opentext

OpenText Network Detection & Response

Identify and eliminate blind spots in the network



Benefits

- Visibility
- Context
- Detection
- Response

OpenText[™] Network Detection & Response (NDR) is leading the next generation of advanced network detection and response solutions for the enterprise. Fusing detection, forensic analysis and proactive threat hunting, OpenText Network Detection & Response empowers high-performance enterprise security teams with total visibility into network traffic. With signature inspection, stateful anomaly detection and machine learning-powered malware conviction, OpenText Network Detection & Response empowers security teams to effectively defend against known threats and to illuminate those otherwise unseen.

OpenText Network Detection & Response provides organizations with 360-degree protection, end-to-end visibility and context for direct answers and powerful insight to take immediate action.

The solution provides complete visibility of east-west traffic across network environments in real time and full-spectrum threat detection that extracts and stores high-fidelity metadata, including an indexed threat hunting repository.

A multi-faceted suite of best-in-breed threat detection allows organizations to thoroughly inspect network traffic from every angle. Users can find unknown, hidden threats to conduct retrospective network traffic analysis and historical data testing to determine if threats infiltrated the environment prior to known indicators being available. They can use meaningful visualizations and flexible network views to see everything in a single pane of glass or create custom views for what matters most for their network. **"MAD Security is** growing extremely rapidly: we've increased our client base by a factor of three in just a few years, and our goal is to grow a further 400 percent in the next three years. We targeted a NDR solution that could scale to help us hit that growth target while keeping our analyst team lean.

"Thanks in large part to OpenText [Network Detection & Response], we can now detect and correlate events, investigate the data and notify the client in an average of just 6.5 minutes—less than half our SLA."

Jeremy Conway, CEO, MAD Security OpenText Network Detection & Response eliminates security blind spots through real-time network visibility. Organizations can see everything on their network via high-fidelity metadata and SmartPCAP, take advantage of full-spectrum threat detection and reduce noise and optimize detection with multiple detection engines examining the network from every angle. Users can thoroughly and proactively investigate detected threats and hunt down unknown threats that did not generate an alert with forensic precision. With seamless response and extensive integrations, organizations can correlate alerts in real time, enrich existing workflows, automate responses, and prevent threats. OpenText Network Detection & Response is the only end-to-end network detection and response platform that allows both security teams and the entire enterprise to collaborate better, reduce security risk, and solve network problems faster than ever before.

Next-gen sensors

• Total network visibility of internal and web-bound traffic

Powerful centralized management

• Customizable dashboards for response, analysis, forensic investigation, and threat hunting

Smart data nodes

• Intelligently extracts and stores rich network metadata within a smart scalable repository for efficient threat hunting and incident response

Protect from all sides



Product features chart

Q See

- Total network visibility See everything happening on the network
- Full-spectrum threat detection Use signature inspection, anomaly detection and ML-based malware conviction
- High-fidelity metadata Gain a better understanding with rich metadata from every transaction

⁻̈̈́Ѽ҉ Know

- **Proactive threat hunting** Leverage indexed enriched data repository
- Smart PCAP
 Quickly access relevant metadata
- Forensic investigation Effectively investigate events with network packets

R Act

- Better detection Take advantage of automated analysis, prioritized workflows
- Faster response Clear queues faster than ever
- Customizable and flexible Tune easily with a wide breadth of integrations

