1. Recorded Future LogICA5 integration

The Recorded Future platform provides real-time threat intelligence.

The complement of information provided by integrating Recorded Future into LogICA5 helps teams make more confident decisions faster. With up-to-the-minute risk scores and evidence, teams can easily see which indicators need attention first, helping them prioritize their time to achieve maximum impact.

When we access the Recorded Future Menu option in LogICA5, we are shown a table with the data imported from the platform.

Recorded Future Ge Ge COrded Future Recorded Future	tión Cuadros de Mando+ 🕢 Eventos TR+ 📓 Regias +			
ecorded Future				
⑦ Recorded Future				
Recorded Future				
P	Búsqueda por IP Min Evidencia	Max Evidencia		Q Buscar
				Mostrar 10 Y De 1
itul-	Description	Duidenaia de D	Detalle A	Acciones
				~ E >
	-			
				~ B ►
				~ 2
				~ B ►
28.0.44	Current risk: Malicious.Triggers 1 of 51 rules	65	false	- 6 -
22.42.141	Current risk: Malicious.Triggers 2 of 51 rules	66	false	
21.110.91	Current risk: Malicious.Triggers 1 of 51 rules	65 f	false	- 0 -
5.37.37	Current risk: Malicious.Triggers 1 of 51 rules	65	false	· B •
	fitulo 1.11.11.11 30.104.239 1.81.21.0.36 4.16.71 5.44.55 20.64 22.62.141 22.42.140 21.110.91	1.11.11.11 Current risk Maklous, Triggers 3 of 51 rules 3.01.04.239 Current risk Maklous, Triggers 2 of 51 rules 3.01.04.239 Current risk Maklous, Triggers 2 of 51 rules 3.01.04.239 Current risk Maklous, Triggers 2 of 51 rules 4.05.71 Current risk Maklous, Triggers 2 of 51 rules 4.05.71 Current risk Maklous, Triggers 2 of 51 rules 4.05.23 Current risk Maklous, Triggers 2 of 51 rules 2.05.44 Current risk Maklous, Triggers 1 of 51 rules 2.05.44 Current risk Maklous, Triggers 1 of 51 rules 2.24.141 Current risk Maklous, Triggers 1 of 51 rules 2.11.0.91 Current risk Maklous, Triggers 1 of 51 rules	I.11.11.11 Current risk Malcious, Triggers 5 of 51 nules 08 33.104.239 Current risk Malcious, Triggers 2 of 51 nules 66 3.88.21.03.8 Current risk Malcious, Triggers 2 of 51 nules 67 4.67.17 Current risk Malcious, Triggers 2 of 51 nules 66 4.82.11 Current risk Malcious, Triggers 2 of 51 nules 66 4.82.11 Current risk Malcious, Triggers 2 of 51 nules 66 4.82.11 Current risk Malcious, Triggers 2 of 51 nules 66 4.82.2 Current risk Malcious, Triggers 2 of 51 nules 66 4.82.4 Current risk Malcious, Triggers 1 of 51 nules 66 2.80.44 Current risk Malcious, Triggers 1 of 51 nules 66 2.22.4141 Current risk Malcious, Triggers 1 of 51 nules 66 2.11.091 Current risk Malcious, Triggers 1 of 51 nules 66	Littititi Current risk: Makicinus, Triggers 2 of 51 rules Od Edder 30.104.239 Current risk: Makicinus, Triggers 2 of 51 rules Od Edder 31.014.239 Current risk: Makicinus, Triggers 2 of 51 rules Od Edder 31.014.230 Current risk: Makicinus, Triggers 2 of 51 rules Od Edder 31.014.230 Current risk: Makicinus, Triggers 2 of 51 rules Od Edder 31.01 Current risk: Makicinus, Triggers 2 of 51 rules Od Edder 34.02.31 Current risk: Makicinus, Triggers 1 of 51 rules Od Edder 34.02.41 Current risk: Makicinus, Triggers 1 of 51 rules Od Edder 23.01.041 Current risk: Makicinus, Triggers 1 of 51 rules Od Edder

20.1 Importing data

Importing Recorded Future data into LogICA5 is done with three tasks that can be configured with the scheduler:

