



# Getting Started Guide: Devo Security Operations

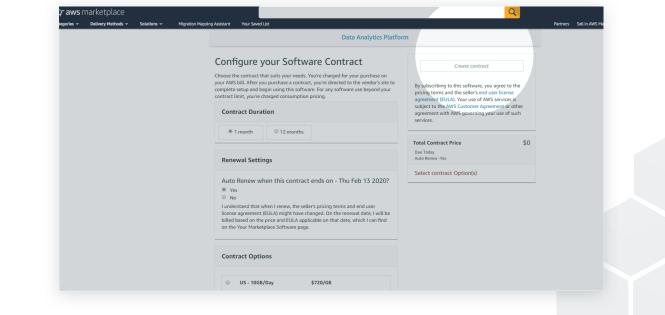
**Devo Security Operations** helps you detect, enrich, and analyze threats, and react with playbook-driven response. It also helps you shorten investigation times and increase the efficacy of decision-making by automating key tasks in the analyst review cycle. Devo Security Operations offers a single platform for triage, investigation, collaboration, and incident documentation that reduces churn.

#### **PART 1: Subscribing to Devo Security Operations**

Data Analytics Platform       Contract of additional of the base of the work of the most instrumented entraprise, provide of the source of the analytics Platform across the instrumented entraprise, provide of the work one. The Deco Data Analytics Platform collects, enhances and analytes machine data, at sole. For an across the entraprise, provide of the work one. The Deco Data Analytics Platform collects, enhances and analytes machine data.       Contract of the view         Woundeds the full walke of machine data of the work of most instrumented entraprise, provide work one. The Deco Data Analytics Platform collects, enhances and analyzes machine, business and operational data, at sole, form across the entraprise, provide work one. The Deco Data Analytics Platform collects, enhances and analyzes machine, business and operational data, at sole, form across the entraprise, provide work of the work of most instrumented entraprise, provide work one. The Deco Data Analytics Platform collects, enhances and analyzes machine, business and operational data, at sole, form across the entraprise to the stere of the work of the work of the work of the work of the entraprise best of the work of the work of the entraprise of the stere of the work of the entraprise of the stere of the work of the entraprise of the entraprise of the stere of the work of the entraprise of the work of the entraprise of the e	Sold by: Devel       Save to list         Save to list       Save to list <tr< th=""><th>👾 aws marketplace Categories 👻 Delivery Methods 👻 Solutions 👻</th><th>Migration Mapping Assistant Your</th><th>Saved List</th><th></th><th></th><th>Q</th></tr<>	👾 aws marketplace Categories 👻 Delivery Methods 👻 Solutions 👻	Migration Mapping Assistant Your	Saved List			Q
Product Overview         Devo unlocks the full value of maching for the world's most instrumented enterprise, period in unsplots for it, scenario, and objensions stand scenario scenari scenario scen	Product Overview         Brew undexks the full value of makine data for the world's most instrumented enterprises, and analyzes machine, business and operational data, at scale, from accoss the enterprise. Body scale read-time insights for machine data for the world's most instrumented enterprise. Body scale read-time insights for most scale the enterprise. Body scale read-time insights for most scale the machine data for the world's most streaming and historical machine data.       Handles terabytes of ingest volume while analyzing periods the machine data.         Sold by       Devoid       Sold by       Devoid         Product Video       See product video C       No-compromise architecture: delivers both scale and speed at lower costs         Dricing Information       Devoid Sold by       No-compromise architecture: delivers both scale and speed at lower costs		÷ DEVO	Sold by: Devo SaaS Data Analytics Platform to collect,			
Highlights Here unlocks the full value of machine data for the world's most instrumented enterprises, putting more data to work now. The Devo Data Analytics Platform collects, enhances and analyses machine, business and operational data, at scale, from an across the enterprise. For duct Video Froduct Video Froduct Video For Devo For Directing Information Data Analytics Platform Data Analytics Platform	Bee unlocks the full value of machine data for the world's most instrumented enterprise, putting more data to work now. The Devo Data Analytics Platform collects, enhances and delivers real-time insights for IT, excurity, and business operations teams from analytics. Devo both streaming and historical machine data. Sold by Devo Product Video See product video (2 Fulfillment Method Software as a Service (Saas) Pricing Information Business or feas may septy.		Overview	Pricing	Usage	Support	Reviews
Putting more data to work now. The Devo Data Analytics, enhances and analyses machine, business and generational data, at scale, from ancrosh enterprises Devo delivers real-time insights for TT, security, and business operations teams from analytics on both streaming and historical machine data. Sold by Devo Product Video See product	Product Video See product video (Saas) Product video See product video (Saas)		Product Ove	erview			
Sold by     Deve       Product Video     See product video C2       Fulfillment Method     Software as a Service (SaaS)   Pricing Information Below are the total costs for these different subscription durations. Additional tables or these may apply. Data Analytics Platform	Sold by     Devo       Product Video     See product video CF       Fulfillment Method     Software as a Service (Saas)		putting more data to wo analyzes machine, busin delivers real-time insigh	rk now. The Devo Data Analytics Platform ess and operational data, at scale, from acr ts for IT, security, and business operations t	collects, enhances and oss the enterprise. Devo	<ul> <li>Handles terabytes of ingest volu</li> </ul>	ime while analyzing
Product Video     See product Video CF       Fulfillment Method     Software as a Service (Saas)   Pricing Information        Below are the total costs for these different subscription durations.        Additional tables or frees may apply.   Data Analytics Platform	Product Video     See product video       Fulfillment Method     Software as a Service (SaaS)		Sold by		Devo		
Fulfiliment Method     Software as a Service (SaaS)   Pricing Information       Below as the total costs for these different subscription durations.   Data Analytics Platform	Fulfillment Method     Software as a Service (Saas)       Pricing Information       Below are the total cosh for three different subscription durations.		Product Video		See product video 🗷		livers both scale and
Below are the total costs for these different subscription durations. Additional taxes or fees may apply. Data Analytics Platform	Below are the total costs for these different subscription durations. Additional taxes or fees may apply.		Fulfillment Method	Softwa	re as a Service (SaaS)		
Additional taxes or fees may apply. Data Analytics Platform	Additional taxes or fees may apply.		Pricing Info	mation			
	Data Analytics Platform		Below are the total costs Additional taxes or fees	for these different subscription durations. nay apply.			
			Data Analytics Plat	form			
Data Description THONTH 12 MONTHS	Data Description 1 MONTH 12 MONTHS		Data D	escription 1 MONTH 12 MONTHS			

