# **Sophos** Intercept X Advanced w/ EDR

Yannick Escudero Snr. Sales Engineer

20.09.2018



## **Organizations Struggle with Endpoint Detection & Response**



## **VISIBILITY & DETECTION**

Blind spots make it difficult to understand what is happening



## **ANALYSIS & INVESTIGATION**

Teams suffer from a lack of data or are overwhelmed by data



Need more talent and hours in the day to respond to incidents

## **Typical Endpoint Detection & Response Tools Also Struggle**



EDR can be overwhelming, rely heavily on expert security analysts



Focused on manual workflows instead of proactive protection and automated response



**RESOURCE INTENSIVE** 

Expensive, time consuming, require dedicated staff

## **Sophos Intercept X: EDR for All**



 Intuitive to use, easy to understand Add visibility, analysis, and response capabilities without adding staff

## More signals, less noise

Automatic incident detection and prioritization, guided investigations, curated threat intelligence

## Rapid Response

Respond to incidents with the click of a button

# How Sophos EDR Can Make You More Secure



## Answering those tough questions with Intercept X

- Am I under attack? Is there something we are missing? How can I be sure?
- How should I respond to this incident? What should I do next?
- What incidents should I be prioritizing?
- What is this file? Is it malicious? Is it a false positive?
- Does this threat exist anywhere in my network?
- Has the attack spread?



