

Automatizovaná bezpečnosť

Plne automatizovaná security a compliance vo svete hybridného cloudu

Jakub Veverka Senior Solution Architect jakub.veverka@redhat.com



6699



2

63% of respondents say their leaders understand that **automation**, **machine learning**, **artificial intelligence and orchestration** strengthens cyber resilience.

Ponemon Institute







CYBER SCAPE

2020

Mistoria 8 Information Complexity		Mich Consults	Paulle state Convolution	
Advanced Threat Protection	ICS + OT	web security	Endpoint Prevention	WAF & Application Security
	APERIO TRAVSHORE BELDEN	Cakamal aurionpro 🖗 aUTHE	INTICE AhnLab A Zovost Q Avira Browner	
		Banacuda OBROADCOM (()		INTRAST DAME CONTRAST
OPSWAT. % paloator RESEC Sussentment SOMICWALL SOPHOS	Crocescour IIIIHALO # dimension	> CEQUENCE" Check Point	CO C	imperva 👰 intearlari 🕉 NETSPI 🦣 enapsis ORACLE 4 palaetto
NAC SDN DDoS Protection DNS Security			igicert' Tintego ivanti kaspersky M Checklee	Penda (portshift Protego Ouaivs ""radware
OFUDO ARAUDONET A TELE CIRCO CARANTA DOUGL Part OBLUECAT clastic	Chebo Cherter Statition	Sericom	epoint Microsoft December OPSWAT. % paloalto	RAPIDD Network riverbed 2 safe-t sevenus St-pe
X AXONIUS (11-11)- CISCO Crberes, Cyxters	Otenable O'ERYE			
E Extreme «reassour TEMPERED O Translent() Reustar Newsource Base	Network Analysis & Forensics	imperva McAfee OM	en lo Endpoint Detection & Response	🐠 1969 📽 Trustwover VERACOIDE 🔬 walarm 🖗 waratek
greeners pirtnox. VERSA Zenteral generatus CRACLE Quere	AWAKE SEROFTER SCGS dudo	MISE NANGGOO Derimeters proc	ofpoint	Application Security Testing
Statistics State Structure	CORE COREIght Yours		COMODO	
	Section Fidelis - Contra Sta	Reblaze Tenecola Intern		
SASE Dependion	SARY Contested a Logithather Communic NETSCOUT	SHIELDAPSQUARE SITTOOUTWAII SOPI	HOS kaspersky M Onenemen nexthink Decomo paloalto	
CATO Romanian forcepoint Paramet (DOSS Anatonics ACALVID) Atting Country & Gentlage Sciences	Sector Sector Stream VERINT	toparte The NO. Trust		
Oquestes & paloetto D sensers & VERSA @ Society Fiddlin Lineer Vision Emocecretes IRAPK	330 Millio	whiteops 25	scaler	Spring 3/3 Chemanie & Interviewe Veracular Cone
MCSP	A41	Data Security		Mobile Security
Traditional MSSP Advanced MSS & MDR	Encryption	DLP	Data Privacy Data Centric Security another	
	B baffle guages Faterland ()		Actifie @ ago Deserved DHD;]	
TEM Minter ONTE Pringie Optiv	TALL PROPERTY CONTRACT OF THE PROPERTY CONTRACT OF THE	Otra Instraligia		Ohryphanite @Lookout Medekeen @NotorLifeLoar @NovSecure
Common Section Common C		STONIC STONIC		doo OPSafe OSaltowa Contractin SOTT OTeleSign ATESKALABS
Risk & Compliance	Security Operations & Incide	nt Response	Threat Intelligence	Messaging Security
