TLP:WHITE

2021 YEAR IN REVIEW

RETAIL & HOSPITALITY ISAC

"RH-ISAC's mission has never been more important as cyber threats rise across all sectors. Facing a pandemic, it would have been understandable for members to prioritize other needs and step back from the ISAC, but the opposite happened. RH-ISAC engagement is up and intelligence sharing is at an all-time high. This is truly a testament of the strong community we've built together, the power of collaboration, and the value that RH-ISAC brings to our members."

Rich Agostino
Senior VP & CISO
Target

Chair of the
RH-ISAC Board
of Directors

RETAIL & HOSPITALITY ISAC

TABLE OF CONTENTS

2021 HIGHLIGHTS

FEBRUARY
Published CISO Benchmark Report

MARCH
Workshop Series for 2021 kicked off at CVS Health

APRIL
Published Industry Trends Report (Accenture) and Enterprise Risk Assessment Benchmark (CyberGRX)

APRIL
Partnered with IBM Security for a cross-functional business exercise for CISOs and C-level executives

JUNE
Co-hosted first retail, hospitality, and travel industry-wide cybersecurity exercise with CISA

JULY
Hosted first virtual workshop for members in Asia-Pacific

JULY
Launched Intelligence and Engineering Advisory Group

SEPTEMBER
Hosted virtual Cyber Intelligence Summit

SEPTEMBER
Launched MISP at the Annual Summit

OCTOBER
Launched Best Practices Podcast

OCTOBER
Partnered with Security Innovation for inaugural Security Awareness Symposium

OCTOBER
Organized first-ever completely in-house mini-tabletop ATO exercise

NOVEMBER
Published joint report with Cofense on phishing programs across the industry

DECEMBER
Launched YARA Rules User Group

DECEMBER
Community responded to Log4j vulnerability

NUMBER OF INTELLIGENCE **REPORTS PUBLISHED**

252 **Daily Intelligence Reports**

This report provides tactical highlights of member sharing activity, cybersecurity news, threats impacting the retail and hospitality sectors, RH-ISAC Member Exchange updates, and various updates for RH-ISAC Core Members.

9 **Intelligence Summary Reports**

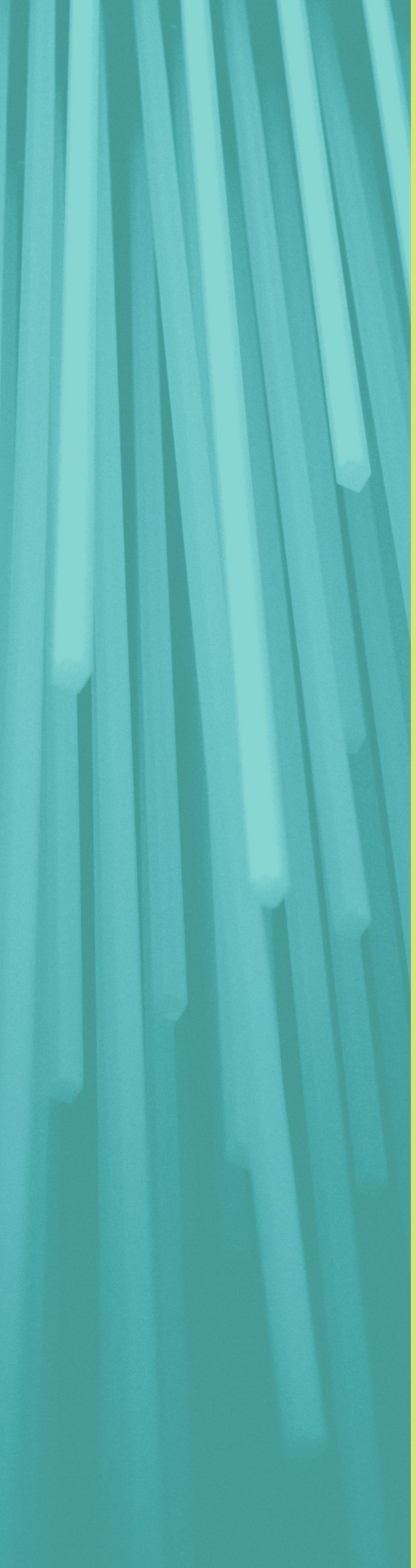
In response to the Log4j/Log4shell vulnerabilities announced in December 2021, RH-ISAC began producing intelligence summaries (INTSUMs), providing members with a threat intelligence product which served as a roll-up of recently shared relevant information, including RH-ISAC actions, as well as upcoming events related to the Log4j vulnerabilities. These INTSUMs were a central location for important developments, ensuring members could seamlessly remain up-to-date without the need to toggle back and forth between a variety of sharing platforms.

