RETAIL & HOSPITALITY ISAC

FOSStering an ISAC: Enabling a Community with Open-Source Tools

JJ Josing – Principal Threat Researcher, RH-ISAC

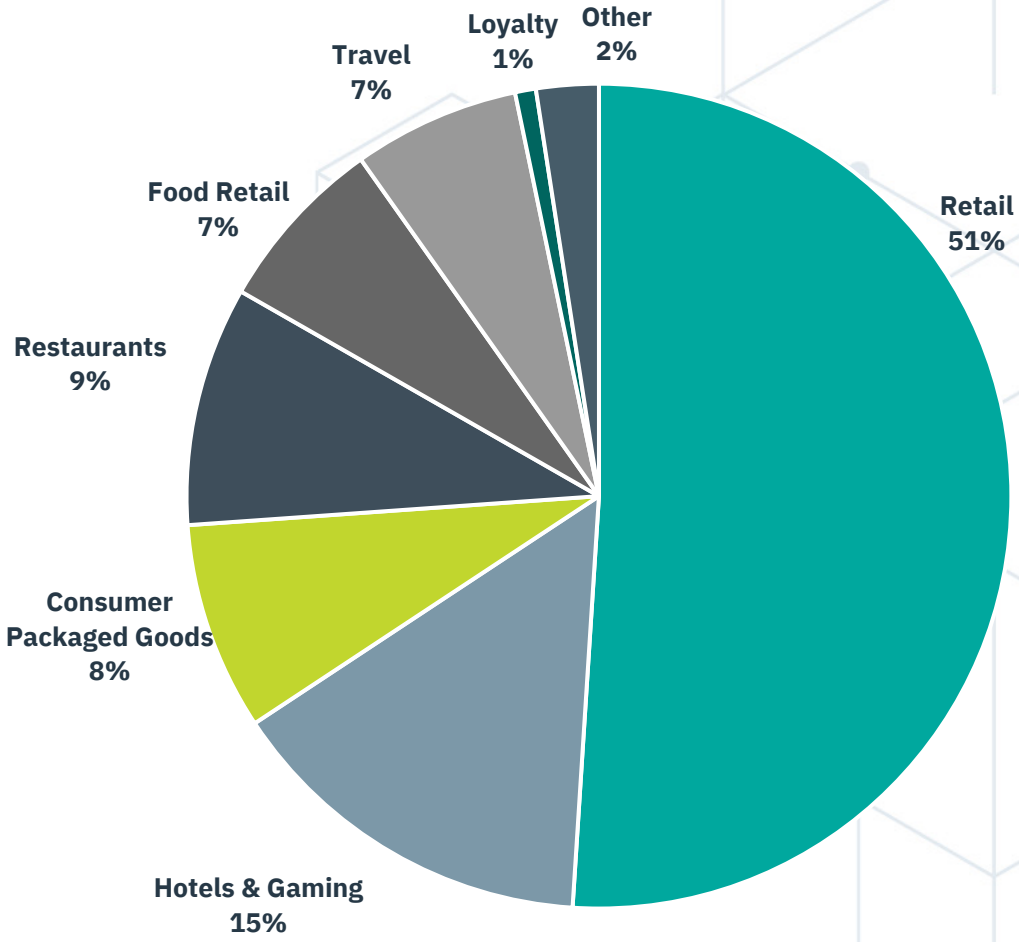
Agenda

- ✓ What is RH-ISAC?
- ✓ Architecture Overview
- ✓ Community Usage
- ✓ RH-ISAC Classification Taxonomy
- ✓ RH-ISAC Galaxies
- ✓ Intel Sharing and Normalization
- ✓ Enriching and Vetting Attributes
- ✓ Intel Interoperability
- ✓ What's Next?

What is RH-ISAC?

Retail & Hospitality Information Sharing & Analysis Center

A secure place for consumer-facing companies to share cybersecurity information and intelligence to not only protect their own companies, but to also strengthen the entire sector — a rising tide lifting all boats



251 Member Companies
3,100+ Member Users

What is RH-ISAC?

Security Collaboration Groups

- ✓ Dark Web
- ✓ Fraud
- ✓ Gift Card Fraud
- ✓ Identity & Access Management
- ✓ Incident Response
- ✓ Operational Technology
- ✓ Risk Management
- ✓ Security Awareness
- ✓ Third-Party Risk Management
- ✓ Vulnerability Management