5

**Step 2** Select your contract options and click the **Create Contract** button.



Part 1 complete Part 2: Step 1-2 of 9

### 🐓 aws marketplace

#### Part-2: Demonstration Guide for Devo Security Operations

Security Operations	* ◙ ⊛							-
A Home > 🔡 Overview Dashboard								
Alerts		Analytics					Investigations	
Most Critical & Not Triaged Alerts		FW traffic duri					Top investigations, sorted by age	
<b>企</b> 6/24	48/134	+	47 R 1				Creased Modified Investigation Importance Killicha	n Assignee Scauz
-		-	TEG.O				3 months about 2 directory travenal Medium Detens 00.129.154.198 Medium Evasion	
¥.		1.5	The state	1 1 0	Ser 1	1 Pro	3 months about 1 User behavior Comms month 1380.100.52.176 High Control	and b I fred Open
٩		1 Sa					2 months 27 days afford Virus High Exploits	wion Cesar Activ
Alert types stacked by ATTDCX MITRE techniques		10	Part I				2 months about 2 GhostNet Virus High Exploits	vion Cesar Activ
ф						A	2 months about 2 Possible DOOS to High Exploits	nion Cesar Activ Jimenez state
960 1960	_						2 months about 2 Possible DDOS to High Exploits	ation Cesar Unde Jimenez revie
400			1				privescalation 2 months 20 days T2004 Upload big Medium Exploits binary file	
5555 5550			5-		and the		2 months about 2 investigation Medium Commo	and & Samuel Open
200								
	_						10 rows 👻 🖂	
¢ ***		Google			Interest Color Masach	maliferica Terris of Use	Investigations labels word cloud	
Model Analytics	Observation Detection	Top entities by	y impact			80		
		Impact $ heta$	IP Hoursame	First seen / Country	City Brites in	Bynes out	<u></u>	
Top Entities by alert				Last seen 0.00009	17.48 MR	13.09.68	minikatz 🖇	
<u>ل</u>				10-02-2020 15:00 10-02-2020 04:00 10-02-2020 15:00			100 m	
200				10-02-2020 15:00 10-02-2020 03:40 10-02-2020 15:00	105.92 KB		mimikatz 40.52.603	
<sup>2</sup> 320				10-02-2020 03:40 10-02-2020 14:40			<u>م</u>	
				10-02-2020 04:00 10-02-2020 15:00				
1 40 M 40 M 40 M	to get and the site of a set			10-02-2020 03:40 10-02-2020 15:00				