Services

Next-gen Services >

Resources

Security - OpenText Blogs >

OpenText threat detection and response solutions >



BR	RICAT	Α.							0	SHBOARD 🗿		Ө на	o nationa da entre	в 🙁 совоит
	B 1 10		م <u>م</u>								LAST		tre	
	G 363										LASTH	OUR 10:52	:06/27/ 🖬 11	53 06/27/ 💼 🦷
•														\frown
	sda .		Na	nder	1 4 - 1 - 1 - 1 - 1		nden reim		al a	ndar.	19/22		wd.yr	40,156
A (=														e e i
↔	Service												Columes	
0 0														
		~			sar-01 🛋 🛊 192.168.		a 192.168.10.3						dra	
				bricata-sen	sor-01 🔎 🛊 192.168.		a (* 172.217.12.195	11:51:50 06/27/22						
•	1,410													
• *					sar-01 🛲 🛊 192.168.		D 0 208.81,1.244							
-				bricata-sen	sar-01 🛤 🛊 192.168.		a 192.168.10.50	11:50:49 06/27/22		38942				
					sar-81 💻 🛊 192.168.		192.168.10.50	11:51:30 06/27/22						
					sor-01 🚅 🛊 192.168.		2 192.168.10.50	11:51:30 06/27/22					fip-data	
					sar41 🛋 🛊 192.168.		2 192.168.10.3							
					sarði 🚅 🛊 192.168.		# 0 192.168.10.3	11:46:36 06/27/22						
					sar-01 🛤 🏟 192.168.		a († 192.168.10.3							
					sar-01 💻 🏟 192.168.		a 192,168,10,3							
					sar-91 🛤 😋 192.168.		a 192.168.12.3							
				bricata-sen	sor-01 🐖 🔅 192,168.		a 192,168,10,3							
BE	Defamici 115					08336-	Search completed in 1	2 millioconda	0.0	SHBOARD Ø	SUPPORT	A IN	o.1.daa	Listing Raws 1 - 13 of 13
		A. ws > Alerts	<u>२</u> छ			04534-	Search completed in 1	2 millinecoods	0	SHBOARD 👔	SUPPORT		0,1 daar aa a	- <u>S</u> LOSOUT
> @ 		A. ws > Alerts	. २ 🔊	atu	aiu	or 111.	Search complete in 1 a Conservation 2001 Monacolary of B War 27	aniineenna	۵ D	SHBOARD ?				- <u>S</u> LOSOUT
> • • • •		A. ws. > Alerts mch alerts. >> aiw	- Q - Đ	อย่าน	ate	04 131 -		den Alexand	@ •	SHBOARD @				- O LOGOUT
· · · · · · · · · · · · · · · · · · ·		A. vrs. > Alerts archalerts > arbu	<u>α</u> Φ		sa Fue ouurce 12	000 1111-		da karanad Da Ada		SHBONID @			106/26/ 🔂 11	- 0 LOGOUT
→ ¹ = 0 6 ·		A. ws. > Alerts archalerts > arbu ms 20 @ Courre 4					Water	an berned at an berned Dest		estu Message		Sat DAY 11:50	106/26/ 🖬 11 11 11 12 14 12 14 15 14 15 14 15 15 15 15 15 15 15 15 15 15 15 15 15	- O LOGOUT
· · · · · · · · · · · · · · · · · · ·	CMC > View	A. Alerts with alerts and alerts	Seve	Sens S bricata-senso #			w	gilaer J. Desc		actuu Message ETPRO DNS SRu	LUST	DAY 21150	106/26/ 🖬 11 11 12/14 1	- O LOGOUT
→ ¹ = 0 6 ·		A. ws > Alerts where the series where the ser		Sens S bricata-senso bricata-senso	ource 1P 1 @ 192.168.10.8 2 @ 195.54.160.149		Barrowski (1991) Bornardow (1991) Barrowski (1992) Destination (P	9) for 1 Dec 53 69		ockar Message ETPAD DNS Sku ET HUNTING Pe	LUST	DAY 11.50	1 06/26/ 1 11 1 06/26/ 1 11 1 00/104 1 00/104 1 7ag 1 7ag 1 7ag 1 7ag 1 7ag	- O LOCOUT
→	CMC > View	A. vis > Alerts where the alerts > I court 4 I	Seve	Sens S bricata-senso bricata-senso	ource 3P 1 © 192.168.10.8 1 © 195.54.160.143 1 © 195.54.160.143		w_27 Decision IP ■ Q 104.7124731	91 fores		actuu Message ETPRO DNS SRu	LAST	Start EAV 11.50 DAV 11.50 DAV 11.50 DAV 11.50 DAV 11.50 DAV 11.50	Encode Encode<	- O LOGOUT