Tools-Based Groups

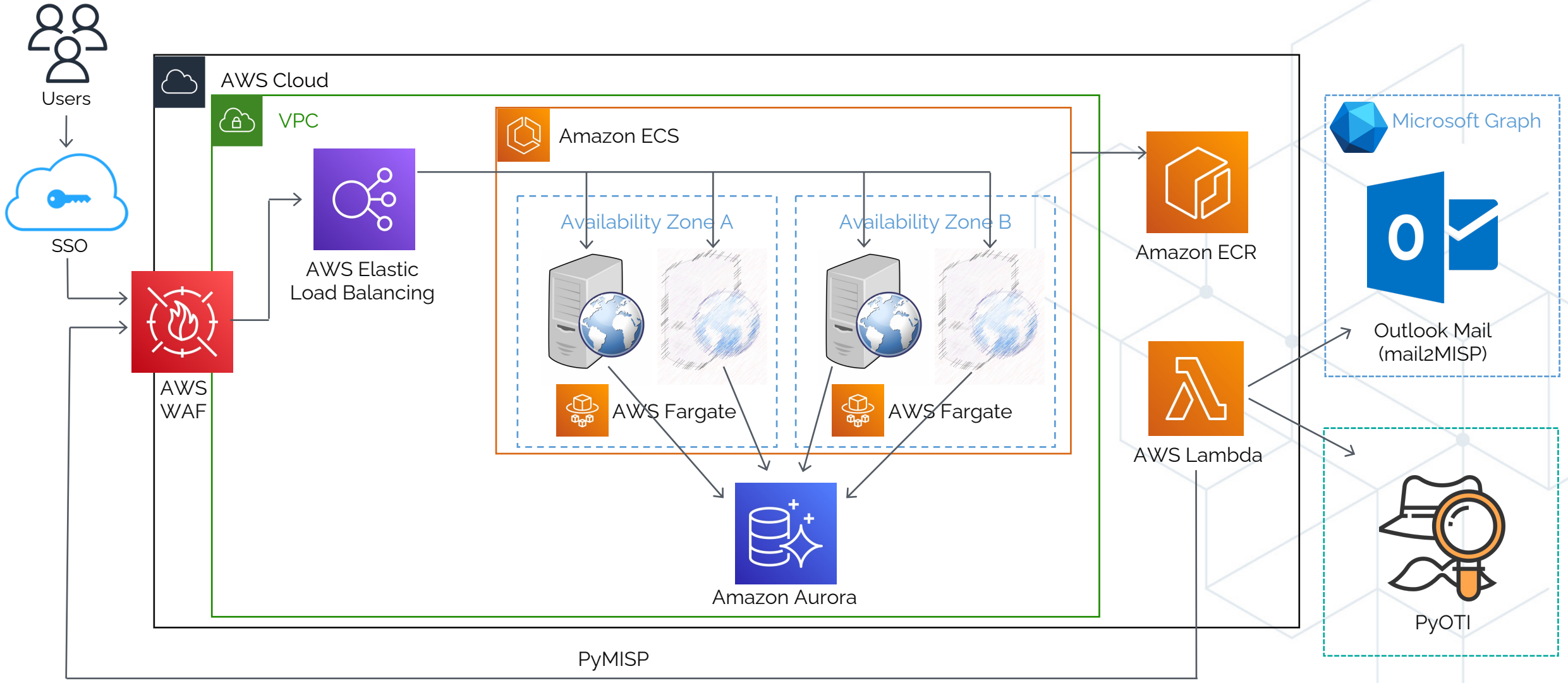
- ✓ Crowdstrike EDR
- ✓ MISP
- ✓ SOAR
- ✓ Splunk

Special Interest Groups

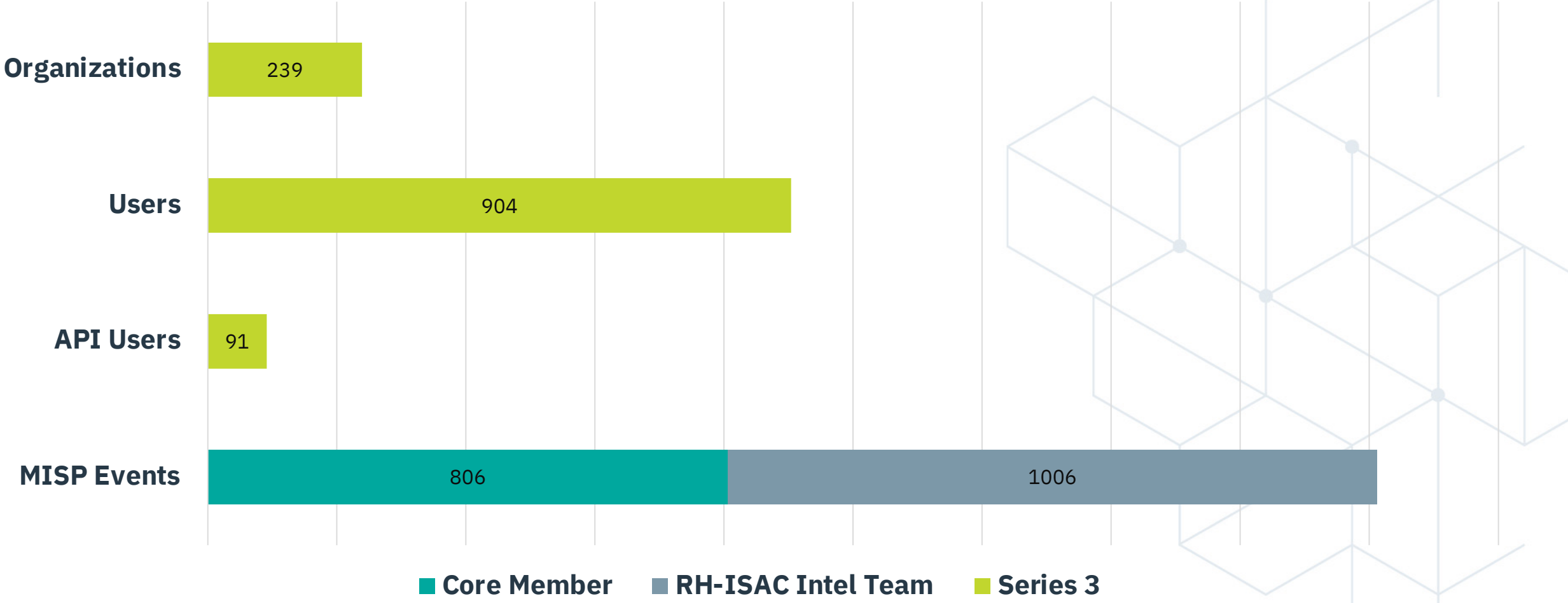
- ✓ Analyst Community
- ✓ BISO Community
- ✓ CISO Community
- ✓ Industry Sector
- ✓ Small Cyber Teams