3 **Community Landscape Enterprise Analysis Reports (CLEAR)**

The CLEAR report analyzes the past four months of member-shared intelligence, supported by relevant content contributed from RH-ISAC Associate Members. The report is delivered in a succinct package so members can see not only what has been trending, but where those sharing trends have spiked, fallen off, etc.

3 **Out-of-Band and After-Action Reports**

Out-of-band reports are published on an 'as needed' basis to give our members additional context and boots-on-ground analysis, or to offer context and recap after an event. These reports provide additional resources to members for significant events that are likely to have a substantial impact on members of the RH-ISAC community.



77%
of members shared in 2021

17K
vetted IOCs shared 2021 YTD

127K
vetted IOCs shared since 2018

7,637
total shares across all sharing channels 2021 YTD

Top Trending Topics

1. Agent Tesla
2. Credential Harvester
3. MITRE/Initial-Access
4. Office 365
5. Phishing

> *"RH-ISAC's intelligence exchange provides a wealth of information that is timely, accurate, and applicable to my team's day-to-day work. RH-ISAC has become an extension of my own team – it enables us to improve our responses to cybersecurity threats, increase our professional development and education, and tackle challenging cybersecurity problems. We are able to source the community for best practices and gain a better understanding of threats to our environment."*

THREAT INTELLIGENCE & INFORMATION SHARING

Threat Intelligence

More than 17,000 vetted indicators of compromise (IOCs) were shared among Core Members in 2021, with 77% of all members actively sharing threat intelligence across the ISAC sharing channels.

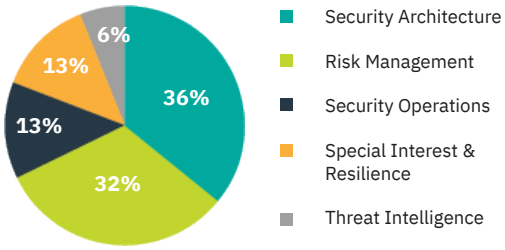
Member Exchange: Requests for Information

RH-ISAC's online community, Member Exchange, which launched in the fall of 2020, has become a popular tool for members to seek advice from peers in the form of Requests for Information (RFIs). RFIs allow members to share their expertise and exchange solutions to commonly shared challenges.

176 RFIs were shared across the CISO, Analyst, Security Awareness, and Identity and Access Management communities, which generated 571 responses.

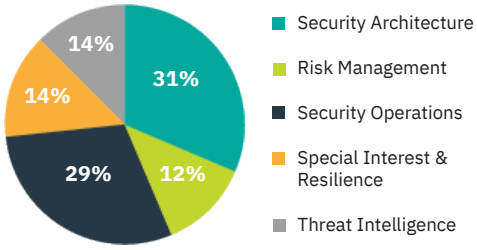
CISO RFIs

91 RFIs | 423 Responses



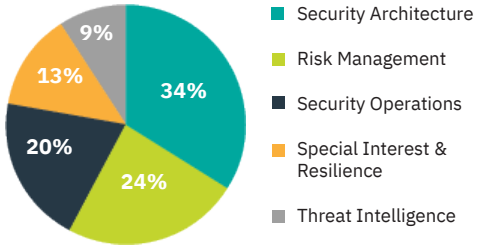
Analyst RFIs

80 RFIs | 140 Responses



Total RFIs

176 RFIs | 571 Responses



Threat Intelligence Briefings

195 individuals from 93 member companies attended the weekly intel calls. These calls allow members to share what they have recently been working on and any threats they have seen that may be relevant to other member companies.

