

# WHAT'S NEW IN NUIX ADAPTIVE SECURITY

### September 2018



# The September 2018 release of Nuix Adaptive Security continues to focus, with laser precision, on solving the questions that keep you up at night:

- How do I amplify the effectiveness of my analysts and incident responders?
- How do I get more from my budget and security infrastructure?
- How do we find more accurately what's important among all the noise?
- How do we respond quickly and effectively to external and internal threats?

#### **RELEASE HIGHLIGHTS**

- Free up endpoint resources. Integration with Windows
  Defender Antivirus means you can remove legacy antivirus
  agents, liberating your endpoint resources and budget.
  From the Nuix Adaptive Security investigator's console you
  can receive Windows Defender alerts, initiate malware scans,
  and review the scan results—at no extra cost.
- Stay FIPS compliant. Organizations and government agencies can now ensure they are meeting the requirements for protecting sensitive information by turning on the FIPS compliance mode, which uses WolfSSL encryption libraries to meet Federal Information Processing Standards 140-2 Level 1 requirements.
- Maximize team effectiveness. The new and improved investigator's console streamlines workflows and reduces the number of steps required to triage alerts, hunt for threats, and respond to incidents. Security analysts and incident responders can spend less time managing the product and more time finding and resolving threats.

666	DASHBOARD	Enterp	rise Security		
-					
	LATEST ALERTS				
0	ld Host Name 28	Timestamp 9/26/2018 3:51:54	Process Name	Logic Engine Rule Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	Description
R	28		powershell.exe	Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule; alert. Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule; alert.	
•		9/26/2018 3:40:12		Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	
0			powershellese	Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule; alert.	
		9/26/2018 3:26:56	powershell.exe	Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	. Rule Alert process \$460 (\Device\HarddiskVolume1\Windows\
¢°.		9/26/2018 3:26:55	powershell.exe	Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	
		9/26/2018 3:20:12	powershell.exe	Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	Rule Alert process 8228 (\Device\HarddiskVolume1\Windows\)
0			powershellexe	Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	Rule Alert process 8228 (\Device\HarddiskVolume1\Windows\)
			powershellexe	Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	Rule Alert process 348 (\Device\HarddiskVolume1\Windows\S)
			powershell.exe	Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	Rule Alert process 348 (\Device\  larddiskVolume1\Windows\Sy
101			powershelLexe	Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	Rule Alert process 4712 (\Device\HarddiskVolume1\Windows\S
				Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	
		9/26/2018 2:40:11		Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert.	
		9/26/2018 2:40:11		Action: Alert Succeeded Status: 0 Rulegroup: SpearPhishAlert Rule: alert	
		0/06/2019 2-19-44	nomerchall ave	Artiner Alart Corraadad Status A Dolanenur CnasrOhichAlart Dolar slart	Dula Alast noncare 2155 A Daniral U soblieblinkona () Windows ()
	ENDPOINT CONNECTIVITY	RISK MON	NITOR		
		Alerts			
	6	ৰ "			
	CONNECTED				
- A					
				Process Endpoint	Logic Rule
•					

Search, filter, and organize single or multiple data sets to effectively triage and respond to an event.

#### **RELEASE HIGHLIGHTS**

- Reduce the time to resolve an incident. New security dashboards proactively display the data and alerts that truly matter. High-value security and system health information such as top alerts and connected or disconnected agents—is automatically collected, analyzed, summarized, and displayed. You can easily prioritize which issues to address first and reduce the time between detecting and resolving the threats that pose the greatest risk to your environment.
- Manage access for greater security and performance. Improved role-based access control provides more flexibility and control when it comes to managing who has access to Nuix Adaptive Security, including what information they can access in the system and what actions they can perform. Role-based access helps maintain the security of your environment, as well as reduce administrative work and IT support. Roles you can assign to users include:
  - Monitor. Read-only dashboard viewing.
  - · Analyst. Access to all events and alert data.
  - **Investigator**. Able to take actions (file download, remediation, isolation) on endpoints.
  - Auditor. Access to system audit logs only.
  - Operator. Able to modify system, agent, and user configuration and management.

#### **ABOUT NUIX ADAPTIVE SECURITY**

Nuix Adaptive Security bucks the endpoint status quo, delivering a proactive approach that provides the visibility, adaptability, and control you've been missing with your traditional endpoint products. By leveraging endpoint analytics, Nuix Adaptive Security can reduce the time it takes to detect an impending or ongoing attack, accelerate recovery time, easily adapt to changing environments, regulations and attack vectors, and ultimately stop incidents in their tracks.