Risk Assessment & Visibility	SIEM	Momen	IN THE AIQ ANOMALI Blueliv.	
			O Durkhare O Centropetal CISCO Scaliber Configure Configure State	The Burney And Burney Burney HOCANA
O NOFEE CO. DOCTO CO. DOCT			Cyberint digital shadows, @powawroots @EclecticiQ	
Nytersenbar @ normanic O tenable @ UpGuard VENAFT O zeguro zteninostri @ meaning	HanSight AHuntsman	IN Accountion	KRSIGHT (FLASHPOINT GROUP)E O HanSight	
Pen Testing & Breach Simulation GRC Security Awareness & Training			NTELAT	
	Netsurion. EventTracker Q Palantir	RAPIDO RSA T		Xaramba Becurity
		CONMILL		RIDE TRILLIUM Upstream proofpoint Season Some SonicWALL
	SECURONAX Solarwinds Splunk>	sumo logic TIBC Trustwave	SixGIL SKURIO	Home SOPHOS @IMEMS Trustwave
	Security Incid	ent Response	SpyCloud @ SUPPress X ThreatConnect Interactionnet	F-Secure CALIMANL Witho
Identity & Access Management	> networks attartieus >		Threat GTOP TRU*STAR WEBROOT	JBICA SAM
Authentication	CYBER INUME	S DARKLIGHT	District Disk Management	Consultu Consulting 9. Continue
Cope	EDELABS encode	OFIREEYE LEM	Constant Visit Management	
HARH DEC ECOSTAR & ForgeRock Orubb Googe TIT ODEE T	Microsoft	N netskope // paloaito		
D'imprivata 🔅 INTRINSIC ID JUMIC' 🔮 LAUNASIS OK Spindrop' 🔤 🎲 oldiniD		RAPID: Haymeon		
🛞 sucruss 🚯 subrus 🏭 🎯 scontartori stani 🚳 🗋 scontenuem 🖾 SEULINII tascent	SEC Servicenow	Secondary Spiunk>	and the pure second sec	· · · · ·
	SWIMLANE	Connect VERINT Witfoo	Blockchain	Fraud & Transaction Security
IDaaS	Security	Analytics		al DATAVISOR CARDINATION emailage ethoca Operander feedzai FICO
okta onelogin ORACLE 🔜 RSA THALES	AWAKE BROADCOM ACT		uardtime 🗟 🕲 IDEE Inter/stellar Nu 🗋 🕼 🕼 🕼 🕅 🕅 🕅 🕅 🖗 🕼 👘 🖗 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘 👘	ne klenTrust @Kount' @LexisNexis' @MagleCube
Privileged Management	en empow //2 exabeam	S Fluency FURTINET	R remme a weather \$ Zamna.	# SICNIFYD & simility & second Tetral Data UNIKEN @ technology (Dwithter.com
Process One IDENTITY Cremedant Specific Without	HanSight Maystax	IMVISION TECHNOLOGIES OF IronNet	Cloud Secu	ity
	#LogRhythm DECUS	ODSErve IT % paloalto	Container	CASB
Commercial Contraction Commercial	patternex Reservoir Labs		anchore Jaqua CAPRILLES BetterCloud bridgecrew (Cavinin III Check Point @ Cave	
Consumer Identity Consumer Identity Jumic' boirradus Microsoft	SEC SECURONIX	SUMO IOGIC	Coutrester	Lacework (% paloalto)
Omman 🧼 💷 sawi Tiulico verato 57 Zamna.	OTHETARAY SVECTRA	Veriato viniware	eportativit (Qualis and Stratig Trining) eportativit (Contactivit Contactivit Contactivit Contactivit Contactivity Conta	ur] VITTWARE COSCIAN Proofpoint. SECURIDO UT SKYFORMATION