The Recorded Future - B Gest	ión Cuadros de Mar	ndo ▼ 🐵 Eventos TR ▼ 🖩 Regl	as 🔹 🧿 Planificación de Tareas 🕶						
Calendario de Tai	reas con eje	cución planificada							
🎁 Tabla de Tareas								+ 0 🛍	2
RECORDED FUTURE	~	Todas las tareas	V Q Buscar					Mostrar 2	25 🗸
		Todas las tareas							
Nombre		Ejecutar Cache de Dominios Recorde		Expresión 🔶	Programado	🕴 Estado 🍦	Acciones		
Ejecutar Cache de IP Recorded Future		Ejecutar Cache de IP Recorded Futur Ejecutar Cache de URL Recorded Fut		On Demand	No	error	e 🕨	/ 8	
		RECORDED FUTURE Elecutar	Cache de Dominios Recorded Future	On Demand	No	error	2		

These three tasks update the IPs, Domains and URLs data. The imported data is used as a cache to be used later in correlation rules or actions. If any search in this data is not successful, the remote query to the Recorded Future API is used instead.

20.2 Query data

Once the data cache is updated, we can consult them by accessing the Recorded Future menu option.

We can classify them by the level of evidence and perform searches for certain IPs, Domains or URLs.

Gestión Cuadros de Mando - 🏶 Eventos TR - 🖩 Reglas -			
Gestión Cuadros de Mando 👻 🏙 Eventos TR 👻 🖩 Reglas 🕶			
re			
Búsqueda por IP Min Evidencia	a Max Evide	encia	Q Buscar
			Mostrar 10 Y De 15
Descripción	Evidencia	Detalle	+ Acciones
Current risk: Malicious.Triggers 5 of 51 rules	68	true	× 🖬
Current risk: Malicious.Triggers 2 of 51 rules	100	false	
	00	Talse	· 🖬 🕨
Current risk: Malicious.Triggers 3 of 51 rules	67	false	
Current risk: Malicious.Triggers 3 of 51 rules Current risk: Malicious.Triggers 2 of 51 rules	67 65		
	65 65	false	~ D >
Current risk: Malicious.Triggers 2 of 51 rules	65 65 65 65	false false	 I I
Current risk: Malicious.Triggers 2 of 51 rules Current risk: Malicious.Triggers 2 of 51 rules	65 65 65 65 65	false false true	~ D
Current risk: Malicious.Tréggers 2 of 51 rules Current risk: Malicious.Tréggers 2 of 51 rules Current risk: Malicious.Tréggers 1 of 51 rules	65 65 65 65 65 66	false false true false	 2 2 2 2 2 2 4 2 4 4<
Current risk: Malicious.Treggers 2 of 51 rules Current risk: Malicious.Treggers 2 of 51 rules Current risk: Malicious.Treggers 1 of 51 rules Current risk: Malicious.Treggers 1 of 51 rules	65 66 66 66 66 66 66 66	false false true false false	
	Descripción Current risk: Malicious.Triggers 5 of 51 rules	Búsqueda por IP Min Evidencia Max Evide Descripción Evidencia Current risk: Malicious:Triggers 5 of 51 rules	Búsqueda por IP Min Evidencia Max Evidencia Max Evidencia Descripción Evidencia Videncia Detalle Current risk: Malidous:Triggers 5 of 51 rules

Each entry in the table can be consulted on the Recorded Future page by clicking on the icon

We can also observe the detail information of the entry by displaying the element with

ulo	Descripción		Evidencia	Detalle	Acciones
11.11.11	Current risk: Malicious.Trig	ggers 5 of 51 rules	68	true	~
P Address 81.11.11.	11				
otal Referencias: 183		5 1 1 4 A	Riesgo A	ctual: Unusual	
rimera referencia rec	opilada: 23 Ago 2017		Puntuac	ión de Riesgo: 5	
lltima referencia reco	pilada: 19 Jul 2020	5 %	1 of 53 F	Risk Rules currently observ	ved.
GEO: Germany, Europe		Contra State			
Unusual					
Historically Link		thods: Malware Packer, FakeAntivirus, NSAnti, Most recent N3DC88b9bd1d1c7a4d26bded8a9ffe6ff511ec3561fedc9ee1			24 Jun 2
Historically Link	e: ReversingLabs. 3 related intrusion me				24 Jun 2
Historically Link: 5 sightings on 1 source https://a1000.reversion étricas steHits: 0	e: ReversingLabs. 3 related intrusion me	darkwebHits: 0	d6646df0f5669ec3e trendVc		24 Jun 2
Historically Link. s sightings on 1 source stips://a1000.reversion étricas steHits: 0 sitlistedCount: 0	e: ReversingLabs. 3 related intrusion me	%30c88b9bd1d1c7a4d26bded8a9ffe6ff511ec3561fedc9ee1 darkWebHits: 0 criticality: 1	d6648df0f5669ec3e trendVc linkedtr	ntrusion: 1	24 Jun 2
Historically Link sightings on 1 source https://a1000.reversin étricas steHits: 0 hitlistedCount: 0 blicSubscore: 5	: ReversingLabs. 3 related intrusion me glabs.com/accounts/login?next=/№3Fqt	k3Dc88b9bd1d1c7a4d26bded8a9ffe6ff511ec3561fedc9ee1 darkWebHits: 0 criticality: 1 undergroundForumHits: 0	d6646df0f5669ec3e trendVc linkedir malicio	ntrusion: 1 usHits: 1	24 Jun 2
Historically Link 5 sightings on 1 source https://a1000.reversin	: ReversingLabs. 3 related intrusion me glabs.com/accounts/login?next=/№3Fqt	%30c88b9bd1d1c7a4d26bded8a9ffe6ff511ec3561fedc9ee1 darkWebHits: 0 criticality: 1	d6648df0f5669ec3e trendVc linkedtr	ntrusion: 1 usHits: 1 is: 183	24 Jun 2

