# IBM Security QRadar SOAR Scale the SOC with QRadar SOAR

**IBM Security** 



Ī



# 49%

SOC team members are only getting to half of the alerts that they're supposed to review within a typical workday



a secon statist the self. Autompticit: resulting antication for free found activities statistics for the second activities and activities

Note Scitched Bed Files/Lee: [ed] sectors (Hef?TentBelieited[["dec.54", "tented scitched Bed files/Lee", "tented scitched Bed files/Lee", [ed] sectors (Hef?TentBelieited[["dec.54", "tented scitched Bed scitched Bed scitched Bed scitched Bed scitched Bed files/Lee [ed] scitched Bed scitched Bed files/Lee [ed] scitched [ide: 1

Note statice and flue.New (wc) allocating threads: 1 Allocating static (LA) autput/wc allo statice and flue.Fluedcapt (wc) starting static (LA) autput/wc allo statice and client.Behrospic Connecting to ResourceBanager at sandbox. WcB statice BHD client.Behrospic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal.Winopic Connecting to ResourceBanager at sandbox. WcB statice (BHD autreal. WcB statice (BHD a

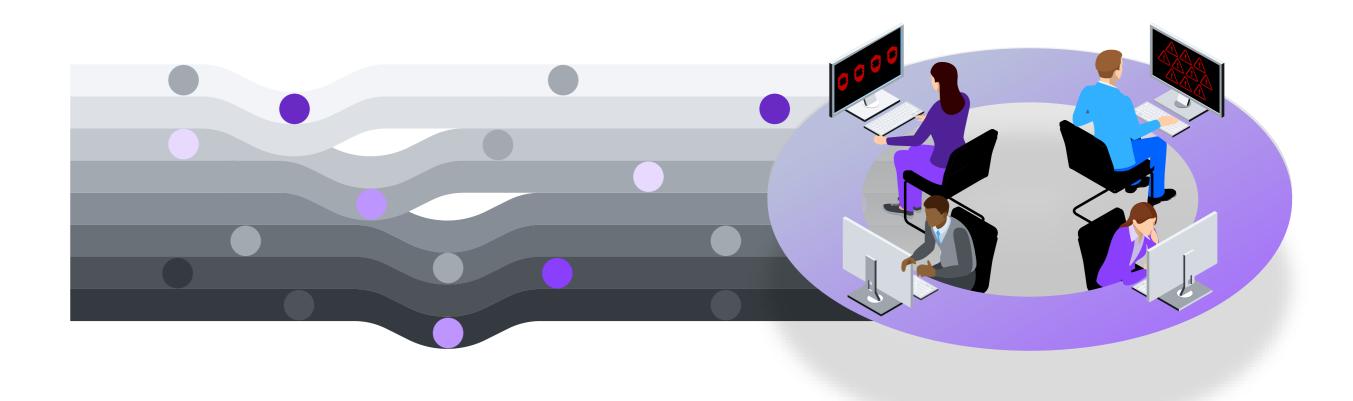


# Security operations needs major improvement

The move to cloud and IT modernization has expanded the attack surface, creating increased security complexity

## Poor visibility 2 out of 3 organizations' external attack surface has expanded in the last year<sup>2</sup>

Disconnected tools 80% of organizations use at least 10 disparate solutions to manage security hygiene<sup>2</sup>



### Keeping up with attackers 29% of security operations processes are immature and need reengineering before they can be automated<sup>1</sup>

Information overload 52% of security environments have become more difficult to manage over the last two years<sup>2</sup>

# 51% of organizations struggle to detect and respond to advanced threats<sup>1</sup>

# Current SecOps

Technology focused

Dependent on experts and heroes

Proprietary ecosystems

# Modernized SecOps

# Usability focused

# Democratize expertise and AI

# Open ecosystem



# IBM Security QRadar SOAR

Streamline your SOC with an automated and intelligent response using the industry's most open and interoperable SOAR platform

Modern incident management experience

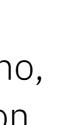
Identify in a single pane the who, what, how, and actions taken on a security investigation and incident response

