IBM QRadar and Endace

Stay ahead of emerging threats with IBM Security and Endace Network History

Cybercriminals are more sophisticated than ever, and attacks on all types of organizations show no signs of slowing down. Endace and IBM Security have joined forces on the IBM Security App Exchange to help security teams combat growing threats using best-in-class solutions.

Combining IBM QRadar with EndaceProbe Analytics Platforms enables analysts to drastically reduce the time required to reconstruct security and network events, understand what's happened and take definitive action. In the QRadar console analysts can go directly from an alert to analyze the related recorded network traffic to see definitive evidence of what has taken place.

What is QRadar?

The IBM® QRadar® Security Intelligence Platform helps security teams accurately detect, understand and prioritize threats that matter most to the business. The solution ingests asset, cloud, network, endpoint, and user data, correlates it against vulnerability information and threat intelligence, and applies advanced analytics to identify and track the most serious threats as they progress through the kill chain.

QRadar allows analysts to:

- Gain comprehensive visibility into on-premises and cloud activity
- Easily view and understand the highest priority potential incidents, versus simply managing individual alerts
- Baseline and analyze asset, network and user activity to identify anomalies that may signal an unknown threat
- Correlate asset, network and user activity against threat intelligence and vulnerability data to identify known threats
- Seamlessly integrate an ecosystem of security solutions to gain greater capabilities from existing solutions
- Leverage artificial intelligence to automate and dramatically accelerate investigation processes
- Report on activities as needed for compliance purposes.



PRODUCTS

IBM QRadar EndaceProbe with Application Dock

BENEFITS

- Analyze network traffic in real-time to detect and predict threats.
- Detect anomalous behavior that may signal an insider threat
- Neutralize threats quickly and efficiently with streamlined investigation workflows.
- Rapid, conclusive and actionable investigations with oneclick drill-down to packet-level detail.
- Easily extend security with QRadar apps from the Security App Exchange
- Deploy new security tools rapidly and on demand with EndaceProbe Application Dock.
- Reduce threat exposure through improved analyst productivity and faster incident investigation.
- Gain a complete, detailed history of network activity to quickly and easily re-trace an attacker's steps

What is the EndaceProbe Analytics Platform?

EndaceProbe[™] Network Analytics Platforms capture, index and store network traffic with 100% accuracy while simultaneously hosting a wide variety of network security and performance monitoring applications in Application Dock[™], EndaceProbe's built-in hosting environment.

Customers can extend their security monitoring capability by deploying security tools on demand, wherever EndaceProbes are deployed. Hosted instances can analyze recorded traffic in real time at full line-rate or analyze recorded Network History for back-in-time investigation.

Accelerating Security Investigations

The Network History recorded by EndaceProbes can be integrated into IBM QRadar using the Pivot-To Vision™ function of the EndaceProbe API. Pivot-To-Vision lets security analysts pivot from threat alerts in IBM QRadar directly to EndaceVision™, the EndaceProbe's built-in investigation tool, to analyze the related, packet-level Network History.

Using the IP address and time range of the trigger event, Pivot-To-Vision focuses the analyst directly on pre-filtered incident data. EndaceVision lets analysts dissect, review and extract the relevant traffic from the terabytes of Network History recorded on the network with ease. Analysts can filter traffic, down to the microsecond level, Application, IP, Protocol, Top Talkers and many other parameters, allowing rapid insights and accurate conclusions.

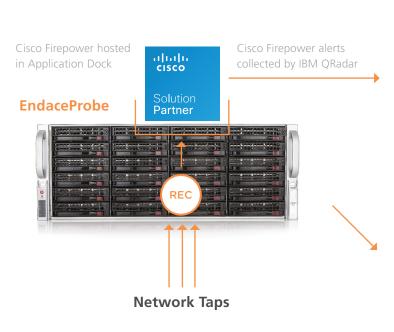
Single-click access to the related packets lets security analysts rapidly establish the root cause of issues, enabling them to act quickly and definitively to resolve critical incidents and to minimize the rest of security threats becoming serious breaches.