47 individuals attended additional threat-intelligence-related meetings and fireside chats on topics including security operations, preparing for the holiday season, and vaccine administration.

Member-Specific Threat Alerts

RH-ISAC processes alerts from a number of sources and sends relevant alerts to specific members impacted by the intelligence. This service helps members identify and address potential security issues.

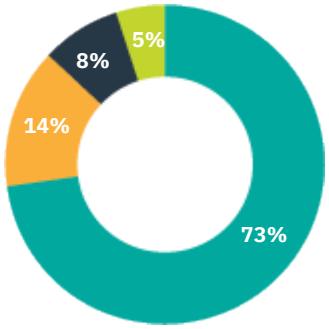
- Alerts Processed: 79,041 | Alerts Selected for Release: 5,478 | Notifications to Members: 726

Note: Emails often contain multiple alerts

WORKING GROUPS, COMMITTEES, & TASK FORCES

Contributions in 2021

80% of Core Member companies attended an RH-ISAC community meeting.



Benchmark Task Force: The Benchmark Task Force oversees key benchmark reports, such as the RH-ISAC|CyberGRX maturity benchmark and our premier CISO Benchmark Report. The CISO Benchmark Report is used by cybersecurity leaders to guide their budgeting and resource allocation decisions for the coming year.

Identity & Access Management: New in 2021, this group held multiple calls that explored how RH-ISAC members were focused on protecting both the enterprise and consumers. As a key element in organizations' efforts in both digital transformation and zero trust, the IAM/CIAM group will continue to share leading practices in this area in 2022.

Incident Response: This year, the Incident Response Working Group created a document featuring a collection of organized bookmarks for online resources and tools to help members onboard new analysts and to introduce experienced analysts to new tools or resources they may have not yet seen. Their regular bi-weekly meetings featured conversations on a variety of topics including automation, Kaseya, supply chain and third-party compromise, internet of things risk, threat hunting, phishing campaigns abusing archive.org, and Log4j.

Security Awareness Working Group: The Security Awareness Working Group was busy this year with planning for RH-ISAC's first Security Awareness Symposium, which took place in October 2021. This program provided members with free training for all of their organization's employees on topics such as phishing and safe work-from-home practices. In addition to lecture sessions, attendees got to put their skills to the test with a hands-on activity and an exercise for application developers.

The Symposium celebrated Security Awareness Month, and provided much needed education to vulnerable departments who came away with a better understanding of their role in their company's security. Through this group's work, companies shared information on their security awareness programs, which provided insights for how others could continue to mature their awareness training programs.

The Security Awareness Working Group also oversaw the first Phishing Benchmark Study completed in conjunction with Cofense, an Associate Member of the RH-ISAC.

Tool Users Groups: RH-ISAC expanded its tool-based user group program, adding groups for Crowdstrike EDR, SOAR, and YARA. These groups join working groups dedicated to discussion of MISP and Splunk that were launched in 2020.

EVENTS

Webinars

17 webinars held in 2021 with **376** total participants

Intelligence Workshops

225 cybersecurity professionals participated across six workshops hosted by CVS Health, Salesforce, Best Buy, PepsiCo, Wendy's, and Canadian Tire

International Workshop – **44** cybersecurity professionals participated in an Asia Pacific workshop hosted by Target

RH-ISAC Cyber Intelligence Summit

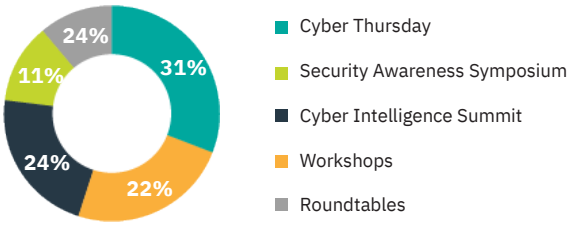
- **379** participants
- **46** speakers
- **5** keynotes
- **6** broadcast studio sessions
- **24** breakout and working group sessions

CISO Roundtable Discussions

138 CISOs and deputy CISOs participated across three CISO Roundtable discussions, each with a key focus area, 2021 Threats and Trends, Supply Chain & Operational Risk, Health of RH-ISAC, Cyber Insurance, Executive Order, and Building Resilience.

