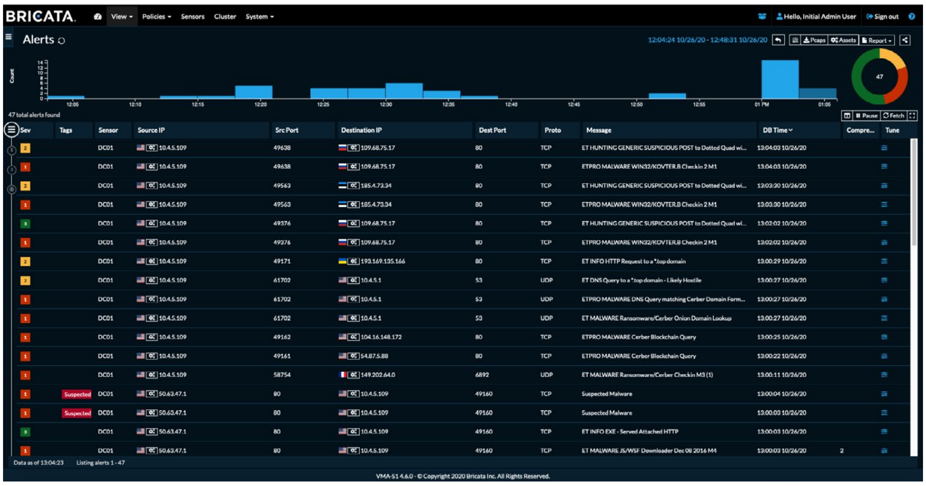
The complete defensive package with OpenText™ Network Detection and Response

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

OpenText's software-based NDR solution, in conjunction with its cost-effective consumption-based pricing, allows organizations to eliminate network blind spots and monitor traffic flows in every direction without compromise.

By default, OpenText NDR analyzes, extracts and captures critical information on every network transaction, good or bad. Security teams are equipped with long-term information to not only react to an incident but retrospectively apply today's intelligence to historical data, ensuring there are no gaps in protection.