EXCUSE ME
RETAIL & HOSPITALITY ISAC
MISP
DO YOU HAVE A MOMENT TO TALK ABOUT WHAT THINGS ARE POSSIBLE THROUGH MISP

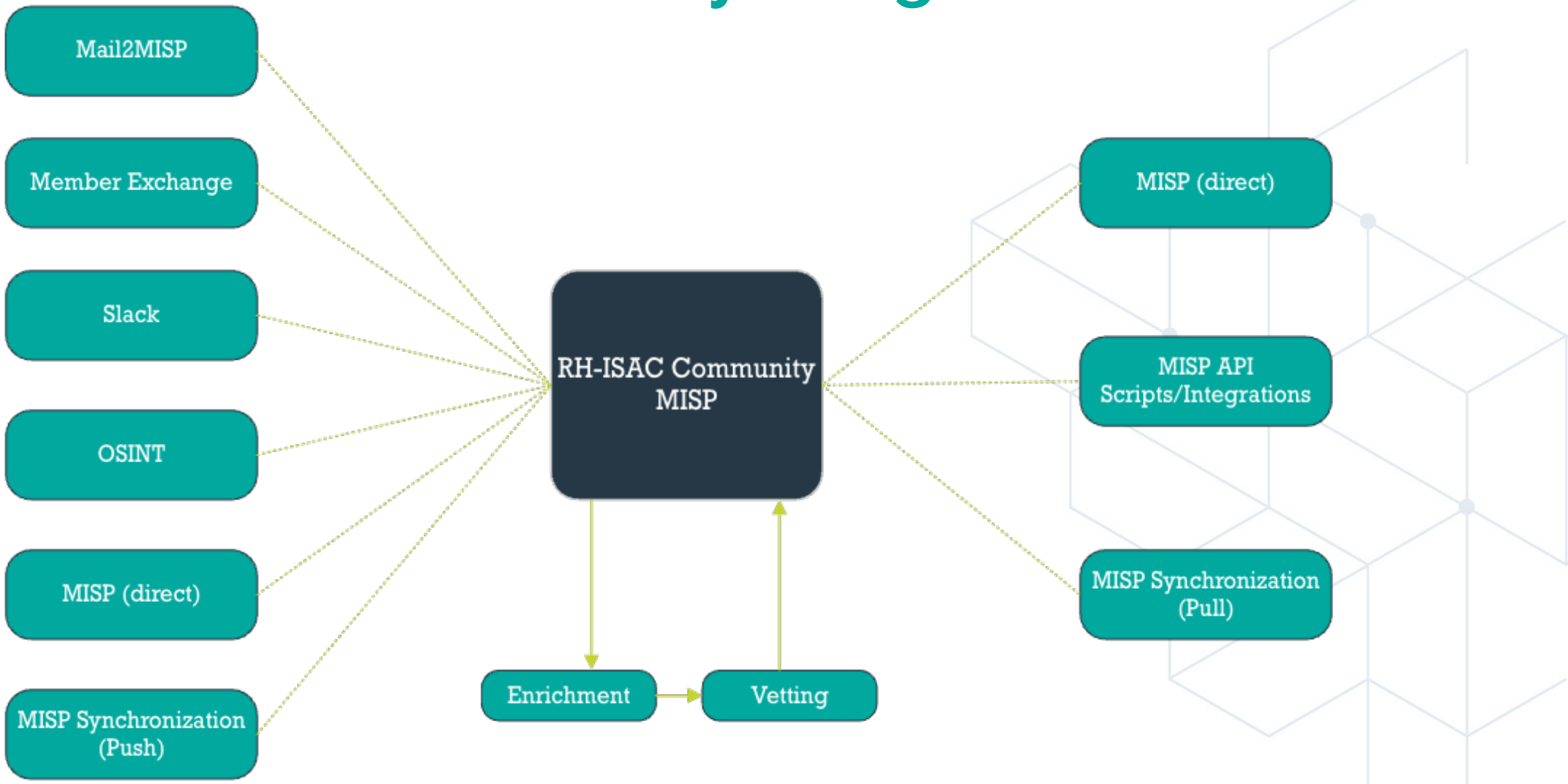
Architecture Overview



Community Usage



Community Usage



RH-ISAC Classification Taxonomy

Intel Source

- rhisac:intel-source="mail2misp"
- rhisac:intel-source="member-exchange"
- rhisac:intel-source="misp"
- rhisac:intel-source="misp-sync"
- rhisac:intel-source="osint"
- rhisac:intel-source="slack"