Case title						
Sim Closed 🚫 F						Action
Details Tas	sks Breacl	n Notes M	embers Attachm	nents Artifacts		
Case details				Artifacts	Pl	aybook status 💊
pharetra mauris ultri	ces et. Aenean ligul	r adipiscing elit. Quisque t a augue, interdum id sem aecenas ac elementum du	per id, feugiat at diam.	4/10 72	%	14
Owner		Last updated		4 hits		Playbooks
Kyle O'Connell		21 Jun 2021 18	::14			
Severity High		Date created 21 Jun 2021 14		3 hits		
				2 hits		Complete 7 📕 In-progress 3 📕 Error
Respond		Non issue		EMAIL DragonAttachr	nent.pdf	Suspended 1 📕 Canceled 1
Threat Investigate	or			1 hit MD5 Hgs6fhd8dhdf		
6	2	8	2		Та	ısk list
Ŭ	_	Ŭ	_			
				Related cases	7	7/14 2
Mitre ATT&CK Tac	tics					
△ Initial Access	> Initial Execution	Persistance	ge Escalation	3/10 15		
O Defense Evasion	Credential Access	△ Discovery ◇ Late	eral Movement	<b>J</b> /10 <b>T</b>	<b>A</b>	Lorem ipsum dolor sit amet,
	ommand and Control	♦ Exfiltration	act			
Confidence				5 matches Lorem ipsum dolor sit amet,		Lorem ipsum dolor sit amet, tetur adipiscing elit. Cras iac
Confidence	Low			ID: 2549	consectetui	Due in 23 min
				Closed		

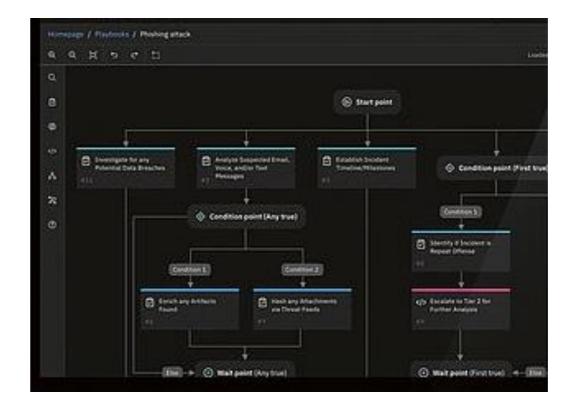
### 300 +available integrations

2()() out-of-the-box templates for privacy regulations

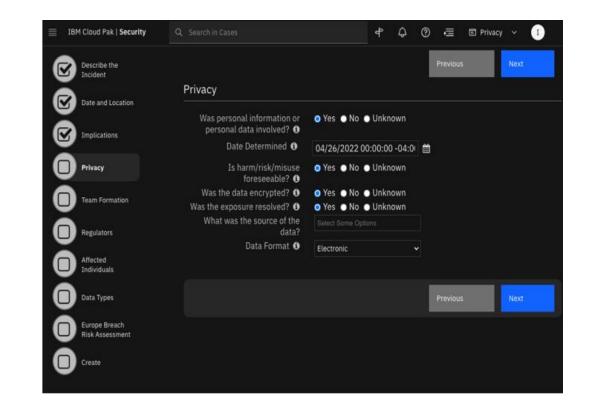
**IBM** Security



Streamline response with automation and intelligence Respond x7 faster with dynamic playbooks that combine people, process and technology



Navigate a complex global regulatory environment Meet time-sensitive reporting requirements to avoid expensive financial penalties with breach response



85% reduction in incident response time<sup>1</sup>





Modern incident management experience Efficiently respond to a case leveraging playbooks that adapt to your unique needs

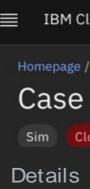
Get started faster

Quickly realize the value of a SOAR tool with easy-to-use functionality

Pre-built playbooks adapt to unique business processes Leverage customizable layout and tailored responses

Accelerated investigation & response Act quicky with automated treat investigation and threat hunting. Respond faster with recommended actions

Broad ecosystem of connectors Connect with your existing infrastructure and get a bi-directional flow