676	ALERTS		My Alerts: 0	Last 24 Hours: 28	Last 7 Days: 28	Total: 28	Unassigned: 28	Assigned: 0	Closed: 0		
							onassigned. Eo	resetted o			
	Alerts (0)										
	Filter		• 6 [1] - po	wershell.exe[4832]	- 9/26/2018 1:0	3:48 AM +0	00:00			00	•
Q	Quick Filter Total										
6			Timestamp:		Proce				Q D N:		
	Date Range: 06/26/2018 03:59 - 09/26/2	018 03:59 👻	9/26/2018 13	03:48 AM +00:00	powe	rshellexe 🛛		V-BOL	lin10		
o?	Assigned:		State:		Paren	Process:		Host M	let Bios Name:		
~~	Select a User		Active, Unass	igned	powe	rshellexe O		JD8-V	/IN10		
$\odot$	Status:		Assigned Use					Host P	let Join Name:		
	Endpoints		Description:								
	All Endpoints Select			cess 4832 (\Device\Hardd	iskVolume1\Windows\Sv	tem32\Window	dowsPowerShelf(v1.0)powershell.exe)				
			Related Even								
	Results: 28 Reset All	By None •	2018-09-26 01:03:48:449 PID 4832 TID 1596 Process: Started (Allowed) \Device\HarddiskVolumeT\Windows\System32\WindowsPowerShell\v1.0\power 0x950005602390328C6884C2FDFCDEF913 (CreateTime 2018-09-26 01:03:48:453 ExitTime 1601-01-01 00:00:00.000) Parent \Device\HarddiskVolumeT\								D5 pstem3
	9/26/2018 1:03:48 AM JD8-Win10		\svchost.exe								
	Active, Unassigned		Filter Rule:								
	A process previously marked as tain Rule Alert process 4832 (\Device\H		Action: Alert Succeeded Status: 0 Rulegroup: Spear/PlishAlert Rule: alert when ( CommonDels : tainted -= TRUE ) && ( CommonDels : g.shells contains lower ( getbasena ( process path ) ) ) = Comment:								
	9/26/2018 1:03:49 AM JDB-Win10		A process pr	eviously marked as tainted	is attempting to spawn i	shell program					
	Active, Unassigned A process previously marked as tain Rule Alert process 4832 ((Device)/H.										
	9/26/2018 1:21:54 AM JDB-Win10										
4	Active, Unassigned A process previously marked as tain Rule Alert process 3264 (\Device\H	vted is attemp arddiskVolum									
0	9/26/2018 1:21:55 AM										

Prioritize which issues to address first by seeing the alerts that truly matter.

# Schedule a demo today. www.nuix.com/demo

**Snuix** 

Nuix (<u>www.nuix.com, ASX:NXL</u>) creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world. We are a passionate and talented team, delighting our customers with software that transforms data into actionable intelligence and helps them overcome the challenges of litigation, investigation, governance, risk and compliance.

**APAC** Australia: +61 2 8320 9444 **EMEA** UK: +44 203 934 1600 **NORTH AMERICA** USA: +1 877 470 6849

Nuix (and any other Nuix trademarks used) are trademarks of Nuix Ltd. and/or its subsidiaries, as applicable. All other brand and product names are trademarks of their respective holders. Any use of Nuix trademarks requires prior written approval from the Nuix Legal Department. The Nuix Legal Department can be reached by e-mail at Legal@nuix.com.

THIS MATERIAL IS COMPRISED OF INTELLECTUAL PROPERTY OWNED BY NUIX LTD. AND ITS SUBSIDIARIES ("NUIX"), INCLUDING COPYRIGHTABLE SUBJECT MATTER THAT HAS BEEN NOTICED AS SUCH AND/OR REGISTERED WITH THE UNITED STATES COPYRIGHT OFFICE. ANY REPRODUCTION, DISTRIBUTION, TRANSMISSION, ADAPTATION, PUBLIC DISPLAY OR PUBLIC PERFORMANCE OF THE INTELLECTUAL PROPERTY (OTHER THAN FOR PREAPPROVED INTERNAL PURPOSES) REQUIRES PRIOR WRITTEN APPROVAL FROM NUIX.