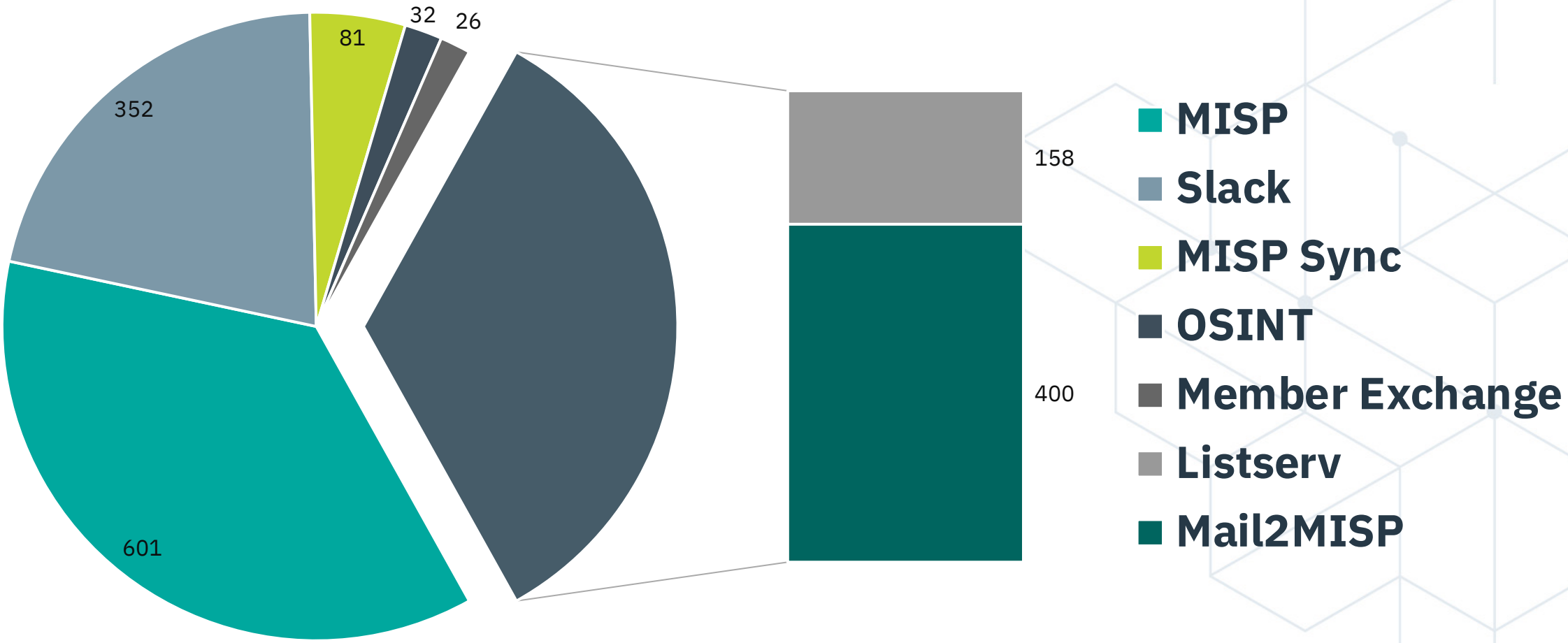
Member Industry

- rhisac:member-industry="consumer-packaged-goods"
- rhisac:member-industry="food-retail"
- rhisac:member-industry="gaming"
- rhisac:member-industry="hospitality"
- rhisac:member-industry="loyalty"
- rhisac:member-industry="restaurants"
- rhisac:member-industry="retail"
- rhisac:member-industry="travel"

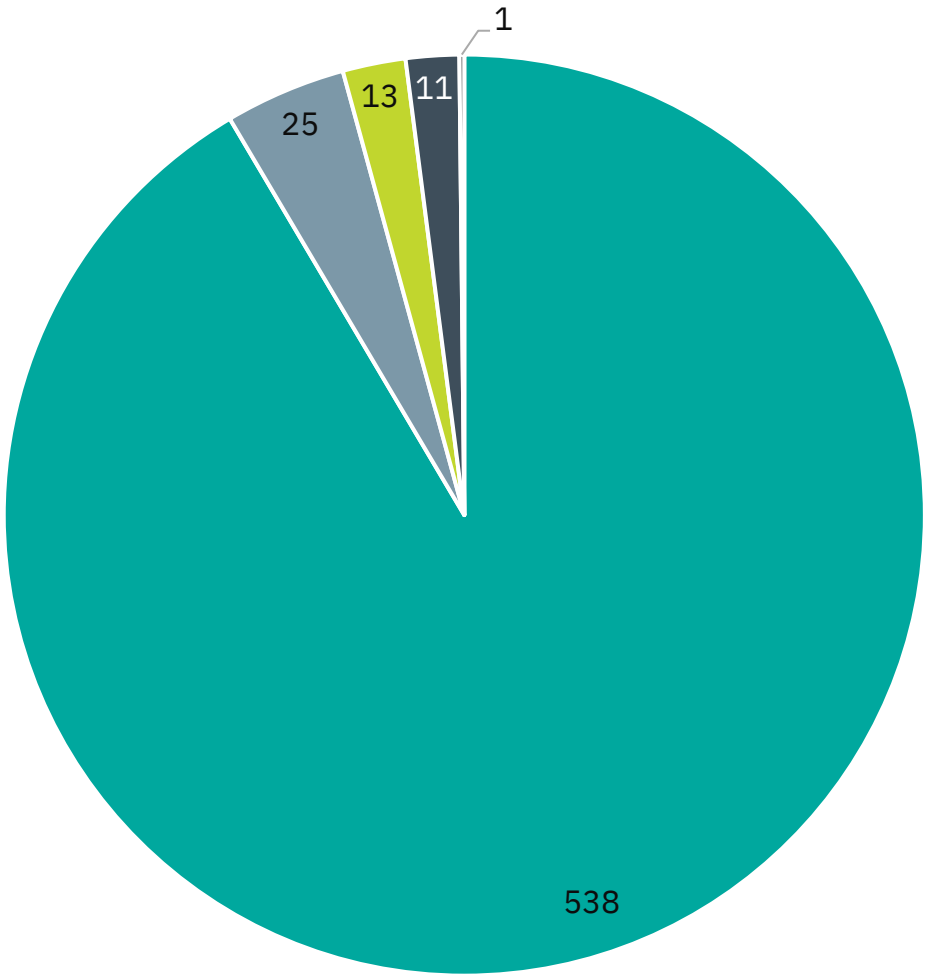
Threat Type

- rhisac:threat-type="ransomware"
- rhisac:threat-type="reconnaissance"
- rhisac:threat-type="rootkit"
- rhisac:threat-type="smishing"
- rhisac:threat-type="spyware"
- rhisac:threat-type="supply-chain-compromise"
- rhisac:threat-type="trojan"
- rhisac:threat-type="vishing"
- rhisac:threat-type="vulnerability"
- rhisac:threat-type="whaling"
- rhisac:threat-type="wiper"
- rhisac:threat-type="worm"