# Intercept X w/ EDR: Detect

<ul> <li>Endpoint Protection</li> <li>Back to Overview</li> </ul>	Most Recent Threat	Cases					See
ANALYZE	Sophos generated	Admin generate	ed				
Dashboard	CREATED ON -	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
Logs & Reports	Apr 18, 2016 12.23PM	High	Malware detected	Mal/ML-PE	Blocked and cleaned	William Morris	WMorrisPC
	Apr 17, 2016 12.23PM	Medium	Exploit	Exploit Lockdown	Cleaned up	Brian Jones	BrianJComp
DETECTION AND REMEDIATION	Apr 16, 2016 12.23PM	Low	Malicious traffic	Tro/PDFJs-AIA	Blocked	Brian Jones	BrianLaptop
A Threat Cases	Apr 15, 2016 12.23PM	High	Ransomware	Exploit Cryptoguard	Running	Eryn Havers	ErynMac
	Apr 14, 2016 12.23PM	High	PUA	Troj/Loic-A	Clean up needed	Gina Baker	Gina Comp
Q Threat Searches	Top Suspicious Ev	ents		See all events	Threat Search		
Suspicious Events		DETECTED ON		NDPOINTS AFFECTED			
MANAGE	Dropper.exe	July 31, 2018 09:01 AM			Search for potential threats on Enter one or more SHA 256 fil		5,
	Giopperexe	5diy 01, 2010 05.01 Am					17.
Le People					192.151.42.1, Beef_Wellington	n.exe, c84c361b7f5dba	eac93828e60d2
Computers	Machir	ne learning	idantifia	a tan			
			luentine		Searches on hashes or file names v uncertain reputation.	will return portable executab	le files with
CONFIGURE					uncertain reputation.		
	suspici	ous events	to invest	rigate		ABC Co	Marcus Jones
	OVe		to invest	igate		ABC CO	Marcus Jones
	Suspicio Most Recent Threat C		to invest	igate		ABC CO	Marcus Jones rp - Primay Admin
SOPHOS CHARTER Admin	OVe			igate		ABC Co	Marcus Jones
SOPHOS CENTER Admin © Endpoint Protection Content of Overview	Most Recent Threat	Cases		igate	CONDITION	ABC Co	Marcus Jones rp - Primay Admin
Contraction Contr	Most Recent Threat C	Cases Admin generate PRIORITY Hign	ed TYPE Malware detected	NAME Mal/ML-PE	Blocked and cleaned		Marcus Jones rp - Primay Admin Sec
SOPHOS CENTER Admin © Endpoint Protection CERCE to Overview ANALYZE	Most Recent Threat ( Sophos generated CREATED ON • Apr 18, 2016 12.23PM Apr 17, 2016 12.23PM	Cases Admin generate PRIORITY High Medium	ad TYPE Malware detected Exploit	NAME Mal/ML-PE Exploit Lockdown	Blocked and cleaned Cleaned up	USER	Marcus Jones rp - Primay Admin Sec DEVICE WMorrisPC
Contraction Contr	Most Recent Threat of Sophos generated CREATED ON ♥ Apr 18, 2016 12.23PM Apr 16, 2016 12.23PM Apr 16, 2016 12.23PM	Cases Admin generate PRIORITY High Medium Low	ad TYPE Malware detected Exploit Mallicious traffic	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA	Blocked and cleaned Cleaned up Blocked	USER William Morris	Marcus Jones rp - Primay Admin Sec
Constant     Admin      Constant     Admin      Constant     Cons	Most Recent Threat of Sophos generated CREATED ON • Apr 18, 2016 12.23PM Apr 16, 2016 12.23PM Apr 16, 2016 12.23PM Apr 15, 2016 12.23PM	Cases Admin generate PRIORITY High Medium Low High	ed TYPE Matware detected Exploit Maticious traffic Ransomware	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard	Blocked and cleaned Cleaned up Blocked Running	USER William Morris Brian Jones Brian Jones Eryn Havers	Marcus Jones rp - Primay Admin Sec DEVICE WMorrisPC BrianJComp BrianLaptop ErynMac
Endpoint Protection     Back to Overview  ANALYZE      Dashboard      Logs & Reports  Detection AND REMEDIATION      Threat Cases	Most Recent Threat of Sophos generated CREATED ON ♥ Apr 18, 2016 12.23PM Apr 16, 2016 12.23PM Apr 16, 2016 12.23PM	Cases Admin generate PRIORITY High Medium Low	ad TYPE Malware detected Exploit Mallicious traffic	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA	Blocked and cleaned Cleaned up Blocked	USER William Morris Brian Jones Brian Jones	Marcus Jones rp - Primay Admin Sec DEVICE WMorrisPC BrianJComp BrianLaptop
Constant     Admin      Constant     Admin      Constant     Cons	Most Recent Thread C Sophos generated CREATED ON • Apr 18, 2016 12.23PM Apr 16, 2016 12.23PM Apr 15, 2016 12.23PM Apr 15, 2016 12.23PM Apr 14, 2016 12.23PM	Cases Admin generate PRIORITY Hign Medium Low Hign High	ed TYPE Matware detected Exploit Maticious traffic Ransomware	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Troj/Loic-A	Biocked and cleaned Cleaned up Biocked Running Clean up needed	USER William Morris Brian Jones Brian Jones Eryn Havers	Marcus Jones rp - Primay Admin Sec DEVICE WMorrisPC BrianJComp BrianLaptop ErynMac
Endpoint Protection     Back to Overview  ANALYZE      Dashboard      Logs & Reports  Detection AND REMEDIATION      Threat Cases	Most Recent Thread C Sophos generated CREATED ON • Apr 18, 2016 12.23PM Apr 16, 2016 12.23PM Apr 15, 2016 12.23PM Apr 14, 2016 12.23PM Apr 14, 2016 12.23PM	Cases Admin generate PRIORITY Hign Medium Low Hign High High ents	ad TYPE Malware detected Exploit Malicious traffic Ransomware PUA	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Tro/Loic-A See all events	Biocked and cleaned Cleaned up Biocked Running Clean up needed Threat Search	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker	Marcus Jones rp - Primay Admin Sec DEVICE WMorrisPC BrianJComp BrianLaptop ErynMac