0

Step 2Select the triage iconfrom the green bar at the top of the dashboard to viewItriaged alerts.

÷= -	Security Operation					
•		> 🙏 Triage				
$\bigcirc$	Filters					
ഹ 國	From20-01-2020 15:55	To 21-01-2020 15:55			Assigned to     Select	
*	Advanced Filters 🗸 🗸					
Q E	Alerts					
Þ	∎ IP: 10.52.60.69 ⊙	Host: 10.52.60.69	🔿 User: nutt 🔿 🔶			
۴Ļ¢	Alert priority	Alert type	Description	Details	Tactic	Technique
000	Critical		Power Shell Exec. Bypass	Suspicious PowerShell download command executed	Privilege Escalation	Exploitation (
4999 47						
	IP: 10.0.0.100 ()					
ŝ	Alert priority	Alert type	Description	Details	Tactic	Technique

### aws marketplace

Step 3	Select the <b>i</b>	nvestigations icon	log from t	he gre	en bar at th	e top of the dashboard.
	Security	Operations 🚦 🙏 🖻 🔶				
		dent Response > 🖸 Investigations				
	D Investi	gation filters				
	01-01-2020 1 년77				Select a user	•
	よく。 Advanced Filte					_
	Investigatio	ns Investigation name	Assigned to	Status	ATT&CK Tactic	Labels K
	High Iti	Unauthorized Powershell execution	2 Jason Mical			(D powershell) (D exploit)
	000 000 High		Miguel Abollado     Miguel Abollado			
	Low High		Cesar Jimenez     Christophe		Pivoting	
	لَيْنَةُ High		L John			(D RDP)
	High High		🛓 Fran Gornez		Privilege Escalation Persistence	RCE     D powershelt     D privilege escalation

6

## Step 4Select the PowerShell Privilege Escalation option under the Investigation,Name column.

Home		oonse > 🧕 Investigations				
	Investigation filt					
From Cal-4					ssigned to elect a user	
	iced Filters 🗸 🗸					
	stigations					
Impor	tance Inv	restigation name	Assigned to	Status	ATT&CK Tactic	Labels
						D powershell D exploit
îţi Higi			2 Miguel Abollado			
000 000 Higi			2 Miguel Abollado			
49999 47 Love			🔔 Cesar Jimenez			
			2 Christophe			
<u>نې</u>	RDF	P Infection Test	🚨 John			
> на		vershell Privilege Escalation	🚊 Fran Gornez			D RCE D powershell D privilege escalation
High	atta	ck				
	-	1.11.1				