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



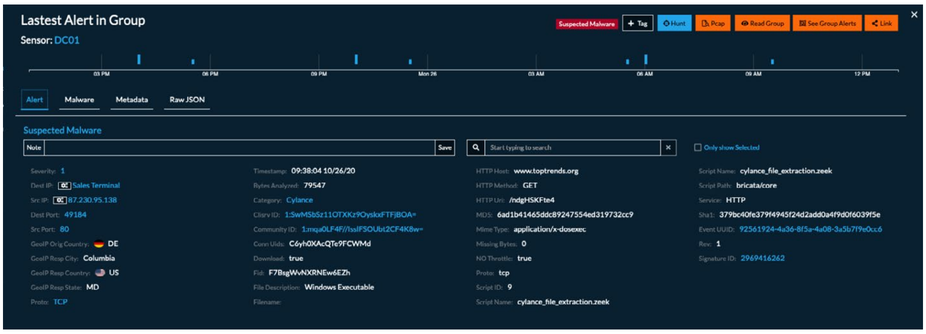
47 total alerts found

Sev	Tags	Sensor	Source IP	Src Port	Destination IP	Dest Port	Proto	Message	DB Time	Compre...	Tune
2		DC01	10.4.5.109	49638	109.68.75.17	80	TCP	ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad wi...	13:04:03 10/26/20		☰
1		DC01	10.4.5.109	49638	109.68.75.17	80	TCP	ETPRO MALWARE WIN32/KOVTER.B Checkin 2 M1	13:04:03 10/26/20		☰
2		DC01	10.4.5.109	49563	185.4.73.34	80	TCP	ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad wi...	13:03:30 10/26/20		☰
1		DC01	10.4.5.109	49563	185.4.73.34	80	TCP	ETPRO MALWARE WIN32/KOVTER.B Checkin 2 M1	13:03:30 10/26/20		☰
3		DC01	10.4.5.109	49376	109.68.75.17	80	TCP	ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad wi...	13:02:02 10/26/20		☰
1		DC01	10.4.5.109	49376	109.68.75.17	80	TCP	ETPRO MALWARE WIN32/KOVTER.B Checkin 2 M1	13:02:02 10/26/20		☰
2		DC01	10.4.5.109	49171	193.169.135.166	80	TCP	ET INFO HTTP Request to a *.top domain	13:00:29 10/26/20		☰
2		DC01	10.4.5.109	61702	10.4.5.1	53	UDP	ET DNS Query to a *.top domain - Likely Hostile	13:00:27 10/26/20		☰
1		DC01	10.4.5.109	61702	10.4.5.1	53	UDP	ETPRO MALWARE DNS Query matching Cerber Domain Form...	13:00:27 10/26/20		☰
1		DC01	10.4.5.109	61702	10.4.5.1	53	UDP	ET MALWARE Ransomware/Cerber Onion Domain Lookup	13:00:27 10/26/20		☰
1		DC01	10.4.5.109	49162	104.16.148.172	80	TCP	ETPRO MALWARE Cerber Blockchain Query	13:00:25 10/26/20		☰
1		DC01	10.4.5.109	49161	54.87.5.88	80	TCP	ETPRO MALWARE Cerber Blockchain Query	13:00:22 10/26/20		☰
1		DC01	10.4.5.109	58754	149.202.64.0	6892	UDP	ET MALWARE Ransomware/Cerber Checkin M3 (1)	13:00:11 10/26/20		☰
1	Suspected	DC01	50.63.47.1	80	10.4.5.109	49160	TCP	Suspected Malware	13:00:04 10/26/20		☰
1	Suspected	DC01	50.63.47.1	80	10.4.5.109	49160	TCP	Suspected Malware	13:00:03 10/26/20		☰
3		DC01	50.63.47.1	80	10.4.5.109	49160	TCP	ET INFO EXE - Served Attached HTTP	13:00:03 10/26/20		☰
1		DC01	50.63.47.1	80	10.4.5.109	49160	TCP	ET MALWARE JS/WSF Downloader Dec 08 2016 M4	13:00:03 10/26/20	2	☰

Data as of 13:04:23   Listing alerts 1 - 47

VMA-S1 4.6.0 - © Copyright 2020 Bricata Inc. All Rights Reserved.

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



Lastest Alert in Group

Sensor: DC01

Suspected Malware

□ Only show Selected

Severity: 1
Dest IP: Sales Terminal
Src IP: 87.230.95.138
Dest Port: 49184
Src Port: 80
GeoIP Orig Country: DE
GeoIP Resp City: Columbia
GeoIP Resp Country: US
GeoIP Resp State: MD
Proto: TCP

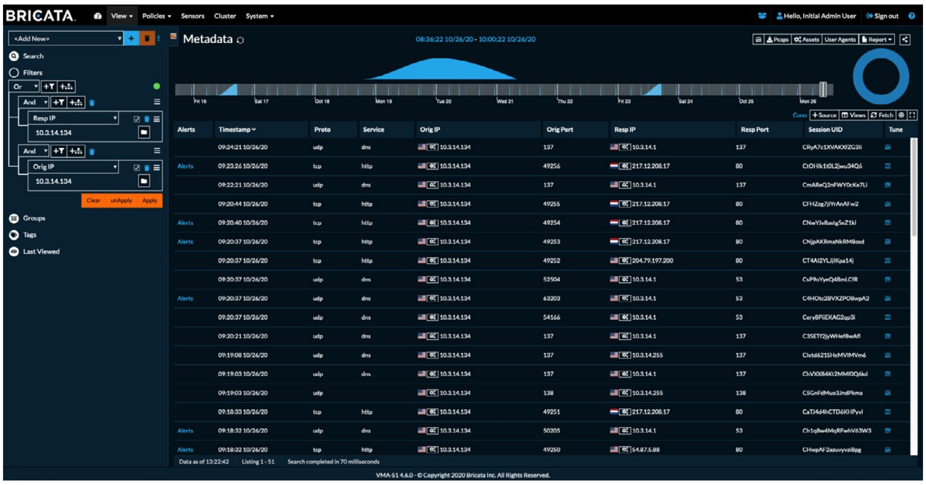
Timestamp: 09:38:04 10/26/20
Bytes Analyzed: 79547
Category: Cylance
Clsrv ID: 1:SwMSbSz11OTXKz9OyskxFTFjBOA=
Community ID: 1:mqa0LF4F//IssIFSOUbt2CF4K8w=
Conn Uids: C6yh0XAcQTe9FCWMd
Download: true
Fid: F7BsgWvNXRNEw6EZh
File Description: Windows Executable
Filename:

HTTP Host: www.toptrends.org
HTTP Method: GET
HTTP Uri: /ndgHSKFte4
MD5: 6ad1b41465ddc89247554ed319732cc9
Mime Type: application/x-dosexec
Missing Bytes: 0
NO Throttle: true
Proto: tcp
Script ID: 9
Script Name: cylance_file_extraction.zeek

Script Name: cylance_file_extraction.zeek
Script Path: bricata/core
Service: HTTP
Sha1: 379bc40fe379f4945f24d2add0a4f9d0f6039f5e
Event UUID: 92561924-4a36-8f5a-4a08-3a5b7f9e0cc6
Rev: 1
Signature ID: 2969416262

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-premises system, so organizations never lose control of their intellectual property and no third-party infrastructure is required to use it.