Intel Source

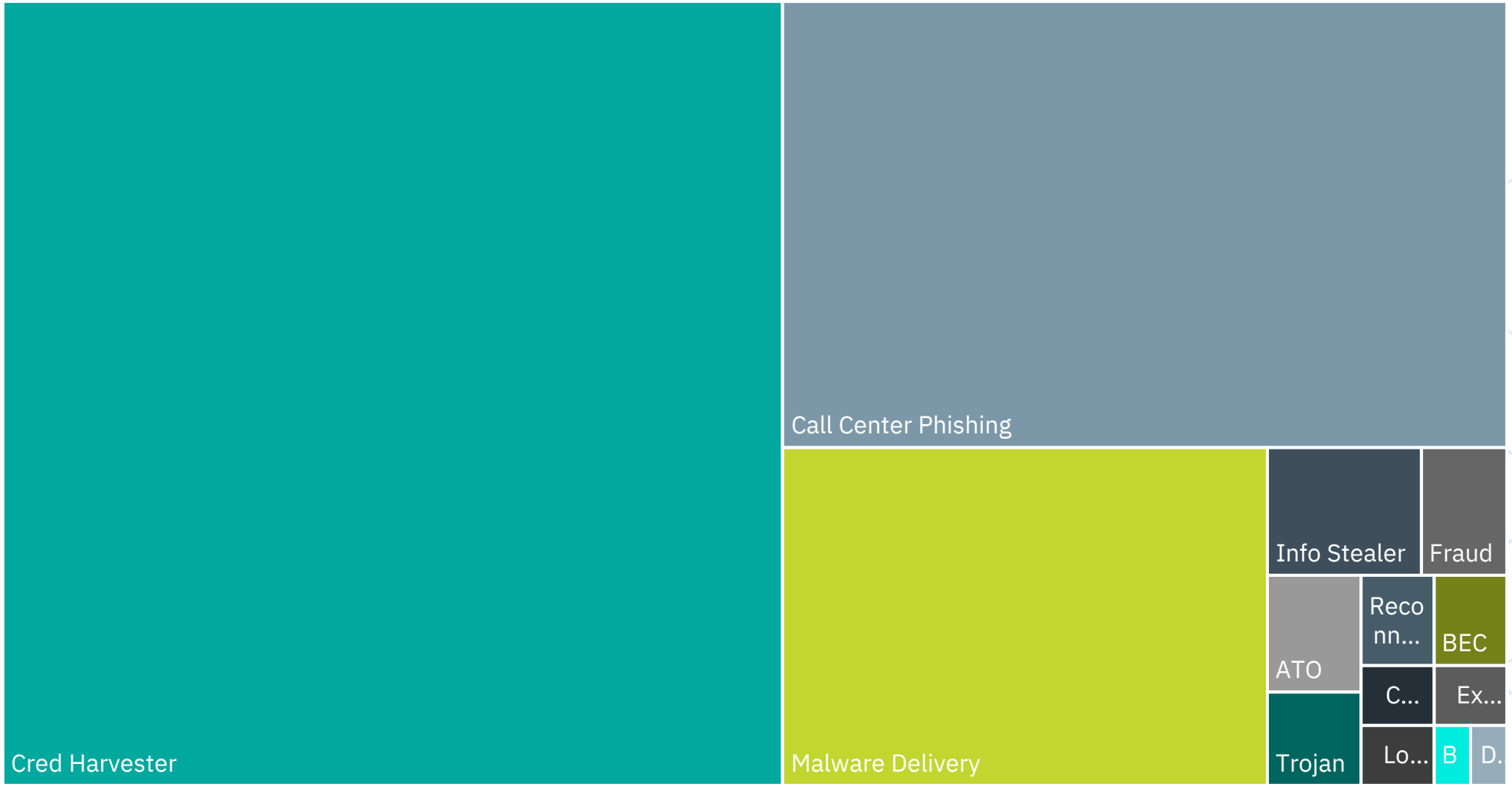


Member Industry



- Retail
- Hospitality
- Consumer Packaged Goods
- Travel
- Gaming

Threat Type



- Cred Harvester
- Call Center Phishing
- Malware Delivery
- Info Stealer
- Fraud
- ATO
- Trojan
- Reconnaissance
- BEC
- CVE Exploit
- Loader Malware
- Executive Impersonation
- Brute Force
- Digital Skimmer

RH-ISAC Galaxies

Threat Actors Galaxy

- ✓ Cataloguing the most prominent and prolific threat groups targeting our community as a resource for member analysts.

Fraud Galaxy

- ✓ Knowledge base for the numerous fraud types that affect RH-ISAC members that can be used to enable them, regardless of team size or budget, to combat fraud.

RH-ISAC Fraud Galaxy Preview

RH-ISAC Fraud galaxy

Galaxy ID	67
Name	RH-ISAC Fraud
Namespace	RH-ISAC
UUID	1c71b253-9769-4f55-8692-a18d1e2ec4b4
Description	Knowledge base of numerous fraud types that affect RH-ISAC members
Version	3
Local Only	No

Kill chain order

« previous | next »

All | Default | Custom 0 | My Clusters | Deleted | View Fork Tree | View Galaxy Relationships