6

### 💐 aws marketplace



A Home → Incident Response → Q Investigati	ons > 🖸 Investigation Details -	Powershell Privilege Esca	Escalation
$\bigcirc$			
		Evidence	Investigation Timeline
<u>ش</u>			
Name* Powershell Privilege Escalation		Comments	Investigation comments
K Importance		Detections	
Q Medium High		Observations	Fred (fred.wilmot@devo.com) 24 days – added context
Status Open			
Asigned to			
Fran Gomez		Related investigations	ns
		Queries	
000 Details		Enrichment	
powershell execution for privilege bypass using accessibilit	y RCE exploit	Entities	
		Association	Chris O'brien (chris.obrien@devo.com) Start writing your new comment here
Chi CE (a)         powershell (a)         privilege escalation		Timetines	
Keywords			
		Files / Analysis	
(?)	Created 17-01-2020 04:49		

Step 6

Under the **Evidence column**, navigate through the menu options, like **Detections**, **Queries**, and **Association** to view the information.

👷 🕆 Home > Incident Response > 👩 Investigations	🔅 🔉 👩 Investigation Details		
$\cap$			
			Investigation Timeline
ŵ			
Powershell Privilege Escalation		Comments	Investigation Detections
X Importance		Detections	
Low Medium High		Observations	Critical Suspicious PowerShell download command executed
Status			
Open			Table : edr.crowdstrike.cannon.processrollup2 ATT&CK Tactic : Privilege Escalat
Asigned to Fran Gomez		•	
↓  Y  ATTBCK Tectic*		Related investigations	
Privilene Escalation		Queries	Critical Suspicious PowerShell download command executed
OCO OCO Details			Table : edr.crowdstrike.cannon.processrollup2 ATT&CK Tactic : Privilege Escala
Details (1999) (2) powershell execution for privilege bypass using accessibility RC	CE exploit	Enrichment	Table : edr.crowdstrike.cannon.processrollup2 Al TeCk Tactic : Privilege Escalat
		Entities	
Labels		Association	
RCE C powershell C privilege escalation		Addition	
		Timelines	Critical Suspicious PowerShell download command executed
> C RCE C powershell C privilege escalation			Table : edr.crowdstrike.cannon.processrollup? ATT&CK Tactic : Privilege Escalati