At Cloud Scale You Have No Choice But Automate

This Japanese Al security camera shows the future of surveillance will be automated

By James Vincent | @jjvincent | Jun 26, 2018, 7:31am EDT



8





Introducing Ansible Automation Platform







Red Hat Ansible Automation Platform has a robust ecosystem ...



SIEM and SOAR: Why they matter



What is a SIEM?

6699

13

Gartner defines the security and information event management (SIEM) market by the customer's need to analyze event data in real time for early detection of targeted attacks and data breaches, and to collect, store, investigate and report on log data for **incident response**, forensics and regulatory compliance. SIEM technology aggregates event data produced by security devices, network infrastructure, systems and applications.





Ansible Automation Platform & SIEM





What is SOAR?

6699

Gartner defines security orchestration, automation and response (SOAR) as technologies that enable organizations to collect security data and alerts from different sources. SOAR allows incident analysis and triage to be performed leveraging a combination of human and machine power. This helps define, prioritize and drive standardized incident response activities according to a standard workflow.





Source:

How Ansible security automation relates to SOAR?

Ansible security automation doesn't compete in the SOAR space.

Ansible Automation Platform complements and extends the custom automation engines included in most SOAR.





Ansible Automation Platform Integration With SOAR





Introducing Ansible Security Automation

What Is Ansible security automation?



Ansible security automation is our expansion deeper into the security use case. The goal is to provide a more efficient, streamlined way for security teams to automate their various processes for the identification, search, and response to security events. This is more complex and higher-value than the application of a security baseline (PCI, STIG, CIS) to a server.

Ansible security automation is a supported set of Ansible modules, roles and playbooks designed to unify the security response to cyberattacks.



Is It A Security Solution?

No. Ansible can help Security teams "stitch together" the numerous security solutions and tools already in their IT environment for a more effective cyber defense.



By automating security capabilities, organizations can better unify responses to cyberattacks through the coordination of multiple, disparate security solutions, helping these technologies to act as one in the face of an IT security event.

Red Hat will not become a security vendor, we want to be a security enabler.



What Does It Do?

Through Ansible Security Automation, IT organizations can address multiple popular use cases.





Investigation Enrichment

Enabling programmatic access to log configurations such as destination, verbosity, etc.

Threat Hunting

Automating alerts, correlation searches and signature manipulation



Incident Response

Creating new security policies to whitelist, blacklist or quarantine a machine



How Can You Trigger The Remediation?

₩НΟ	HOW	THROUGH	EXAMPLES
splunk >	Systems with logic on board, such SOAR or SIEM, can trigger actions when a set of conditions are matched. Actions can simply be launching scripts or directly linux commands.	RED HAT ANSIBLE Engine RED HAT	Splunk can use <i>custom search command</i> or, <i>custom alert action scripts</i> to execute a perl/python script that calls Ansible Linux command.
IBM.			Through <i>Workflow actions</i> Splunk can call Ansible Tower APIs.
FURTINET.	Systems with no logic on board, such base firewalls or IDS, has to rely on their underlying OSes, usually Linux-based, to trigger any external action. For those systems a DIY approach is likely to be necessary, using a combination of scripting, OSes' facilities and third party programs to check the conditions and consequently trigger actions.	RED HAT ANSIBLE Engine	Snort can output as syslog and use syslog-ng's <i>program()</i> destination combined with a filter. Check Point can schedule a <i>cronjob</i> in the management station.
RED HAT ANSIBLE Tower	Ansible Tower can provide a central point of coordination for all the technologies involved in a remediation process. Ansible Playbooks can be used as security workflows to coordinate actions between different areas of the IT stack and Job Templates can be shared through APIs across different teams.	Infoblox 💸 FERTINET.	



FUTURE

MON

Investigation Enrichment: Application Behaviour

The Assessment Of Abnormal Behaviours Involves Multiple Steps Like Validating An Ip Address Against Multiple Sources, Searching The Environment For Signs Of Infiltration, Etc. And Then Process And Present The Information To The Security Analyst.



splunk >

Detects an anomaly from the behaviour of an application. Asks Snort & Check Point for more information.



Implements a new rule to collect more information in the affected perimeter.



Raises the level of logging on low level networking perimeter.

splunk>

Consolidates information for the triage.





Restore original configurations.



Incident Response: Sql Injection Attack

Dos Mitigation Requires Up To 10 Manual Steps Between Identification And Remediation.





A Error Based SQL Injection event is logged, syslog-ng launches an ansible playbook which exports the log and ships it to Splunk.

splunk'>

Ansible module creates a new notable event, Splunk ES correlates other sources and confirms it's a SQL Injection attack. Using adaptive response actions launches a playbook toward Check Point passing the attacker's IP.



Ansible module creates a new firewall rule to blacklist the IP source of the attack.



After *n* seconds that Error Based SQL Injection event disappeared, syslogng launches an ansible playbook to update Splunk.



Ansible module marks notable event as *Resolved*.



How Do We Get There?

- Reconsider automation as a strategic defense, not just another tactical tool
- Discover what automation tools are the most used in your org, and why
- Assess selected tools' capability to mitigate risks of automation
- Include automation software as target for pentesting

- Pilot automated host and network security for noncritical applications
- Evaluate feasibility of centralized automation and lock down of platforms against rogue scripting
- Let your automation vendor know what security tools you are using, and how you'd like them to interact with each other
- Pressure security vendors to start integrating with automation tools



Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