Enter value to search | Filter

ID	Published	Value	Synonyms	Owner Org	Creator Org	Default	Activity	#Events	#Relations	Description	Distribution	Actions
170414	N/A	Bonus Abuse		MISP	MISP	✔		0	0 0	The numerous fake accounts benefit from new signup bonuses, coupons and other attractive offers. While these promos are an excellent way to attract new players, they can quickly make your platform run at a loss if you hand out too many of them.	All	
170418	N/A	Booking Fraud		MISP	MISP	✔		0	0 0	A type of fraud targeting hospitality room and/or trip booking systems. Booking fraud can target customers with fraudulent opportunities or target businesses either using stolen customer credentials or demanding refunds.	All	
170428	N/A	Bricking		MISP	MISP	✔		0	0 0	Returning items after stripping valuable components.	All	
170407	N/A	Cancellation		MISP	MISP	✔		0	0 0	A type of fraud leveraging loyalty points, rebooking from a fraudulent travel agent account to collect commissions, or rebooking through cashback sites.	All	
170429	N/A	Card Not Present (CNP)		MISP	MISP	✔		0	0 0	A type of credit card scam in which the customer does not physically present the card to the merchant during the fraudulent transaction.	All	
170415	N/A	Chip Dumping		MISP	MISP	✔		0	0 0	Another fraudulent practice at the poker table. Like with gnoming, the idea is to make multiple accounts join the same table in order to cheat the system and influence the results in favor or against one particular player.	All	
170422	N/A	Credit Card Validation		MISP	MISP	✔		0	0 0	The act of checking credit cards to identify valid cards that can be used to commit fraud.	All	
170410	N/A	Cross-Retailer Fraud		MISP	MISP	✔		0	0 0	Buying items at lower price in one store and returning to a store for a higher return value.	All	

RH-ISAC Fraud Galaxy Preview

Booking Fraud	Card Not Present (CNP)	Gaming Fraud	Loyalty Fraud	Physical Gift Card Tampering	Receipt Fraud	Site Automation Attacks
Booking Fraud	Card Not Present (CNP)	Bonus Abuse	Loyalty Fraud	Physical Gift Card Tampering	Bricking	Credit Card Validation
Cancellation		Chip Dumping			Cross-Retailer Fraud	Digital Skimming
Employee Rate Targeting		Gaming Fraud			Employee Fraud	Gift Card Validation
Fake Events		Gnoming			Empty Box Fraud	Spoofed Gift Card Sites
No Show		Multi-Accounting			Open Box Fraud	
		Top Up Abuse			Price Arbitage	
					Receipt Fraud	
					Return Fraud	
					Switch Fraud	
					Triangulation	
					Wardrobing	

RH-ISAC Fraud Galaxy Preview

RH-ISAC Fraud :: Digital Skimming

Cluster ID	170421
Name	Digital Skimming
Parent Galaxy	RH-ISAC Fraud
Description	Threat actors stealing user data by injecting malicious JavaScript into a e-commerce website. Threat actor typically injects malicious code via three vectors: • Using legitimate admin credentials, either stolen, bought, guessed or brute forced • Exploiting vulnerabilities in e-commerce software or operating systems • Software supply chain attack to compromise a third-party JavaScript library used by e-commerce software.
Default	Yes
Version	1
UUID	90f2a981-46b1-4d3f-9611-b49f4ae96cb6
Collection UUID	c5be9f83-832e-46b8-a808-f516ea15da83
Source	RH-ISAC Intel Team, RH-ISAC Community, and OSINT
Authors	RH-ISAC Intel Team
Distribution	All communities
Owner Organisation	MISP
Creator Organisation	MISP
Connector tag	misp-galaxy:rhisac-fraud="Digital Skimming"
Events	0

RH-ISAC Fraud Galaxy Preview

Tabular view | JSON view

Key	Value
kill_chain	rhisac-fraud-tactics:Site Automation Attacks
member-industries-targeted	Retail
member-industries-targeted	Hospitality
member-industries-targeted	Travel
member-industries-targeted	Gaming
mitigation	Scan for vulnerabilities regularly
mitigation	Take inventory of your attack surface
mitigation	Regularly perform site content audits
mitigation	Follow web application security best practices
mitigation	Conduct frequent penetration tests for e-commerce applications

Page 1 of 1, showing 10 records out of 10 total, starting on record 1, ending on 10

Intel Sharing and Normalization – Sharing Templates

Credential Harvester – Phishing Link: A template for sharing credential harvester phishing link intel.

Phishing Attribution	
Sender:	
Reply-to:	
Subject:	
Email Source IP:	
Email Body (text):	
Threat Actor:	

Embedded Links: The malicious URL in the e-mail body. (one per row)

Redirect URL: The redirect URL, if any, from the malicious link. (one per row)

Credential POST: The domain, hostname, IP, or URL where credentials are posted. (one per row)	
IOC Type (domain, hostname, IP, or URL):	IOC Value:

Research Links: A link to an external analysis. VirusTotal, urlscan, any.run, etc. (one per row)

- ✓ **MISP Templates**
- ✓ **Mail2MISP**

Intel Sharing and Normalization – Mail2MISP

- ✓ Using fork of mail_to_misp
- ✓ Connecting email infrastructure to MISP
- ✓ Replaces old Listserv

https://github.com/MISP/mail_to_misp

Intel Sharing and Normalization – MISP Objects

- ✓ spearphishing-link
- ✓ spearphishing-attachment
- ✓ cs-beacon-config

Intel Sharing and Normalization – Documentation

PDF Documents

- ✓ Accessing the RH-ISAC MISP
- ✓ Generating an AuthKey
- ✓ Syncing MISP Instances
- ✓ MISP Intel Sharing Template
- ✓ Delegated Sharing
- ✓ Tags in the RH-ISAC Community MISP Instance

Video Tutorials

- ✓ How to Access RH-ISAC MISP
- ✓ How to Generate an AuthKey
- ✓ How to Create an Event
- ✓ How to Add Attributes to an Event using Sharing Templates
- ✓ How to Add Attributes to an Event using Freetext Parsing
- ✓ How to Add Individual Attributes to an Event