This information can be expanded by consulting Recorded Future directly by pressing the button \blacktriangleright .

20.3 Apply Recorded Future Actions

>_

The query for obtaining information on threats can be executed from the LogICA5 log and event data panels. We select the fields that we want to analyze, either domains, IPs or URLs and click on the Actions icon:

LogICA							• •			
		Ejecutar acción								0
	Li			_						0
		Acción		· •						
			Ping Whois				_	(in the second se	r Columnas 🔶 Se	
			Port Scan				errar	B umpla	r coumnas	ieccionar Columnas
			Nmap Blacklist				_			
	Panel de elecuci		Whitelist integrationITOP							
	Panel de ejecuci		Insert into Mongo Collection Test						□ ▼ >_ Q	Q < 101 (
	T Filtrar		IgnoreCVE Related Log Lines							
	- 1		IP Threat Detail (Event) IP Threat Detail							
	Cola	Conjunto	URL Threat Detail (Event)	Even	Evento	Fecha	Hora	Mensaje base	Origen: IP	Origen: Nom
	1 DEFAULT	r - 19	 Domain Threat Detail (Event) Threat Check (Event) 		PASS_ERR	2020-10-01	15:22:00		5.30.104.239	

A window is displayed in which we can select the action to apply.

If we select "IP Threat Detail (Event)", the Recorded Future query of the IP selected in the panel is executed. If data is obtained, it is shown in detail:

LogICA	=				0 U	≣ 0	a =	ъ 🚨	admin 🗝 💡
SUALIZACIÓN	Descrip	Ejecutar acción						0	
Cuadros de Mando									
Seguimiento de Incidentes								ä	
Gestión de Informes		Acción IP Th	reat Detail	× 🔲 🕨				ō	
DMINISTRACIÓN	Li							0	
9 Planificación de Tareas									
Visor de Riesgo 🤇		IP Threat Detail Obtains information details about				9.10		+ Seleccio	nar Columnas
i Gestión de Agentes <		Obtains information details about	threats and risk of this IP address						
0 Gestión Vulnerabilidades 🥠		Parámetros							
D Auditoria Interna SIEM ·	Panel de elecuci	Consola Detalles direccion	IP)_ Q Q	- 0.5
Monitorización		Entidad	Tipo	Acciones				~ ~ ~	
Recorded Future	T Filtrar	5.30.104.239	IpAddress	~ 2					
DNFIGURACIÓN	Cola					Mensaje bas	se Origen	- 18 0	rigen: Nombi
🖇 Configuración Plataforma 🛛 🤇	D 1 DEFAULT	5.30.104.239			20	-	5.30.10		
Control Correlación		Primera referencia recopilada	a: 16 Ene 2020						
a Configuración Seguridad <		Última referencia recopilada:	24 Ene 2020						
L Configuración de Activos <		ASN: AS15802	ORG: Emirates Integrated Tel	ecommunications Company PJSC (EITC-DU)					
Conf. Parámetros Riesgo		GEO: , United Arab Emirates,							
		G	Unusus Risk so 2 of 53						
	GRUPO ICA © 2020	Reglas de Riesgo Deseno	adenadas		_		Log	CA - Gestión I	Eventos Seguridad