6



#### **Step - 6 continues**

	Excrete serve in a	A service of the s			lation				
<pre>Subsection Section Sectio</pre>									
<pre>Bit Set Set Set Set Set Set Set Set Set Se</pre>	Control Contro	Subjective in a construction of a constructio		Evidence	Investigation Timeline				
Image: Second	<pre>Second Second Seco</pre>			Comments	Investigation queries				
Image: market in the second secon	Image: Image		K Importance	Detections		mentidaes com) - 34 dae			
	A set of the set of	A real property (Property 1) and the set of the set	C Hodium High	Observations					
			Deen .		3 and origi	Host -> "10.52.60"			
			Fran Gomez × •	Analytics     Related investigations					
			Distance Freedom						
	Image: Image	Image: Control of Cont	Details						
			Lukets						
			D RCE D powershell D phylicity escalation D	Association — Timelines	Chris O'brien (chris.obri Start writing your new qu	ien@deva.com) ery.here			
		Carty Question: If A      A	Reywords     D RCC      D powershell     D privilege escalation	Files / Analysis					
Image: Starting Operation:       Image: Starting Operation:         Image: Starting Operation:       Image: Startinge		Scotty Operation: II A O O For a house and a state of the scatter of th	Counted 17-03-2020 10-45						
Image: Sector	Scoly Operators Disposed Dis	Succipientes DEparentiques         Succipientes DEparentes DEparentiques	3						
	Control Quertion 1   A los / bartel Regres / 0 Descrite Regres / 0 Descrit	Cardity Operation:       11       1							
	Control Quertion 1   A los / bartel Regres / 0 Descrite Regres / 0 Descrit	Cardity Operation:       11       1							
Control Operations 1 A R B A B A B A B A B A B A B A B A B A	Construction         Construction<	Cardity Operation:       11       1							
	Construction         Construction<	Cardity Operation:       11       1							
	Construction         Construction<	Cardity Operation:       11       1							
	Constructions is independent in the second secon	Cardity Operation:       11       1							
	Constructions is independent in the second secon	Cardity Operation:       11       1							
	Constructions is independent in the second secon	Cardity Operation:       11       1							
	Construction         Construction<	Cardity Operation:       11       1	9			Security Operations DFIR pow			
<pre></pre>	<pre></pre>	<pre>I Nr ) Notestingers ) notegets ) notesting Statestinger Statestin</pre>							
Image: market in a particular in a	Meximum	Med	A Home → Incident Response → Q Investigations → Q Investigation I	Details - Powershell Privilege Esca	alation				
Image: Section of the sec					Investigation Timeline				
Image: Section of the sec	Image: Control of the state of th	Image: Section Sect	<u>ش</u>			C) Query metanometric sa	wrinn limit 150 tone system		
Image: Construction	Image: Control of the second of t	Num	Romen <sup>a</sup> Powershell Privilege Escalation	Comments			<b>limit 150</b> type system		
Image: Section of the sec	All Carbon   All Carbon   And Carbon   Carbon <t< td=""><td>All of local   All of local <td>Criterian Parantina Provincia Constanta Autoritati Provinci</td><td>Comments </td><td></td><td>٢</td><td>wing (imit 152 type pyram</td><td>ţ.</td><td>×</td></td></t<>	All of local   All of local <td>Criterian Parantina Provincia Constanta Autoritati Provinci</td> <td>Comments </td> <td></td> <td>٢</td> <td>wing (imit 152 type pyram</td> <td>ţ.</td> <td>×</td>	Criterian Parantina Provincia Constanta Autoritati Provinci	Comments 		٢	wing (imit 152 type pyram	ţ.	×
Image: Section of the sec	In Club Curbo   Curbo <td< td=""><td></td><td>Construction     Construction     Construction     Construction     Construction     Construction     Construction     Construction     Construction     Construction     Construction</td><td>Comments Detections Observations Madeds</td><td></td><td><u>ی</u></td><td>mmg 1998 190 type symm</td><td>ţ,</td><td>×</td></td<>		Construction	Comments Detections Observations Madeds		<u>ی</u>	mmg 1998 190 type symm	ţ,	×
Image: Second second consider for an index plane and go consider for a second consider for an index plane and go consider for a second consider for an index plane and go consider for a second consider fo			Annormal Protogen Tradition     Annormal Protogen Tradition     Annormal Protogen Tradition     Annormal Protogen     Annormal	Comments Detections Cbservations Models Analytica	Relationships Incomp Outgoing Linit Incont Incomp Entities	<u>ی</u>		ť	×
Image: Construction for private grant constructine grant construction for private grant construction for pr			Anner     A	Comments Detections Observations Medita Analytics Related Investigations	Relationships	<u>ی</u>		t reconnection	×
			Image: A manual manage inclusion	Comments Detections Detections Detections Comments Analysis Related Investigations Counties	Relationships	<u>ی</u>		EXALMADE .	~
Interime     Interime <b>Interim</b>	Tension         Data         Description           Difficult states         Difficult states         Difficult states         Difficult states	Teaching         Teaching         Teaching           DITIO         presented III         presented III         presented III         presented IIII           It and exame IS III. SIG 1000 ft         Council VIII. SIG 1000 ft         Council VIII. SIG 1000 ft         Presented IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Image: Second	Comments Detections De	Relationships	<u>ی</u>		PARTIANZA A	~
			Arrow Control Marge Exclusion     Marrie      Mar	Connection Descolaria Constructions Pacifica National Investigations Advantages Constructions Constr	Relationships	<u>ی</u>		Evantacose	
				Connection Descolaria Constructions Pacifica National Investigations Advantages Constructions Constr	Relationships	<u>ی</u>		Eraturseka	~
ტ 			Arrow and a second and a s	Comments Detectors Comments Detectors Contents Addet sectors Contents Contents Contents Contents Contents Contents	Relationships	<u>ی</u>		transcore	
				Comments Detectors Comments Detectors Contents Addet sectors Contents Contents Contents Contents Contents Contents	Relationships	<u>ی</u>			
Security Operations: DRB powered to Daws	Security Operations: EPIE powersity Date	Security Operations. El® powend by Daw		Comments Detectors Comments Detectors Contents Addet sectors Contents Contents Contents Contents Contents Contents	Relationships	<u>ی</u>		Pantakases	
Security Operations: Of Bigumental Joso	Security Operations: LPRB powered by Deep	Security Operations Diff powersity Date		Comments Detectors Comments Detectors Contents Addet sectors Contents Contents Contents Contents Contents Contents	Relationships	<u>ی</u>		Territoria	
Security Operations Diffigurement to Deep	Security Operations Bill powersity Dave	Security Operations Dilli powers/ly:Dec		Comments Detectors Comments Detectors Contents Addet sectors Contents Contents Contents Contents Contents Contents	Relationships	<u>ی</u>			
Security Operations . DNII powered to Dove	Security Operations Bill powersity Date	Security Operations Dilli powers/ly:Dwo		Comments Detectors Comments Detectors Contents Addet sectors Contents Contents Contents Contents Contents Contents	Relationships	<u>ی</u>			
Security Operations DRE powered by Dave	Security Operations Bill powersity Date	Security Operations Dilli powers/ty:Dwo		Comments Detectors Comments Detectors Contents Addet sectors Contents Conte	Relationships	<u>ی</u>			
Security Operations DRE powered by Dave	Security Operations Diff powershy Dave	Security Operations DIE governity Dave		Comments Detectors Comments Detectors Contents Addet sectors Contents Conte	Relationships	<u>ی</u>		ERATURADE A	
				Comments Detectors Comments Detectors Contents Addet sectors Contents Conte	Relationships	<u>ی</u>		ERATINGUE	
				Comments Detectors Comments Detectors Contents Addet sectors Contents Conte	Relationships			EPARTAGON	
			Arrow and a second provider of a second provid	Comments Detectors Comments Detectors Contents Addet sectors Contents Conte	Relationships			EPARTAGON	