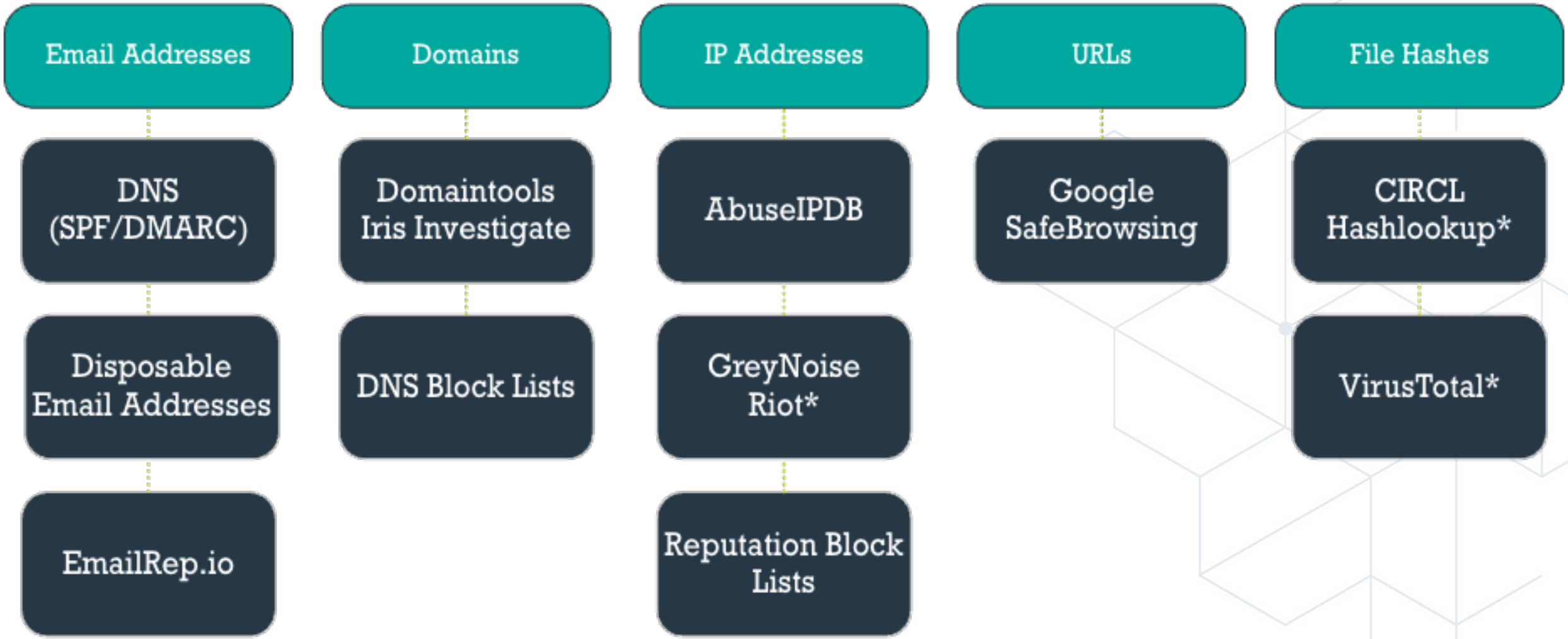
Enriching and Vetting Attributes – PyOTI

- ✓ Python Open Threat Intelligence
- ✓ Modular Framework
- ✓ Standardizes Disparate Intel APIs

https://github.com/RH-ISAC/PyOTI

https://github.com/MISP/misp-taxonomies/tree/main/pyoti

Enriching and Vetting Attributes – Services Used



Enriching and Vetting Attributes – Enrichment Tags

Cobalt Strike Beacon Uploaded to VT and Config extracted daily batch for 2023-10-10

Event ID	4863
UUID	4e31dfb6-70b7-59e2-9411-78c560fd0631
Source Organisation	[redacted]
Member Organisation	
Creator user	
Protected Event (experimental)	Event is in unprotected mode.
Tags	RHISAC misp x enriched x TLP green x malware_intelligence x malware_cobaltstrike x
Date	2023-10-09
Threat Level	Medium
Analysis	Completed
Distribution	This community only
Published	Yes 2023-10-11 14:24:30
#Attributes	77 (10 Objects)

Enriching and Vetting Attributes – Enrichment Tags

2023-10-11	**Object name:** cs-beacon-config **References:** 0				
2023-10-11	Payload delivery	**md5:** md5	842eaae1b1774977d0622754b69752b9	trojan.beacon/cobaltstrike x rhisac: vetted x	md5 of sample containing the cobaltstrike shellcode
2023-10-11	Payload delivery	**sha1:** sha1	72dbccf144158f90be0df3321d4fc6f7973b0d19	trojan.beacon/cobaltstrike x rhisac: vetted x	sha1 of sample containing the cobaltstrike shellcode
2023-10-11	Payload delivery	**sha256:** sha256	11be9f485f787b0856b584aa3ba05d8eda71029be9fa1c47a72e267273a54784	trojan.beacon/cobaltstrike x rhisac: vetted x	sha256 of sample containing the cobaltstrike shellcode
2023-10-10	Network activity	**c2:** url	1.14.45.126/push		This sample communicates with this C2
2023-10-11	External analysis	**jar-md5:** md5	b50b86d735412685eb6044ad8d01781c	java x rhisac: vetted x	md5 of adversary cobaltstrike.jar file
2023-10-10	Other	**watermark:** text	175065ea		This is the watermark of the sample
2023-10-11	External analysis	**vt-sha256:** sha256	11be9f485f787b0856b584aa3ba05d8eda71029be9fa1c47a72e267273a54784	trojan.beacon/cobaltstrike x rhisac: vetted x	sha256 of sample uploaded to VT

Enriching and Vetting Attributes – Enrichment Tags

(TLP:GREEN) IPs Associated with Malicious SMTP Authentication Attempts, 8-15 June 2023