Conclusion

Deploying IBM QRadar with EndaceProbe Analytics Platforms allows analysts to extend security monitoring and network recording capability. Pivot-To-Vision allows analysts to drill down into QRadar alerts for the definitive evidence needed to act quickly and decisively.

The combination of Endace and IBM provides state-of-the-art network security management and 100% accurate Network History to give analysts a complete view of what's happening on the network.

Example Configuration with Cisco Firepower and IBM QRadar



IBM QRadar

Dashb	eard Offenses Log Activity Network Activity Assets Reports F	tisks Valnerabilitie	rs Admie				
anch.	• Oxion Seasons • WARD Filter Manue Crimeia E Sava Results @ Coroni *	- False Postive Rules	* Amora *				
					Start Time	1/16/2018	+ 6.18
					Vie	w: Salect An t	· nelto0
							Uning Sear
urree	vt Filters:						Using Gear
	m Rule is BB.DeviceDefinition: IDS / IPS (Clear Filter)						
Cur	rent Statistics						
Total R			120ms				
Jone P	ies Searched 224 (2MB Tetal) Index File Count 83 (86	8 2905 Total Mars Details					
lecor	da Matched Over Time						
2.04							
104							
	6-30 AM 6-45 AM 7-00 AM 7-15 AM	7:30 AM	7.45 AM	0.00 AM	ets am	8.30 AM	8:45 AM
	6-30 AM 6-45 AM 7-00 AM 7-15 AM	7:30 AM	7.45 AM	5 00 AM	8:15 AM	8.10 AM	8:45 AM
	6.30 AM 6.45 AM 7.00 AM 7.15 AM	7:30 AM	7.45 AM	8 00 AM	8:15 AM	8:30 AM	6:45 AM
	6.30 AM 6.45 AM 7.00 AM 7.15 AM	7:30 AM	7.45 AM	8.50 AM	elisam	8.30 AM	E AS AM
			Event Count	0.00 AM	Time 🖛	8.30 AM	
	Event Name	Log Source	Event Count		Time - 2:16:30 PM	8:30 AM	Samb
	Event Name OS-WHDOWS Microsoft Windows SMB remote code exocution attempt	Log Source Claco Firepower	Event Count 3	Jan 16, 2018, 1	Time - 2:16:30 PM 2:16:30 PM	8.30 AM	6amb 6amb
	Event Name OS-WRICOVIS Microsoft Windows SMD emote code execution attempt OS-WRICOVIS Microsoft Windows SMD emote code execution attempt	Log Source Cisco Firepower Cisco Firepower	Event Count	Jan 16, 2018, 1 Jan 16, 2018, 1	Time ▼ 2.16.30 PM 2.16.30 PM 2.16.30 PM	8.30 AM	Gamb Gamb Samb
	Event Name OS WNDOWS Microsoft Microsoft The mode code seeculion alternat OS WNDOWS Microsoft Windows State Immedia code seculion alternat OS WNDOWS Microsoft Windows State Immedia code seculion alternat OS WNDOWS Microsoft Windows State Immedia code seculion alternat Anternated Microsoft Anternative State Immedia code seculion alternative Anternated Microsoft Anternative State Immedia	Log Source Cisco Firepower Cisco Firepower Cisco Firepower	Event Count 3 1 1	Jan 16, 2018, 1 Jan 16, 2018, 1 Jan 16, 2018, 1 Jan 16, 2018, 1 Jan 10, 2018, 1	Time 210.30 PM 210.30 PM 210.30 PM 210.30 PM 210.30 PM	8.30 AM	Gamb Gamb Samb
	Event Name OS VHRGOVE Microsoft White Soft memory code encoders attempt OS VHRGOVE Microsoft Whiteses SMB memory code encoders attempt OS VHRGOVE Microsoft Whiteses SMB memory code encoders attempt OS VHRGOVE Microsoft Whiteses SMB memory code encoders attempt OS VHRGOVE Attracted Whiteses SMB memory code encoders attempt OS VHRGOVE Attracted Whiteses SMB memory code encoders attempt OS VHRGOVE Attracted Whiteses SMB memory code encoders attempt of the Attracted VHRGVE	Log Source Claco Fitepower Claco Fitepower Claco Fitepower Claco Fitepower Claco Fitepower Claco Fitepower	Event Count 3 1 1 1 7	Jan 16, 2018, 1 Jan 16, 2018, 1	Time - 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM	8.30 AM	Gamb Gamb Samb Bamb Bamb Bamb