Total Participation

76% of Core Member companies participated in an RH-ISAC event in 2021.



EXERCISES

This year our members had the opportunity to participate in virtual exercises including the first industry-wide tabletop exercise in partnership with CISA, two capture-the-flag exercises with Booz Allen Hamilton, and an ATO Mini-Tabletop Exercise.

First-Ever Industry-Wide Tabletop Exercise, in partnership with CISA (EX-RH2021)

In June 2021, RH-ISAC conducted the first-ever industry-wide tabletop exercise in partnership with the Cybersecurity and Infrastructure Agency (CISA). The one-day event guided practitioners, both RH-ISAC members and non-members alike, through three modules of a fully customized scenario. Participants engaged in lively discussion across each module, focusing on information sharing, incident identification, and, in module three, executives and other leadership joined in the exercise to discuss their role and response to the scenario.

Capture-the-Flag Exercises

More than 120 individuals and 40 teams participated in two virtual capture-the-flag exercises in partnership with Booz Allen Hamilton. Both exercises included offensive and defensive challenges across six disciplines: coding, cryptography, forensics, networking, reverse engineering, and web exploitation. Based on the exercises, forensics and networking were the challenges that members excelled at, while coding and reverse engineering were two areas for improvement.

ATO Mini-Tabletop Exercise

In October 2021, the ATO Task Force organized a fully custom, mini-tabletop exercise with a scenario focused on ATO threat mitigation and response. The purpose of the exercise was to examine RH-ISAC members' protocols associated with mitigating the risk of account takeover (ATO) attacks. The three modules took participants through intital notification of an incident, to intra-team communication to confirm reports, and culminated with implementation of incident response protocols.

Application Security Excercise

October's Security Awareness Symposium featured an interactive exercise catering to participants' skill levels. Technical employees took part in a cyber range exercise focused on key code vulnerabilities, while general employees participated in a cyber escape room, identifying unsafe work practices.

TOP TRENDING CONTENT

The Member Exchange has allowed us to evolve how we share information with two key audiences: cybersecurity leaders, and analysts, engineers, and threat hunters. Below is a snapshot of the most downloaded content on the Member Exchange in 2021.

CISO Community

Sixty-two percent of the 321 users that are a part of the CISO Community are actively engaged in discussions, presentations, and sharing documents. Here's the top content users were most interested in:

1. **SecurityScorecard**: The community was interested in a scorecard to provide key security metrics at a glance for leadership. This most downloaded document was an example of a scorecard that included a traffic light rating for confidential data protection, cyber defense and response, and security compliance.
2. **2020 CISO Benchmark Report:** This report highlighted key concerns of CISOs, such as security architecture, security operations, and risk management.
3. **Ransomware Playbook:** This document serves as a template for preparation, prevention, and response to a ransomware attack.

Analyst Community

Thirty-seven percent of the 1,565 users that are a part of the Analyst Community are actively engaged in discussions, presentations, and sharing documents. Here's the top content users were most interested in:

1. **Cybercrime Forum User Allegedly Selling Data Stolen from Acxiom:** Alert to our members that a user on a cybercrime forum posted a listing that advertised more than 240GB of stolen data from the database marketing company, Acxiom.
2. **FBI FLASH Indicators of Compromise Associated with Darkside Ransomware:** FBI document encouraging users to report if any of the noted IOCs associated with the Darkside Ransomware have been observed in their network.
3. **TLP:AMBER - Weekly Flashpoint Intelligence:** A series of Flashpoint intel reports on zero-days, breaches and malware, and methods of bypassing MFA.