> 5 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CMC > View CMC > View tube tube contract	A	5eve	Sens S bricata-senso bricata-senso bricata-senso bricata-senso	ource 3P © 192.168.10.8 © 195.54.160.149 © 195.54.160.149 © 195.54.160.149	5rc P., 33733 39920 57542	w_2F Presidention (F) @ 0 112 146 10.3 @ 0 118 71.24731 @ 0 118 7.124731 @ 0 118 7.124731	11 fair 1 fair 1 Dec., 1 53 60 60 60 60		no Aust Message ETFRIO Dires Sau ET HUNTING Pe ET HUNTING Pe	LAST	DAV 11.50	Crief (26/26/ 27) 11 11 11 11 11 11 11 11 11 11	- O LOGOUT
> 5 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CMC > Viet CMC > Viet CMC > Viet CMC > 04 CMC = 04237042 04371042 0437134042 073214042 07324042	A. Alerts X with a block of the second seco	Seve	Sens S bricata-senso = bricata-senso = bricata-senso = bricata-senso =	ource 3P 1 © 192.168.10.8 1 © 195.54.160.143 1 © 195.54.160.143	5rc P 33733 39920 57842 55736	w.⊊? Desisation (P ■ © 112.166.10.3 ■ © 118.71.247.31 ■ © 118.71.247.31	11 fair 1 fair 1 Dec., 1 53 60 60 60 60		uskas Message ETPRO DIVIS SILL ET HUNTING PO ET HUNTING PO ET HUNTING PO	LLST Effectivity Encry solible Apache Is solible Apache Is solible Apache Is solible Apache Is	DAY 2011 DAY 11.50 Day 10.50 Day 10.	Columno dela 2 pt - Kary	- O LOGOUT
> 5 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CMC > Vier CMC > Vier CMC > Vier CMC > Vier CMC > Vier Common CMC > Vier Common CMC > Vier Common CMC > Vier CMC >	Alerts s Alerts wh w court	Seve	Sens S bricata-senso = bricata-senso = bricata-senso = bricata-senso =	ource 3P 1 (2) 192.168.10.8 1 (2) 195.2168.10.3 (2) 195.54.100.149 (2) 195.54.100.149 (2) 195.52.10.66 (3) 195.21.100.238 (4) 117.14.166.217	Src P 33733 39920 57542 55736 443	■ 97 ■ 0 112 164 103 ■ 0 112 164 103 ■ 0 118 71 20731 ■ 0 118 71 20731 ■ 0 118 71 20731 ■ 0 118 71 20731 ■ 0 118 71 20731 ■ 0 118 71 20731	3) for benevit Dec., 53 69 69 69 69 69 69 69 69 69 69 69 69 69		or Mar Message ETPHO DNS Sku ET HUNTING Po ET HUNTING Po ET HUNTING Po ET MAUNARE M	LLST Elsecurity Encry solible Apache Is solible Apache Is solible Apache Is solible Apache Is solible Apache Is telespreter or Co	DAY 25st DAY 11.50 Day 11.	66/26/ En 11 11 12 11 13 11 14 11 15 11 15 11 15 11 15 11 15	- O LOGOUT
> 5 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	CMC > Viet	A. Alerts vs > Alerts x mrth alerts x mrg 10 0	Seve	Sers S bricata-senso = bricata-senso = bricata-senso = bricata-senso = bricata-senso = bricata-senso =	ource 3P (0) 192,168,10.8 (0) 195,54,103,149 (0) 195,54,103,149 (0) 195,54,103,149 (0) 195,54,103,149 (0) 195,54,103,149 (0) 195,54,103,149 (0) 197,14,166,217 (0) 10,1,6,101	Src P 33733 39920 57842 55736 443 47891		3) Jose		or Mar Message ETPRO DAS Sku ET HUNTING PC ET HUNTING PC ET HUNTING PC ET MAURIAE M ET SCANJANS Y	LAST	DAY 25st DAY 11.50 Day 11.	66/26/ En 11 11 12 11 13 11 14 11 15 11 15 11 15 11 15 11 15	- O LOGOUT
	CMC > Vier CMC >	Alerts wrs > Alerts wrs wrs Alerts x	Seve	Sens S bricata-senso = bricata-senso = bricata-senso = bricata-senso = bricata-senso = bricata-senso =	ourre 32 (c) 192,168,108, (c) 195,54,108,149 (c) 195,54,108,149 (c) 195,54,108,149 (c) 195,521,08,64 (c) 196,211,10,238 (c) 117,14,166,217 (c) 10,14,109 (c) 217,160,03,242	Src P 33733 39920 57842 55736 443 47391 65132		10 Jan 10 10 Jan 10 1 Gend		akui Message ETHIO DNS SAU ETHINTING PO ETHINTING PO ETHI	LAST Elsecurity Encry ssible Apache I ssible Apache I ssible Apache I tespreter or C febserver Unar E Win32/Itemc are: Cylance	DAY Start DAY 11:50 	166/26/ Tree 11 11 12 11 13 11 14 11 15 11 15 11 15 11 15 11 15 11	- O LOGOUT