Or
And
Resp IP ☑
10.3.14.134
And
Orig IP ☑
10.3.14.134

Metadata

08:36:22 10/26/20 - 10:00:22 10/26/20

Alerts	Timestamp	Proto	Service	Orig IP	Orig Port	Resp IP	Resp Port	Session UID	Tune
	09:24:21 10/26/20	udp	dns	10.3.14.134	137	10.3.14.1	137	CRyA7c1XVAKXfZG3li	☰
Alerts	09:23:26 10/26/20	tcp	http	10.3.14.134	49256	217.12.208.17	80	CtOHlk1t0L2jwu34Q6	☰
	09:22:21 10/26/20	udp	dns	10.3.14.134	137	10.3.14.1	137	CmAReQ2nFWY0cKe7Li	☰
	09:20:44 10/26/20	tcp	http	10.3.14.134	49255	217.12.208.17	80	CFHZzg7jlYrAnAFw2	☰
Alerts	09:20:40 10/26/20	tcp	http	10.3.14.134	49254	217.12.208.17	80	CNwYJv8astg5eZ1kl	☰
Alerts	09:20:37 10/26/20	tcp	http	10.3.14.134	49253	217.12.208.17	80	CNjpAKRmaNkRM8osd	☰
	09:20:37 10/26/20	tcp	http	10.3.14.134	49252	204.79.197.200	80	CT4AI2YLJjIKpa14j	☰
	09:20:37 10/26/20	udp	dns	10.3.14.134	52504	10.3.14.1	53	CsP9oYyeQ4BmLCfR	☰
Alerts	09:20:37 10/26/20	udp	dns	10.3.14.134	63203	10.3.14.1	53	C4HOtc2BVXZPO8wpA2	☰
	09:20:37 10/26/20	udp	dns	10.3.14.134	54166	10.3.14.1	53	Cery8PiiEKAG2qp3i	☰
	09:20:21 10/26/20	udp	dns	10.3.14.134	137	10.3.14.1	137	C3SETf2jyWHef8wAfl	☰
	09:19:08 10/26/20	udp	dns	10.3.14.134	137	10.3.14.255	137	Cletd621SHeMVIMVm6	☰
	09:19:03 10/26/20	udp	dns	10.3.14.134	137	10.3.14.1	137	ChVXX84Kt2MMf0Q6kd	☰
	09:19:03 10/26/20	udp		10.3.14.134	138	10.3.14.255	138	C5GnFdMuo3JndPkma	☰
	09:18:33 10/26/20	tcp	http	10.3.14.134	49251	217.12.208.17	80	CaTJ4d4hCTD6KHPyvl	☰
Alerts	09:18:32 10/26/20	udp	dns	10.3.14.134	50205	10.3.14.1	53	Ch1q8w4MqRFwhV63W3	☰
Alerts	09:18:32 10/26/20	tcp	http	10.3.14.134	49250	54.87.5.88	80	CHwpAF2azuvyvzi8pg	☰