	Cost NetCOVIS Microsoft Windows SMD smooth code execution alternat OS WHCOVIS Microsoft Windows SMD smooth code alternat Alternative Accession and a Nature Code Code and Alternative Microsoft Code (Code Code Code Code Code Code Code Code	Log Source Cisco Firepower Cisco Firepower Cisco Firepower Cisco Firepower Cisco Firepower Cisco Firepower	Event Count	Jan 16, 2016, 1 Jan 16, 2018, 1	Time 210.30 PM 210.30 PM 210.30 PM 210.30 PM 210.10 PM 210.10 PM 210.10 PM 211.30 PM	8.10 AM	Gamb Gamb Samb Samb Samb Samb Samb Samb
	CO WINCOVS Microsoft Whitewas SMB remarks costs execution attempt CO WINCOVS Microsoft Whitewas SMB remarks costs execution attempt CO WINCOVS Microsoft Whitewas SMB remarks costs execution attempt of WINCOVS MICROSOFT WHITEWAS SMB remarks costs execution attempt of WINCOVS ATTEMPT (WINCOVS COST) Wincovs Costs (WINCOVS COST) WINCOVS COST (WINCOVS COST (WINCOVS COST (WINCOVS COST) WINCOVS COST (WINCOVS COST (WINCOVS COST (WINCOVS COST) WINCOVS COST (WINCOVS	Log Source Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower	Event Count 3 1 1 1 1 7 7 1	Jam 16, 2016, 1 Jam 16, 2018, 1	Time 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.13.30 PM 2.13.30 PM 2.13.30 PM	8.30 AM	Gamb Samb Samb Bamb Rado Rom Troja
	Event Name Sound Don't Mexican With Internet State and the state of the state Sound Don't Mexican With Internet State and the state of the state Sound Don't Mexican With Internet State and the state of the state Sound Don't Mexican With Internet State of the state of the state of the state of the state State of the state of the state State of the state of the state State of the state	Log Source Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower Claco Firepower	Event Count	Jan 16, 2016, 1 Jan 16, 2016, 1 Jan 16, 2018, 1	Time 2.10.30 PM 2.10.26 PM 2.13.26 PM 2.13.26 PM	8.10 AM	Samb Samb Samb Samb Inform Trojar Inform Trojar
	C0 1975/010 Permittente O1 1975/010 Permittente	Log Source Claco Firepower Claco Firepower	Event Count 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Jam 16, 2016, 1 Jam 16, 2018, 1	Time 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.15.36 PM 2.15.36 PM 2.15.36 PM 2.01.36 PM 2.01.	8.30 AM	Camb Samb Samb Hoem Trojar Inform Trojar
	Loss team 0.5 VIPD-015 Mitroson Mittelanens Mittelanen sollen anderen 0.5 VIPD-015 Mitroson Mittelanen Mittelanen sollen anderen 0.5 VIPD-015 Mitroson Mittelanen sollen anderen 0.5 VIPD-015 Mitroson Mittelanen sollen anderen 0.5 VIPD-015 Mitroson Mittelanen sollen anderen Mittelanen s	Log Searce Claco Firepower Claco Firepower	Event Count 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Jam 16, 2016, 1 Jam 16, 2018, 1 Jam 16, 2016, 1 Jam 16, 2016, 1	Time ▼ 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:10 PM 2:10:20 PM 2:10:20 PM 2:00:20 PM 2:00:20 PM 2:00:20 PM	8.30 AM	Gamb Samb Samb Samb Samb Samb Inform Trojar Inform Trojar Inform Trojar
	Constitution On UNDOWN Threads the set of the second sec	Log Source Claco Firepower Claco Firepower	Event Count	Jan 16, 2016, 1 Jan 16, 2018, 1	Time * 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:31 PM 2:10:31 PM 2:00:32 PM 2:00:32 PM 2:00:32 PM 2:00:50 PM	8.30 AM	Gamb Gamb Samb Siamb Intern Trojar Inform Trojar Inform Physio Buffer