	CMC > View CMC >	A	5 Seve	Sens S bricata-senso = bricata-senso = bricata-senso = bricata-senso = bricata-senso = bricata-senso = bricata-senso = bricata-senso =	ource 39 (0) 192,168,10.8 (0) 195,54,103,149 (0) 195,54,103,149 (0) 195,54,103,149 (0) 195,211,10,238 (0) 117,14,166,217 (0) 10,18,101 (0) 217,160,0242 (0) 10,28,101	: Src P., 33733 39930 57842 55736 443 47891 65189 80		3) Tomoral 1 Desc. 1 33 40 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 40 40 40 40 40 40 40 40 4		akus TEPRIO DAS Sau ET HUNTENG Pe ET HUNTENG PE FUE FUE FUE FUE FUE FUE FUE FUE FUE FU	LAST Elsecurity Encry solide Apache I solide Apache I solide Apache I teopreter or C reference Una E Win32/Item are: Cylance ni32/Vicker Sze	DAY 11-50 DAY 11	06/26/ 20 1 1 0 1	- O LOCOUT
	CMC > View	A	5 Sect	Serra S bricata-senso beicata-senso beicata-senso beicata-senso bricata-senso bricata-senso beicata-senso beicata-senso beicata-senso	ource 3P 0 192,168,10.8 0 195,54,100,149 0 195,54,100,149 0 195,54,100,149 0 195,210,66 0 198,211,10,238 0 198,211,10,238 0 198,211,00,0342 0 10,28,101 0 10,28,101	5rc P., 33733 39320 57542 53736 443 47891 63189 80 43757	Constant (C) C	3) Tomoral 1 Desc. 1 33 40 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 50 40 40 40 40 40 40 40 40 40 4		Message ETHIO DIVS Silu ETHIO DIVS Silu ETHIOTONG Pic ETHIOTONG PIC ETHIOTONG PIC ETHIOTONG PIC ETHIOTONG PIC ETHIOTONG PIC ETHI	LAST Esecurity Encry solide Apache I solide Apache I solide Apache I eteopreter or C riebserver Unas E Win32/Pience are: Cylance n32/Ficker Ste n32/Ficker Ste	DAY 11.54 DAY 11	الم	- O LOCOUT
	CMC > View	A. Arrest Alerts where the alerts where the alerts	5 Seve	Sers S bricata-senso bricata-senso bricata-senso bricata-senso bricata-senso bricata-senso bricata-senso bricata-senso	auree 12 a 19554 108 108 a 19554 108 149 a 19554 108 149 a 19554 108 149 a 19554 108 149 a 19564 108 149 a 19562 108 a 1977 14 106 149 a 1977 14 106 149 a 1977 14 106 149 a 1972 14 109 a 1972 14 100 a 10	5rc P., 33733 39520 57542 55736 443 47891 65189 80 49787 49787	Constants	20 Jan Bonda Dend 33 83 83 83 83 83 83 83 83 83 83 83 83		Message ETPAD Dord Sau ET HUNTING Po ET HUNT	LAST Elecurity Encry solide Apache I solide Apache I solide Apache I solide Apache I teorgreter or Cl Pelsorver Unau E Win32/Picker Ste in32/Picker Ste ible 20mbra Ac	DAY 11.34 DAY 11	En Cél/26/ 20 11 11 11 11 11 11 11 11 11 11	- O LOCOUT
	CMC > View CMC >	A. Arrs Alerts	5 Serte	Sere	auree 12 a 19554 108 108 a 19554 108 149 a 19554 108 149 a 19554 108 149 a 19554 108 149 a 19564 108 149 a 19562 108 a 1977 14 106 149 a 1977 14 106 149 a 1977 14 106 149 a 1972 14 109 a 1972 14 100 a 10	Src P., 33233 39930 57842 55736 443 47891 65189 89 47967 48763 47963	Decisionar (P decisionar (P decisionar (P) decisionar	20 Jan Bonda Dend 33 83 83 83 83 83 83 83 83 83 83 83 83		also Hessage ETHIO DAS Sau ETHIOTONG PR ETHIOTONG PR ETHI	Listi Electrity (Intyre) suble Apache I suble Apach	DAV 2011 DAV 11.50 DAV 11.	Contraction	- O LOCOUT