#### Case det

Descriptio Lorem ip pharetra Nullam p

Owner Kyle O'Co

Severity High

Phase Respond

#### Threat In

Artifacts in

6

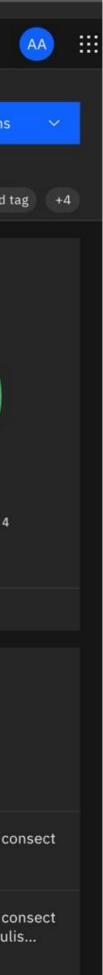
Mitre AT

 $\triangle$  Initia O Defer

Collect

Confidence 🔺 High 🔷

 Actions 								
Tasks Breach Notes Members Attachments Attlacts Furst to:	Cloud Pak for Security   Case Manage	ement				4 0	Æ	IBM MSS 🗸
Market Strate Consecteur adipiscing elit. Quisque tristique nisi risus, vel mauris ultrices et. Aenean ligula augue, interdum id semper id, feugiat at dian. Lacerat posuere elementum. Maecenas ac elementum dui. Muth hits Max, risk score 4/10 7 2 % 4 hits Muth hits Max, risk score 4/10 7 2 % 4 hits Muth hits Max, risk score 4/10 7 2 % 4 hits Muth hits Max, risk score 4/10 7 2 % 4 hits Muth hits Max, risk score 4/10 7 2 % 4 hits Muth hits Max, risk score 4 hits Muth fut control 6 scored at the score of t	title	Notes Memb	oers Attachme	ents Artifacts	5	First 1	ag Sec	
Investigator       MD5       Hgs6fhd8dhdfi7q8       View playbooks         2       8       2       View artifacts (10)       Task list       Complete       Unassigned         rT&CK Tactics       Access ◇ Initial Execution ○Persistance ◇ Privilege Escalation se Evasion ○Credential Access ◇ Discovery ◇ Lateral Movement       Matching artifacts       3/10       1.5       ▲ Lorem ipsum dolor sit amet, consectetur         *       S matches       Lorem ipsum dolor sit amet, consectetur       S matches       E Lorem ipsum dolor sit amet, consectetur	<sup>n</sup> sum dolor sit amet, consectetur adipi mauris ultrices et. Aenean ligula augu lacerat posuere elementum. Maecena	ue, interdum id semper id as ac elementum dui. Last updated 21 Jun 2021 18:14 Date created 21 Jun 2021 14:09 Resolution		With hits 4/10 4 hits INT 10.31.9 3 hits USER Joe B 2 hits	72% 92.255 loggs	Complete	Pla	14 aybooks rogress 3 Error 4
T&CK Tactics         Access ◇ Initial Execution ○ Persistance △ Privilege Escalation         Se Evasion ○ Credential Access △ Discovery ◇ Lateral Movement         tion △ Command and Control ◇ Exfiltration ○ Impact         S matches         Lorem ipsum dolor sit amet, consectetur         S matches         Lorem ipsum dolor sit amet, consectetur				MD5 Hgs6fl		Task list	books	Uppersidented
e Lorem ipsum dolor sit amet, consectetur tetur adipiscing elit. Cras iacul	Access Initial Execution Per se Evasion Credential Access	Discovery 🔷 Lateral Mo		Active cases		7/14		2
	e Medium 📕 Low			Lorem ipsum dolo	r sit amet, consectetur	tetur	adipiscir	ng elit. Cras iacul





# Streamline response with automation and intelligence Respond x7 faster with dynamic playbooks that combine people, process, and technology

Modern canvas for automation Easily build and design automations in an award-winning experience

### Dynamic playbooks

React with confidence to changing incident conditions

### Reusable and smart automation

Standardize activities and accelerate development with reusable sub-playbooks

### Importable and exportable

Easily move between different systems and incorporate new content



Playbook designer: Phishing attack	Save	ଝ ର 🖸
asks		
itial (12	) 🗸	
ngage (1455	) ✓ 😥 Attach eml file	
ctivate Corporate Incident Man (9	) $\checkmark$	
ata Breach – Individual notificati (56		
ata Breach – Authority notificati (131	) 🗸 Parse email attachmen	
ata Breach – General notification (89	) $\checkmark$	
espond (213	) <	
omplete (2	, <u> </u>	
		tract Subject, Sender, d Recipient from email
	Collect all data before continuing	
id task	+	

Navigate a complex global regulatory environment Meet time-sensitive reporting requirements to avoid expensive financial penalties with breach response

Stay ahead of evolving privacy regulations

Maintain up-to-date breach response plans that map data to 300+ complex, global privacy laws and regulations e.g., GDPR, HIPAA

### Integrated breach response

Accelerate response to data breaches by integrating repeatable, auditable processes while leveraging privacy-specific tasks directly into the overall incident playbook

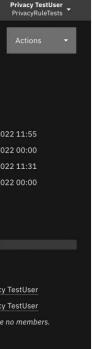
### Breach risk assessments

Evaluate the risk of harm to your business and generate clean reporting documentation

### Generate case reports

Easily share breach incident details across teams and with leadership to improve visibility and collaboration