	Event team Construction Con	Log Searce Claco Firepower Claco Firepower	Event Count 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Jam 16, 2018, 1 Jam 16, 2018, 1	Time ▼ 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:32 PM 2:13:32 PM 2:00:30 PM 2:00:36 PM 2:00:50 PM	8.30 AM	Gamb Samb Samb Samb Samb Samb Samb Inform Trojae Inform Trojae Inform Trojae Inform Trojae Inform
	Construction C	Log Searce Claco Firepower Claco Firepower	Event Count 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Jam 16, 2018, 1 Jam 16, 2018, 1	Time * 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:31 PM 2:10:31 PM 2:10:31 PM 2:00:30 PM 2:00:30 PM 2:00:30 PM 2:00:50 PM 2:00	8.30 AM	Gamb Gamb Samb Fairin Inform Tropan Tropan Tropan From Fysilo Bather Memo Bather
	Col IntelColIN Structure Team (International Action Structure) Col IntelColIN Structure Team (International Action Structure) Col IntelColIN Structure Team (International Action Structure) ColIN Structure) ColIN Structure	Log Searce Casco Pressover Casco Pressover Casco Pressover Casco Pressover Casco Pressover Casco Pressover Casco Pressover Casco Pressover Casco Prespower Casco Prespower Casco Prespower Casco Prespower Casco Prespower Casco Prespower Casco Prespower Casco Prespower Casco Prespower	Event Count	Jam 16, 2018, 1 Jam 16, 2018, 1	Time ▼ 2-16.30 PM 2-16.30 PM 2-10.30 PM 2-10.30 PM 2-10.30 PM 2-10.31 PM 2-10.31 PM 2-10.30 PM 2-00.36 PM 2-00.56 PM 2-00.56 PM 2-00.56 PM 2-00.56 PM	8.30 AM	Gambo Gambo Sambo Sambo Sambo Samo Friedown Friedown Friedown Friedown Friedown Butther Butther Butther
	Construction C	Log Seerce Claco Fleepower Claco Fleepower	Event Count	Jam 16, 2018, 1 Jam 16, 2018, 1	Time ▼ 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.30 PM 2.16.31 PM 2.15.26 PM 2.15.26 PM 2.05.26 PM 2.05.26 PM 2.05.66 PM 2.05.66 PM 2.05.66 PM 2.05.66 PM	6.10 AM	Gamba Samba Samba Samba Samba Samba Samba Intern Trojan Intern Trojan Intern Trojan Intern Duffer Buffer Buffer Buffer
	Cal structure Cal str	Log Searce Claco Freponet Claco Freponet	Event Count 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Jum 16, 2016, 1 Jum 16, 2016, 1 Jum 16, 2016, 1 Jum 16, 2018, 1	Time ▼ 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:30 PM 2:10:31 PM 2:10:31 PM 2:10:32 PM 2:10:32 PM 2:00:32 PM 2:00:32 PM 2:00:36 PM 2:00:36 PM 2:00:36 PM 2:00:36 PM 2:00:36 PM	8.30 AM	Gambo Gambo Sambo Sambo Sambo Sambo Friedow Inform Trojam Inform Trojam Inform Philio Buffer Buffer Buffer Buffer Buffer Unkno
	Construction C	Log Seerce Claco Fleepower Claco Fleepower	Event Count 1 1 1 1 1 1 1 1 1 1 1 1 1	Jam 16, 2018, 1 Jam 16, 2018, 1	21630 M 21630 M 21630 M 21630 M 21630 M 21630 M 21630 M 21630 M 21630 M 20530 M 200	8.10 AM	Gamb Gamb Samb Samb Samb Samb Hoem Tropan Inform Tropan Inform Philo Buffer Buffer Buffer Buffer

Pivot directly from alerts in Cisco Firepower Console or alerts in IBM QRadar to view related traffic in EndaceVision

EndaceVision



This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission [FCC] Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction document, may cause harmful interference to radio communications.

Endace[™], the Endace logo and DAG[™] are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA). For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com