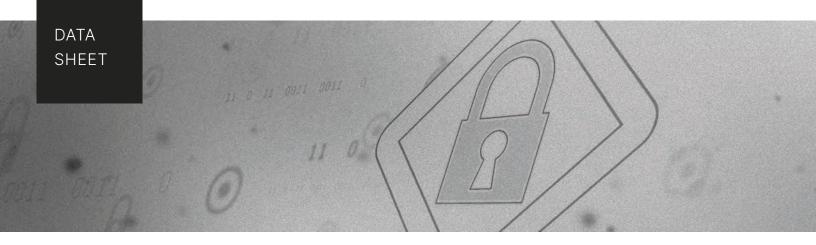
·III Recorded Future®



Recorded Future for IBM Security SOAR

Orchestration and automation drive digital transformation by enabling organizations to optimize existing processes, reduce costs, fill personnel gaps, and gain a competitive edge. For SOAR solutions to work effectively, however, they require a series of defined playbooks designed to describe threats and how to handle them using repeatable, automated security workflows. These playbooks are only as smart and effective as the data used to construct them. Without actionable, real-time data on active and emerging threats, security teams face problems like an overload of information, a lack of context, and more.

Contextualized Intelligence

Recorded Future's IBM Security SOAR integration helps security teams to quickly identify high-risk security events, rule out false positives, and address low-level events through automation. Teams can automate the retrieval of external data for details and context on IOCs from Recorded Future in a playbook. With this intelligence from the broadest set of sources, you can trust that IBM Security SOAR can automatically make real-time decisions that strengthen your organization's security.

Augmenting investigations with external threat data from Recorded Future allows analysts to resolve incidents faster and validate risk assigned to artifacts while reducing risk to the environment. Recorded Future for IBM Security SOAR automatically enriches artifacts added to incidents with real-time intelligence context. When an analyst captures an artifact in SOAR, the integration automates a request to Recorded Future for the current evidence-based intelligence insights. Recorded Future also integrates alerts into IBM Security SOAR as new incidents, with additional context on related IOCs including Insikt Notes, for a more complete and confident understanding of potential risks.



BENEFITS

- Reduce manual research time
- Simplify incident
 response workflows
- Respond quickly with transparency and context
- Confidently take action on real-time alerts or threats
- Maximize your investment in IBM Security SOAR

·III Recorded Future®

licious i	indicators									
Tasks	Details	Breach	Notes	Members	News Feed	Attachi	ments Stats	Timeline	Artifacts	Ema
Value	: All 🕶 🔍	Type: All	© Date	Created: All	O Has At	ttachment: /	All 🚳 Has Hit	s: All 🛛		
							Description			
Hits	Related I	Туре		Value		-	Recorded future enri	chment		
	0 0	Threat CVE ID Malware MD5 Hash					Malicious Risk score 89 Summary: 5 of 14 Risk Rules currently observe Reference count: 15735 Evidences:			
		Malware SHA-	1 Hash				Evidences. Rule triggered: Threat Researcher Criticality: 1 Evidence: 172 sightings on 9 sources including: Security Affairs, ISC Sans Top 10 IP Report, ISC Latest			
		Malware SHA-256 Hash					Headlines, Threat Post, SANS Internet Storm Center. Most recent link (Aug 28, 2020):			
	0	URL					04/07/2021 17:35	04/07	/2021 17:40	
	^{ated} /07/2021 1	7:33		Created By	/					
Тур	e			Related						
IP Address: Source				ified in the ar (currently Re						
	scription									
Re	corded futu	re enrichme	nt							
Su Re ⁻ Evi	Ilicious Risk mmary: 4 of ference cou idences:	54 Risk Rul nt: 32	es current	ly observed.						
Ru Cri Evi	le triggered ticality: 1 idence: 13 s	: Historical S	1 source: A	nary Attacke AbuseIP Data		ecent link	(Feb 13, 2018):			

ABOUT RECORDED FUTURE

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

www.recordedfuture.com