> *"The intel we receive can help spot a pattern, be on alert for certain malicious activity, or even stop an attack. The information can help your team develop new strategies, implement better practices, or learn about new tools and get real feedback on them. The more intel and information you share to help others, the more others are going to want to share to help you."*

Growth Milestones

2021 YEAR END — 224 Members
198 Core Members + 26 Associate Members

2020 YEAR END — 187 Members
161 Core + 26 Associate Members

2019 YEAR END — 155 Members

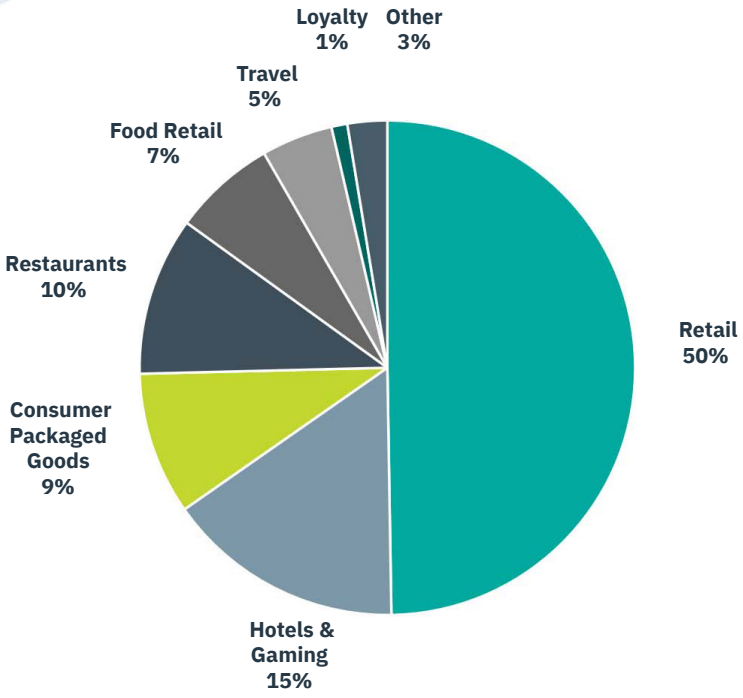
2018 YEAR END — 136 Members

2017 YEAR END — 107 Members

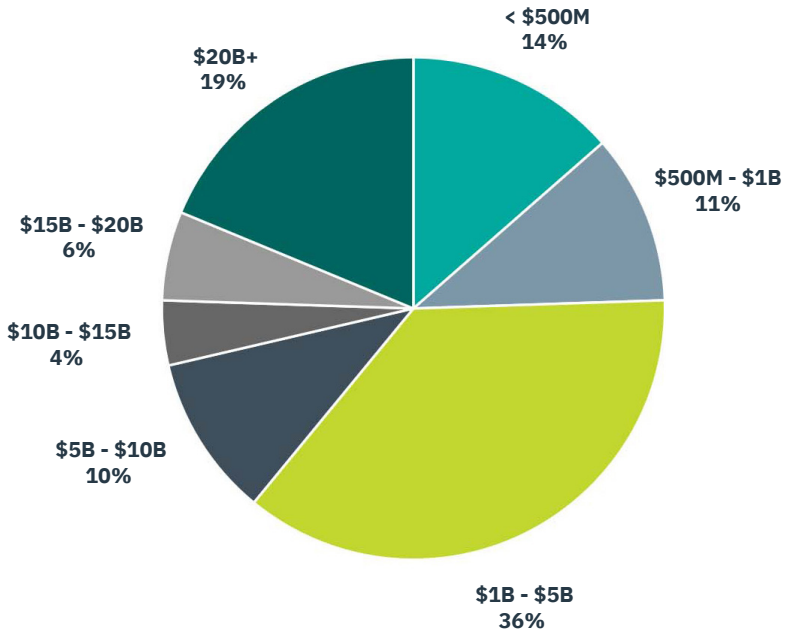
2016 YEAR END — 83 Members

MEMBER SNAPSHOT

Industry



Revenue



The Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) is the trusted community for sharing sector-specific cybersecurity information and intelligence. The RH-ISAC connects information security teams at the strategic, operational, and tactical levels to work together on issues and challenges, share best practices and benchmark among each other – all with the goal of building better security for the retail, hospitality, and travel industries through collaboration. RH-ISAC serves all consumer-facing companies, including retailers, restaurants, hotels, gaming casinos, food retailers, consumer products, travel companies and more.

For more information, visit rhisac.org.

RETAIL & HOSPITALITY ISAC