Endpoint Protection	Most Recent Threat of Sophos generated CREATED ON ▼ Apr 18, 2016 12.23PM Apr 16, 2016 12.23PM Apr 16, 2016 12.23PM Apr 14, 2016 12.23PM Top Suspicious Eve NAME	Cases Admin generate PRIORITY High Medium Low High High ents DETECTED ON	TYPE Malware detected Exploit Malicious traffic Ransomware PUA	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Tro/Loic-A See all events NDPOINTS AFFECTED	Biocked and cleaned Cleaned up Biocked Running Clean up needed	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker	Marcus Jones rp - Primay Admin Sec DEVICE WMorrisPC BrianJComp BrianLaptop ErynMac Gina Comp
	Most Recent Threat of Sophos generated CREATED ON ● Apr 18, 2016 12.23PM Apr 16, 2016 12.23PM Apr 17, 2016 12.23PM Apr 15, 2016 12.23PM Apr 14, 2016 12.23PM Top Suspicious Evo NAME Dropper.exe	Cases Admin generate PRIORITY High Medium Low High High High Ents DETECTED ON July 31, 2018 09:01 AM	ad TYPE Malware detected Exploit Malicious traffic Reinsomware PUA THREAT SCORE E 31 1	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Tro/Loic-A See all events NDPOINTS AFFECTED 2	Biocked and cleaned Cleaned up Biocked Running Clean up needed Threat Search Search for potential threats on	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker	Marcus Jones rp - Primay Admin Sec DEVICE WMorrisPC BrianJComp BrianLaptop ErynMac Gina Comp
	Most Recent Threat ( Sophos generated CREATED ON ♥ Apr 18, 2016 12.23PM Apr 15, 2016 12.23PM Apr 15, 2016 12.23PM Apr 15, 2016 12.23PM Apr 14, 2016 12.23PM Dropsciences	Cases Admin generate PRIORITY High Medium Low High High Bettected on July 31, 2018 09:01 AM July 29, 2018 12:04 PM	TYPE Malware detected Exploit Malicious traffic Ransomware PUA THREAT SCORE E 31 1 1	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Tro/Loic-A See all events NDPOINTS AFFECTED 2	Biocked and cleaned Cleaned up Biocked Running Clean up needed Threat Search Search for potential threats on	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker	Marcus Jones rp - Primay Admin See DEVICE WMorrisPC BrianJComp BrianJComp ErynMac Gina Comp
	Most Recent Threat of Sophos generated CREATED ON ▼ Apr 18, 2016 12.23PM Apr 15, 2016 12.23PM Apr 15, 2016 12.23PM Apr 15, 2016 12.23PM Apr 14, 2016 12.23PM Dropper exe Quiver exe DancingCats.exe	Cases Admin generate PRIORITY High Medium Low High High High DETECTED ON July 31, 2018 09:01 AM July 29, 2018 12:04 PM July 20, 2018 10:57 AM	ed TVPE Malware detected Exploit Malicolus traffic Ransomware PUA THREAT SCORE E 31 1 25 3 29 2	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Troj/Loic-A See all events NDPOINTS AFFECTED 2	Biocked and cleaned Cleaned up Biocked Running Clean up needed Threat Search Search for potential threats on Enter one or more SHA 256 fil	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker	Marcus Jones rp - Primay Admin Se DEVICE WMorrisPC BrianJComp BrianLaptop ErynMac Gina Comp
Computers	Most Recent Threat ( Sophos generated CREATED ON ♥ Apr 18, 2016 12.23PM Apr 17, 2016 12.23PM Apr 16, 2016 12.23PM Apr 15, 2016 12.23PM Apr 15, 2016 12.23PM Drop Suspicious Ev NAME Drop Per exe Quiver exe DancingCats.exe Tweetbot, exe	Cases Admin generate PRIORITY High Medium Low High High DETECTED ON July 31, 2018 09:01 AM July 20, 2018 10:57 AM July 04, 2018 09:07 AM	ad TYPE Malware detected Exploit Malicious traffic Ransomware PUA THREAT SCORE E 31 1 25 23 22 4	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Troj/Loic-A See all events NDPOINTS AFFECTED 2 3 5	Biocked and cleaned Cleaned up Biocked Running Clean up needed Threat Search Search for potential threats on Enter one or more SHA 256 fil	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker a your network les hashes or file names n.exe, c84c361b7f5dbac	Marcus Jones rp - Primay Admin Se DEVICE WMorrisPC BrianLaptor ErynMac Gina Comp S, eac93828e60d2
	Most Recent Threat of Sophos generated CREATED ON ● Apr 15, 2016 12, 23PM Apr 16, 2016 12, 23PM Apr 16, 2016 12, 23PM Apr 16, 2016 12, 23PM Apr 16, 2016 12, 23PM Dopper exe Guiver exe Dancing Cats, exe TweetDot exe Adware, WPSOffice	Cases Admin generate PRIORITY High Medium Low High High High DETECTED ON July 31, 2018 09:01 AM July 29, 2018 12:04 PM July 20, 2018 10:57 AM	TYPE Malware detected Exploit Malicious traffic Ransomware PUA THREAT SCORE 8 31 25 22 22 4 19 5	NAME Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Tro/Loic-A See all events NDPOINTS AFFECTED 2 3 5 4	Biocked and cleaned Cleaned up Biocked Running Clean up needed Threat Search Search for potential threats on Enter one or more SHA 256 fil 192.151.42.1, Beef_Wellington Searches on hashes or file names v	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker a your network les hashes or file names n.exe, c84c361b7f5dbac	Marcus Jones rp - Primay Admin Sec DEVICE WMerrisPC BrianLaptop ErianLaptop ErianLaptop ErianLaptop Si,