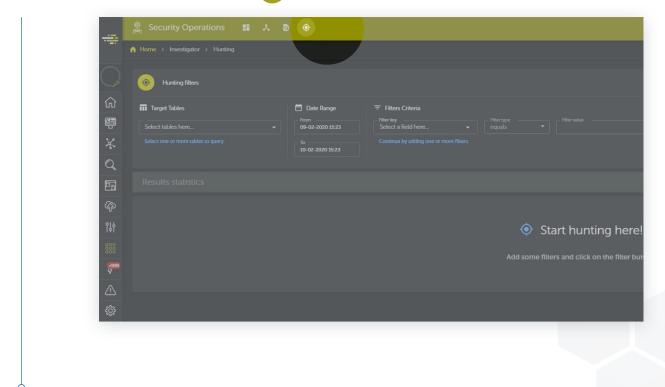
#### 💒 aws marketplace

A Home > Incident Response > 🧕 Investigation	🛚 🛪 👌 Investigation Deta				
$\bigcirc$					
<b></b>					
Name*					
Powershell Privilege Escalation					
K, Importance					
C Medium				Files Selected	
Status					
Open			Drag & drop		
Asigned to			or browse your files		
¢↓↓ I¢I ATTBCK Tactic*					
Privilege Escalation					
Details			Files included in this investigatio	n	
(999) y powershell execution for privilege bypass using accessibility R	CE exploit		Name	User	Size
Labets			bluekeep.pcap	fred.wilmot@devo.com	
RCE     D     powershell     D     privilege escalation		Association			
		Timelines	backbone.js	fred.wilmot@devo.com	
Keywords			index_secops_usaf_09_01_20202.html		
o ice provinsi principa economica	_	Files / Analysis			

Select the **Files/Analysis** option to view the files included in the investigation.

Step 7

**Step 8** Select the **Hunting icon** (<i>) from the green bar at the top of the dashboard.



### aws marketplace

#### Step 9

Select the **main dashboard icon**  to navigate back to the main dashboard.





## Thank you.

For more information, visit **go.aws/2uYGnSs** 