IBM Security QRadar SOAR Dash	boards <del>-</del> Inbox Artifacts Incidents C	Create incident 🛛 🔫	۵	Playbooks Privacy TestUser PrivacyRuleTests	*				
Wiki				New Page +					
	<ul> <li>Privacy</li> </ul>								
Manage Resource Library Privacy Security IR	guidance documents, including pe Three asterisks (***) or an ellipsis product for editorial reasons, such statutes or regulation, hyperlinks U.S. States and Territories Alabama Alaska Arizona Arkar Indiana Jowa Kansas Kentuck New Hampshire New Jersey Ne	enalties where applicable. () indicate that irrelevant text h n as clarification. This editing is d are provided to the latest version nsas California Colorado Com y Louisiana Maine Maryland ew Mexico New York North Cal	igned into law), regulations (laws made by agencies) nas been removed from a section. Brackets ([]) indica one to make the statute or regulation more easily rea of each law freely available on the Internet. necticut Delaware District of Columbia Florida C Massachusetts Michigan Minnesota Mississippi rolina North Dakota Ohio Oklahoma Oregon Pe ti Virginia Virgin Islands Washington West Virgir	te text that was added or changed in th dable. For complete versions of the eorgia Guam Hawaii Idaho Illinois Missouri Montana Nebraska Nevad nnsylvania Puerto Rico Rhode Island	a				
	U.S. Federal and Trade Orga		IBM Security QRadar SOAR Dashbox		Create incident 🛛 🛨			Q @ 1	Playbooks
	Bank Secrecy Act CMS DARS/D HIPAA/HITECH Act NACHA NC						Playbook progr	ress No playbooks	s started
	U.S. Special Jurisdictions Arkansas (Insurance) Arkansas Illinois (State Agencies) Marylar Rhode Island (Insurance) Texas	nd (Insurance) Montana (Insura	ince					<b>Summary</b> ID Phase	11845 Initial
	Washington (Insurance) Washin	gton (State Agencies)	Tasks Details Breach No	tes Members News Feed	Attachments Stats	Timeline Artif	facts Email	Severity Date Created	High 05/04/20
			0% Complete	Owner: 0 selected 🛛 👻	Status: Active 🔫	Selected 👻 🗛	ldd Task	Date Occurred Date Discovered	
			Task Name	Owner	Due Date	Flags	Actions	Date Determined Was personal	05/04/20 Yes
			Initial				-	information or personal data involved?	
IBM <b>Security</b> QRadar SOAR Dashb.	oards → Inbox Artifacts Incidents Cre	eate incident 👻	Initial - (Data Breach - Organizational)					Incident Type	Malware
Describe the			🖆 🔗 *Assess the Risk	Unassigned 🗸	<b>Ø</b> 05/05/2022 00:00	<b>9</b> 0 <b>%</b> 0	:	People Created By Owner	A Privacy
Date and Location	Europe Breach Risk Asse	essment	Engage				-	Members	There are
Implications	To determine whether you are require breach could potentially have a range This could include damage like discrir	of significant adverse effects on i	indi 🛛 🖄 🖉 *Initial Triage	Unassigned <del>-</del>	⊙ No due date	<b>9</b> 0 <b>%</b> 0	:	Related Inci No related incident	
Privacy	higher and similarly where the likeliho	ood of these occurring is greater, t	fication obligations. Where the consequences of a bree the risk is also heightened. If in doubt, you should err each, you may not always have the full and comprehe	on the side of caution.					
Team Formation			, you should revise the Breach Risk Assessment.						
Regulators			iate types from the list below. Note that depending u the same time, as well as any combination of these.	pon the circumstances, a breach can					
Affected Individuals	Confidentiality breach		isclosure of, or access to, personal data						
Data Types	<ul> <li>Integrity breach</li> <li>Availability breach</li> </ul>		Iteration of personal data. Iss of access to, or destruction of, personal data, sucl , a lost decryption key in the case of encrypted data,						
Risk Assessment	Does the type of breach indicate risk Unknown	to the individual?							
	Explain how the type of breach has a	affected the level of risk to the inc	dividual.						



#### Thousands of open integrations at the center of your ecosystem **vm**ware<sup>\*</sup> Microsoft Azure **©ROWDSTRIKE** paloalto<sup>®</sup> **Carbon Black.** Delinea NOZOMI NETWORKS k> Google Cloud ·||· 1touch.io Recorded Future mongoDB<sub>®</sub> FERTINET THALES Security . . . **A**kamai CHECK POINT" • ExtraHop **(**)sysdig Jira Software ANOMALI **WIZ**<sup>+</sup> 🗖 aqua **:t** JUNIPer CYBER**ARK** FLASHPOINT Infoblox 🐳 THREATQUOTIENT 🔀 illumio Open **Open source and** fido **MITRE** quad9 Cybersecurity Schema ATT&CK ALLIANCE

aws	<b>Eszscaler</b> ™	cybereason	
tenable network security	service <b>nuw</b>	Trellix	splunl
ARMIS	RED HAT ANSIBLE	proofpoint.	
okta	Qualys.	MANDIANT	
snowflake		SAMSUNG	IBM
BIGFIX	Jonapsis		
<b>TANIUM</b>	CLAROTY	<b>OMPRIME</b>	mimecast
RiskLens <sup>®</sup>	(I) SentinelOne®	AP nets	skope 7

open community





**IBM** Security



# Thank you

© 2023 International Business Machines Corporation IBM and the IBM logo are trademarks of IBM Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark. This document is current as of the initial date of publication and may be changed by IBM at any time. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT, SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. Client examples are presented as illustrations of how those clients have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. Not all offerings are available in every country in which IBM operates. It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