# Intercept X w/ EDR: Detect

Endpoint Protection Back to Overview	Most Recent Threat	Cases					S
ANALYZE	Sophos generated	Admin generate	ed				
Dashboard	CREATED ON -	PRIORITY	TYPE	NAME	CONDITION	USER	DEVICE
E Logs & Reports	Apr 18, 2016 12.23PM	High	Malware detected	Mal/ML-PE	Blocked and cleaned	William Morris	WMorrisPC
E Lugs & Repuits	Apr 17, 2016 12.23PM	Medium	Exploit	Exploit Lockdown	Cleaned up	Brian Jones	BrianJCon
DETECTION AND REMEDIATION	Apr 16, 2016 12.23PM	Low	Malicious traffic	Tro/PDFJs-AIA	Blocked	Brian Jones	BrianLapte
A Threat Cases	Apr 15, 2016 12.23PM	High	Ransomware	Exploit Cryptoguard	Running	Eryn Havers	ErynMac
a Inreat Cases	Apr 14, 2016 12.23PM	High	PUA	Troj/Loic-A	Clean up needed	Gina Baker	Gina Com
Q Threat Searches							
Suspicious Events	Top Suspicious Ev	ents		See all events Th	hreat Search		
	NAME	DETECTED ON	THREAT SCORE E	ENDPOINTS AFFECTED			
MANAGE	Dropper.exe	July 31, 2018 09:01 AM	31 1	12.			
Le People	Quiver.exe	July 29, 2018 12:04 PM	<b>25</b> 3	3			
	DancingCats.exe	July 20, 2018 10:57 AM	23 2	23	Easily searc	ch by IP add	ress.
Computers	Tweetbot.exe	July 04, 2018 09:07 AM	22 4	16			
CONFIGURE	Adware.WPSOffice	July 03, 2018 5:37 PM	19 5	54	file nam	ne, hash, et	C
	Packed.Generic.533	June 28, 2018 2:19 PM	17 1	n (		ie, nasn, eu	<b>U</b> •
	Dashboard Overview / Endpoint Pro	otection Dashboard				ABC Co	
SOPHOS CENTRAL Admin	Overview / Endpoint Pro					ABC Co	rp - Primay Admi
SOPHOS CENTRAL Admin Sendpoint Protection Central Admin	Overview / Endpoint Pro	Cases	rd			ABC Cor	rp - Primay Admi
© Endpoint Protection Back to Overview	Overview / Endpoint Pro	Cases Admin generate		NAME			rp - Primay Admi
SOPHOS Admin Converse Admin Conversion	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON V	Cases Admin generate PRIORITY	type Malware detected	NAME Mal/ML-PE	CONDITION Blocked and cleaned	USER	rp - Primay Admi S
CONTRACT       CONTRACT       CONTRACT      CONTRACT      CONTRACT	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ▼ Apr 18, 2016 12:23PM	Cases Admin generate	TYPE	La construction de la constructi	CONDITION Blocked and cleaned Cleaned up	USER William Morris	p - Primay Admi S DEVICE WMorrisPC
Constant Admin      Constant Admin      Constant Admin      Constant Admin      Constant Admin      Constant Admin      Logs & Reports	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON V	Cases Admin generate PRIORITY High	TYPE Malware detected	Mal/ML-PE	Blocked and cleaned	USER William Morris Brian Jones	rp - Primay Admi S DEVICE WMorrisPC BrianJCor
Contract Admin  Contract Contraction  Contract	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ♥ Apr 18, 2016 12:23PM Apr 17, 2016 12:23PM	Admin generate PRIORITY High Medium	TYPE Malware detected Exploit	Mai/ML-PE Exploit Lockdown	Blocked and cleaned Cleaned up	USER William Morris Brian Jones Brian Jones	rp - Primay Adm S DEVICE WMorrisPi BrianJCoi
CONTRACT       CONTRACT       CONTRACT      CONTRACT      CONTRACT	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ♥ Apr 18, 2016 12:23PM Apr 17, 2016 12:23PM	Cases Admin generate PRIORITY Hign Medium Low	TYPE Malware detected Exploit Malicious traffic	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA	Blocked and cleaned Cleaned up Blocked	USER William Morris Brian Jones	rp - Primay Admi S DEVICE WMorrisPC BrianLapt ErynMac
	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ♥ Apr 18, 2016 12:23PM Apr 17, 2016 12:23PM Apr 15, 2016 12:23PM	Cases Admin generate PRIORITY High Medium Low High	TYPE Malware detected Exploit Maliclous traffic Ransomware	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard	Blocked and cleaned Cleaned up Blocked Running	USER William Morris Brian Jones Brian Jones Eryn Havers	rp - Primay Admi S DEVICE WMorrisPC BrianLapt ErynMac
Contract Admin  Contract	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ♥ Apr 18, 2016 12:23PM Apr 17, 2016 12:23PM Apr 15, 2016 12:23PM	Admin generate PRIORITY Hign Medium Low Hign Hign	TYPE Malware detected Exploit Maliclous traffic Ransomware	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Troj/Loic-A	Blocked and cleaned Cleaned up Blocked Running	USER William Morris Brian Jones Brian Jones Eryn Havers	DEVICE WMorrisPC BrianLapt ErynMac
	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ♥ Apr 18, 2016 12:23PM Apr 16, 2016 12:23PM Apr 15, 2016 12:23PM Apr 14, 2016 12:23PM	Admin generate PRIORITY Hign Medium Low Hign Hign	TYPE Malware detected Exploit Malicious traffic Ransomware PUA	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Troj/Loic-A See all events	Blocked and cleaned Cleaned up Blocked Running Clean up needed	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker	WMorrisPC BrianJCom BrianLapto