Event ID	4111
UUID	96911755-0941-41b6-97d1-b7ed871e7576
Source Organisation	[redacted]
Member Organisation	
Creator user	
Protected Event (experimental)	Event is in unprotected mode.
Tags	RHISAC enriched x misp x travel x ato x TLP green x
Date	2023-06-16
Threat Level	Low
Analysis	Completed
Distribution	This community only
Published	Yes 2023-06-20 17:21:43
#Attributes	8 (0 Objects)
First recorded change	2023-06-16 19:30:48

Enriching and Vetting Attributes – Enrichment Tags

Date	Category	Type	Value	Tags
2023-06-17	Network activity	ip-src	58.187.66.179	pyoti:reputation-block-list="spamhaus-pbl" x pyoti:reputation-block-list="barracudacentral-brbl" x rhisac: vetted x
2023-06-17	Network activity	ip-src	2.57.171.18	pyoti:abuseipdb="low" x
2023-06-17	Network activity	ip-src	103.251.167.20	pyoti:abuseipdb="high" x pyoti:reputation-block-list="spamhaus-xbl" x pyoti:reputation-block-list="spamcop-scbl" x rhisac: vetted x
2023-06-17	Network activity	ip-src	105.155.36.94	pyoti:reputation-block-list="spamhaus-pbl" x rhisac: vetted x
2023-06-17	Network activity	ip-src	137.117.254.184	pyoti:abuseipdb="medium" x
2023-06-16	Network activity	ip-src	4.236.143.88	
2023-06-16	Network activity	ip-src	2a03:75c0:3c:af24:bc98::1	
2023-06-16	Network activity	attachment	CTI-TIR-0040-23-TL.txt	

Intel Interoperability - Integrations

One Click Apps

Install App → Generate API Key → Configure App w/Key, Tag, and Server → Tweak as Needed

Custom Scripts

Install App → Generate API Key → Configure App w/Key, Tag, and Server → Tweak as Needed

- ✓ Integrations with 17 named platforms
- ✓ Several custom or one-off integrations
- ✓ Several more currently in the works

- ✓ Splunk
- ✓ CrowdStrike
- ✓ Chronicle
- ✓ Defender for Endpoint
- ✓ Azure Sentinel
- ✓ IntSights
- ✓ IronPort
- ✓ NetSkope
- ✓ SecureX
- ✓ MISP
- ✓ XSOAR
- ✓ Polarity
- ✓ ThreatConnect
- ✓ ThreatQ
- ✓ Anomali ThreatStream
- ✓ OpenCTI
- ✓ CTIX

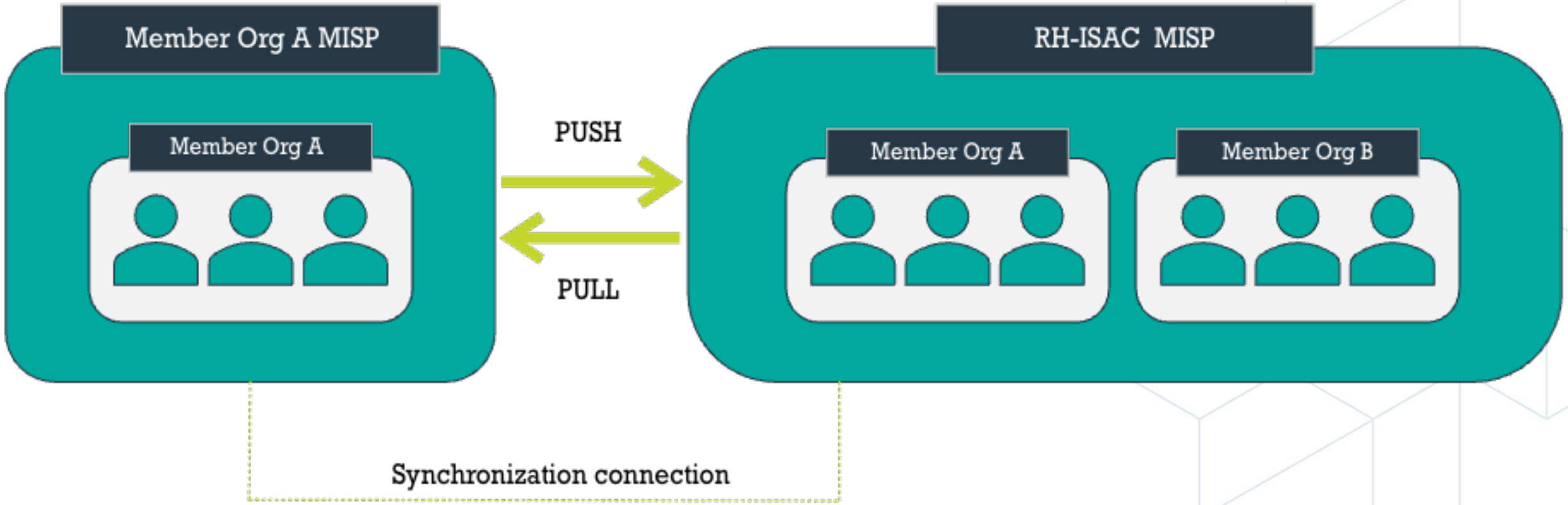
Intel Interoperability – RH-ISAC Integrations

- ✓ Splunk
- ✓ Microsoft Graph API
- ✓ Crowdstrike
- ✓ Generic Scripts

https://github.com/RH-ISAC/intel-integrations/tree/main/misp

Intel Interoperability – 3rd Party Integrations

Intel Interoperability – MISP Sync



What's Next?

- ✓ MISP Workflows
- ✓ MISP Warninglists
- ✓ More contributions to the MISP community

Questions?

circl.lu
Computer Incident Response Center
LUXEMBOURG

MISP
Threat Sharing

Do you work for a consumer-facing organization and are interested in membership?

✓ **https://rhisac.org/join**

#ProtectAsOne