Data as of 13:22:42 Listing 1 - 51 Search completed in 70 milliseconds

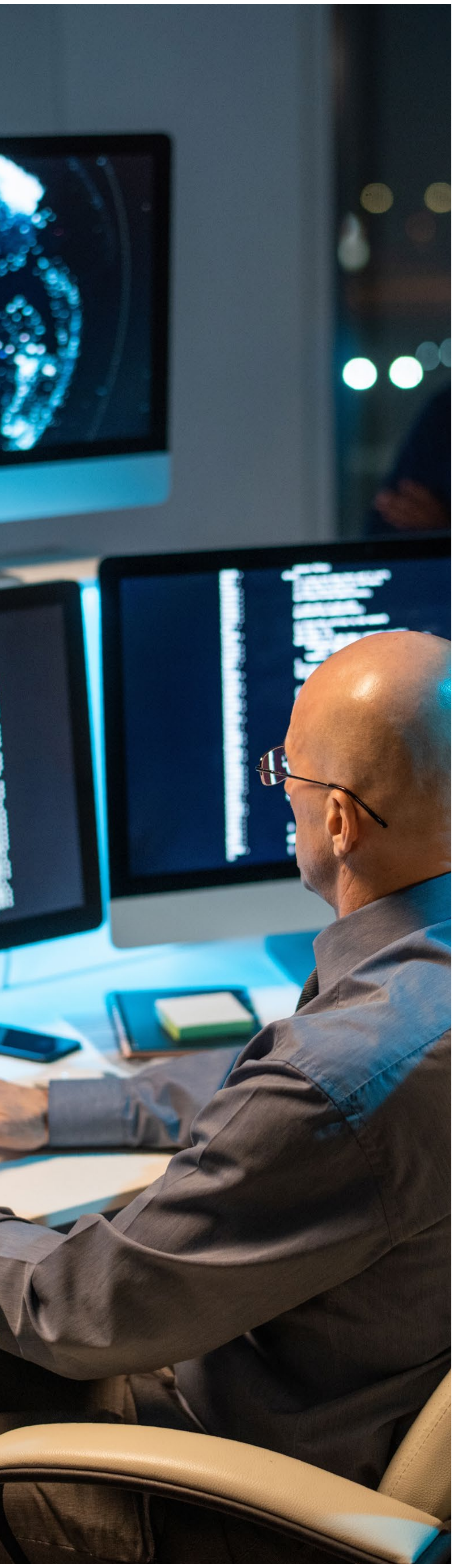
VMA-S1 4.6.0 - © Copyright 2020 Bricata Inc. All Rights Reserved.

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

CSO Magazine recently reviewed the OpenText NDR (formerly Bricata) platform, finding it to be among the best in the industry in terms of complete NDR protection.[7] During that trial, OpenText NDR was able to detect both the presence of malware landing on a client system and the fact that the malicious program then beaconed out and infected other hosts using lateral movement, something that would have been camouflaged to many other IDS systems.

OpenText NDR also incorporates the advanced defensive technique of threat hunting. Every tracked incident has a bright orange button in the corner that is used to initiate a threat hunt. Once started, OpenText NDR 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.

[7] CSO Online, Review: Bricata adds threat hunting to traditional IPS/IDS. (2018)



The threat hunting interface is extremely easy to use, tapping into the same interface that cybersecurity teams use every day. 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 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, OpenText NDR does such an excellent job of streamlining the process that only minimal training is ever required.

There are also several advanced threat hunting features bundled into the interface that are typically only found in dedicated threat hunting programs. For example, traffic can be examined to look for anomalies manually, even ones that are not triggering alerts. This function is useful when users form a hunch and need to do their own investigating.

OpenText NDR versus real-world threats

OpenText NDR's unique blend of robust baseline protection and advanced threat hunting features fares well against the kinds of threats making headlines today.

Take the example of the city of Atlanta, or the ransomware that swept through Europe last year. In those cases, alert security teams caught and mitigated the initial infection on a client machine. Unfortunately, they were blind to lateral movement and had limited or no threat hunting tools, so they did not discover the spread of malware throughout the network until many other clients started to go down. OpenText NDR not only catches the initial landing of malware, but also tracks its lateral movement to give defenders a complete picture of the threat and the full scope of the problem.

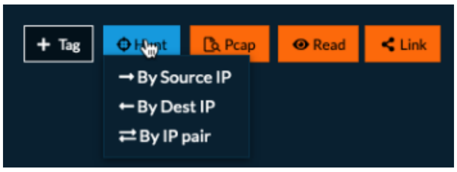


FIGURE 4: NETWORK THREAT HUNTING SIMPLIFIED

In the case of U.S. 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, but that only protects against future incursions. They would still be vulnerable to anything hackers had left behind and would have no way of knowing if they had been breached in the first place.

That would not be the case with OpenText NDR. Users could easily go back at least 11 days (longer if configured for it) to see if any threats bypassed the new access rules before they were in place. This would give plant operators peace of mind via a reliably complete view into their situation.

opentext™

Learn More

Cyber Resilience - OpenText Blogs

OpenText Threat Detection and Response Solutions

The big picture

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

- Accurate baseline protection through NDR
- The ability to look back and check for threats against historic traffic data
- Advanced protections, such as network threat hunting
- A single interface for every element in the toolset to minimize training and skill level requirements
- Be extremely easy to use

The OpenText™ 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 OpenText NDR and how this innovative platform can help you defend your network from the most insidious threats, without negatively impacting productivity? Contact us

Connect with us:

OpenText CEO Mark Barrenechea's blog
Twitter | LinkedIn

opentext.com/contact