	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ▼ Apr 18, 2016 12:23PM Apr 16, 2016 12:23PM Apr 15, 2016 12:23PM Apr 14, 2016 12:23PM Top Suspicious Ev	Cases Admin generate PRIORITY Hign Medium Low Hign Hign Hign ents	TYPE Malware detected Exploit Malicious traffic Ransomware PUA THREAT SCORE E	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Troj/Loic-A See all events TI See all events AFFECTED	Blocked and cleaned Cleaned up Blocked Running Clean up needed	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker your network	DEVICE WMorrisPC BrianLapt ErynMac Gina Com
	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ♥ Apr 18, 2016 12.23PM Apr 15, 2016 12.23PM Apr 15, 2016 12.23PM Apr 14, 2016 12.23PM Top Suspicious Ev NAME	Cases Admin generate PRIORITY Hign Medium Low High High High High Ents DETECTED ON	TYPE Malware detected Exploit Malicious traffic Ransomware PUA THREAT SCORE E 31 1	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Troj/Loic-A See all events TI ENDPOINTS AFFECTED 12	Blocked and cleaned Cleaned up Blocked Running Clean up needed nreat Search Search for potential threats on	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker your network	DEVICE WMorrisPC BrianLapt ErynMac Gina Com
	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ♥ Apr 18, 2016 12:23PM Apr 17, 2016 12:23PM Apr 15, 2016 12:23PM Apr 14, 2016 12:23PM Drop Suspicious Ev NAME Dropper.exe	Cases Admin generate PRIORITY Hign Medium Low Hign High Cents DETECTED ON July 31, 2018 09:01 AM	TYPE Malware detected Exploit Malicious traffic Ransomware PUA THREAT SCORE E 31 1 26 3	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Troj/Loic-A See all events TI ENDPOINTS AFFECTED 12	Blocked and cleaned Cleaned up Blocked Running Clean up needed nreat Search Search for potential threats on	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker your network es hashes or file names	p - Primay Admi S DEVICE WMorrisPC BrianJCon BrianLapt ErynMac Gina Com
	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ▼ Apr 15, 2016 12.23PM Apr 17, 2016 12.23PM Apr 15, 2016 12.23PM Apr 15, 2016 12.23PM Drop Suspicious Ev NAME Dropper.exe Quiver.exe	Cases Admin generate PRIORITY Hign Medium Low Hign Hign High DETECTED ON July 31, 2018 09:01 AM July 29, 2018 12:04 PM	TYPE Maiware detected Exploit Malicious traffic Ransomware PUA THREAT SCORE E 31 26 3 20 2	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Tro/Loic-A See all events TH ENDPOINTS AFFECTED 12 3 3 3 3 5 6	Blocked and cleaned Cleaned up Blocked Running Clean up needed nreat Search Search for potential threats on Enter one or more SHA 256 fil 192.151.42.1, Beef_Wellingtor	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker your network es hashes or file names n.exe, c84c361b7f5dbac	DEVICE UDEVICE WMorrsPC BrianLapto BrianLapto ErynMac Gina Com
Computers  Computer  Com	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ▼ Apr 18, 2016 12.23PM Apr 16, 2016 12.23PM Apr 16, 2016 12.23PM Apr 16, 2016 12.23PM Drop Suspicious Ev NAME Dropper exe Guiver.exe DancingCats.exe	Admin generate PRIORITY High Low High High dents DETECTED ON July 31, 2018 09:01 AM July 29, 2018 12:04 PM July 20, 2018 10:57 AM	TYPE Malware detected Exploit Maliclous traffic Ransomware PUA THREAT SCORE E 31 1 26 23 22 4	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguard Tro/Loic-A See all events TH ENDPOINTS AFFECTED 12 3 3 3 3 5 6	Blocked and cleaned Cleaned up Blocked Running Clean up needed nreat Search Search for potential threats on Enter one or more SHA 256 fil	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker your network es hashes or file names n.exe, c84c361b7f5dbac	p - Primay Admin Si DEVICE WMorrisPC BrianLapto BrianLapto ErynMac Gina Com
Endpoint Protection     Admin      Endpoint Protection     Back to Overview  ANALYZE      Dashboard     Logs & Reports      Logs & Reports      Fireat Cases     Threat Searches      Suspicious Events  ANALKE	Overview / Endpoint Pro Most Recent Threat Sophos generated CREATED ON ▼ Apr 18, 2016 12:23PM Apr 16, 2016 12:23PM Apr 16, 2016 12:23PM Apr 15, 2016 12:23PM Apr 16, 2016 12:23PM Construction Drop Suspicious Ev NAME Dropper.exe Quiver.exe DancingCats.exe Tweetbot.exe	Admin generate PRIORITY High Low High High dents DETECTED ON July 31, 2018 09:01 AM July 29, 2018 12:04 PM July 20, 2018 10:57 AM	TYPE Malware detected Exploit Malicious traffic Ransomware PUA THREAT SCORE E 31 26 33 23 23 22 4 19 5	Mal/ML-PE Exploit Lockdown Tro/PDFJs-AIA Exploit Cryptoguaro Troj/Loic-A See all events I ENDPOINTS AFFECTED 2 3 3 3 45	Blocked and cleaned Cleaned up Blocked Running Clean up needed nreat Search Search for potential threats on Enter one or more SHA 256 fil 192.151.42.1, Beef_Wellingtor Searches on hashes or file names y	USER William Morris Brian Jones Brian Jones Eryn Havers Gina Baker your network es hashes or file names n.exe, c84c361b7f5dbac	p - Primay Admi S DEVICE WMorrisPC BrianLapti ErynMac Gina Com S, eac93828e60c





Search for item

Clean and block

## Intercept X w/ EDR: Investigate with SophosLabs Threat Intelligence

>	Search for item Clean and block	>			Search for item	Clean and block	>	Search for item Clean and block
Process deta	What does this do? ails: dropper.exe	Process details	: dropper.exe			What does this do?	Process details: dropper.exe	What does this do?
Reputation at time	e case was created Uncertain	Process details	Report summary	Machine learning	File properties	File breakdown	Process details Report Summary Alachine le	File propercies File preakdown
a construction of the second second	Known good Not detected at time case was created gate this item to determine whether it is harmful.	SOPHOS LABS TH		analysis Current report crea	ted: Jun 06 2018 12	45pm	SOPHOS LABS Threat Intelligence Current report	t created: Jun 06 2018 12.45pm wn good and 61 million know bad items analysed
	5 Threat Intelligence	Giobal Reputation	- Teport automotiv				Attribute of Dropper.exe Seen in: Known ba	d files Known good files
Request latest	intelligence	Known bad				Known good	Unknown packs     In Million     Tiny code section     2.1 Million	205 K 1.0 Million 980K
Note: Requesting SophosLabs for an	the latest intelligence will submit a copy of the file to alysis	Prevalence First seen	Low. 📵 mon dd, yyyy tEttPM				No icon     Uses encryption	2K
Path: Process ID:	c:\program files\temp\dropper.exe 9999	Last seen AV detection	mon dd, yyyy tt:ttPM Malware (high confid	ence) 15 anti-malware	products detect this fil Go to VirusTota		Code similarity <b>()</b> 82% suspicious Over 52 million	n known good and 61 million know bad items analysed
SHA256:	2cf24dba5fb0a30e26e83b2ac5b9e29e1b161 e5c1fa7425e73043362938b9824 Copy	Machine learning analysis	Attributes: Genetic similarity:	87% suspicious			Compensate     C	99% 96%
Start time: End time:	Apr 01, 2016 12:20PM Still running when threat case created on April 12, 2016 12:23PM		File path:	61% suspicious			loquake3.x86_64.exe	95%
Duration: Actions done to this artifact:	11 days None						V1ConsionLinet ava	85%
Actions performed by this artifact:	d 1 executable file written 1 program run	• Acce	ss latest	threat ir	ntelligen	ce from S	ophosLabs	82%
			reat rese ore mach		-	•	is files	

#### × Clean and block You're about to clean up this item on any computer where we've found it and block it on all your computers. Respond to incidents with a click of a button Why are you blocking this item? Full disclosure of potential threat activity • Clean and remove this suspicious file and black list it Isolate machine(s) • Note: You can see the items you've blocked or unblock them again in your Blocked Items list. Clean file, blacklist or whitelist • Investigate further, create forensic snapshots • Jones -Cancel Confirm y Admin C Endpoint Pro Create forensic snapshot () Suggested next steps ANALY75 Actions SHA256 Hash 🔻 Name W Reputation **T** Туре 🐺 Cleaned T Path Dashboard · Set status and priority for the case New High ۳ e92e02dtt752778c13c1d78 Installer.exe Actions Uncertain Process c:\program files\a path name No E Logs & Reports 8ac0781a335b86fc0f4158b · Investigate 1 process we've marked with an "uncertain" reputation. See graph Actions be8f9810623a390c12 below for details Clean and b Generate threat case Isolate the computer while you investigate. Request threat intelligence report DETECTION AND REMEDIATION 2bf24dba5fb0a30e26e83b2a Updater.exe c:\program files\a path name No c5b9e29e1b161e5c1fa7425 Uncertain Process Scan the computer e73043362938b9824 A Threat Cases c:\program files\a second path name Actions ۲ Q Threat Searches Actions ۳ c:\program files\a third path name Actions ۳ Suspicious Events c:\program files\a fourthpath name 3cf24dba5fb0a30e26eB3b2a Keylogger.exe Process Bart Malware NO c:\program files\a path name which Actions . MANAGE c5b9e29e1b161e5c1fa7425 is long and will wrap in the table row e73043362938b9824 A People Computers SOPHOS

## Intercept X w/ EDR: Respond





## Benefits

- Get started quickly
  - Built on Intercept X the industry's #1 endpoint protection
  - Endpoint protection and EDR in a single solution
  - Part of Sophos Central
- Add visibility, context, and investigation capabilities without adding staff
  - Increase endpoint defenses, remove blind spots
  - Guided investigations
  - Machine learning prioritizes incidents, analyzes files, provides suggestions
  - SophosLabs threat intelligence on-demand
  - Make more informed decisions in less time
- Respond to incidents with a single click
- Prove compliance posture with increased ease

PROUL	ста 🗸 solutions 🗸 ритская зароат сонуму 🖬 ۹ ք
Start your trial today.	This information will be sent to Test Cloud Partner Dashboard Access a trusted Sophos Partner
Your 30-day, free trial includes	First Name *
Endpoint Protection	
Secure Web Gateway	Last Name *
Mobile Control	Business Email*
Server Protection	
Secure Wi-Fi	Next
Device Encryption	
Secure Email Gateway	By subent thing this form you can serve to be contacted allow. Sophies products and services from manifester of the Sophies group of contacted and services companies afraction test or write units serviced as products and services. Spring of committee to safeguarding out an vacy if you want more international more efficiency.
S Intercept X	committed to safeguating your privace if you want to be

# Coming Soon: Join the Early Access Program

Free to trial

Access via Central

**Demo from Live Webcast** 

# See here: https://vimeo.com/284228948/24498738a8

Sophos Confidential 15

