RETAIL & HOSPITALITY ISAC

RH-ISAC Working & Discussion Groups

RH-ISAC hosts collaborative working groups to address specific topics of interest and provide members an opportunity to collectively discuss solutions, share best practices, and develop guidelines on current issues. Members may join any group(s) they like.

Security Collaboration Groups

ATO Prevention

This strategic-level group is focused on identifying and promoting the adoption of group industry best practices regarding account takeover (ATO) threats, as well as sharing mitigation strategies.

Dark Web

A specialized group dedicated to identifying, tracking, and indexing sellers and threat actors that target the retail and hospitality industries. Working at an elevated TLP level with stricter guidelines, the group may share more sensitive internal data, with the goal of making intelligence actionable for organizations.

Identity & Access Management

In this group, you'll hear from others working on IAM for their enterprise, customers, or both. In monthly calls, an RH-ISAC member shares a presentation on their company's journey followed by a Q&A session.

Incident Response

This group brings IR teams together to discuss strategies and share experiences, tools, best practices, playbooks, and methodologies. Participants also collaborate on incident investigations, threat hunts, and tabletop exercises.

Risk Management

This is a strategic-focused group that works on developing enterprise risk management policies that can mitigate the impact and likelihood of attacks. In partnership with CyberGRX, a benchmark initiative allows all RH-ISAC members to complete a free self-assessment, analyze common high risk areas, and discuss strategies to improve security posture.

Contact support@rhisac.org to join a group

Security Awareness

This working group is dedicated to educating and training employees on information security best practices and developing a security-minded culture within their organizations. Meetings cover topics such as phishing program strategies, application and secure code training, and leveraging threat detection tools to identify risky behavior.

Security Operations

This group shares operational strategies to help improve the efficiency and effectiveness of security program capabilities. The group arranges monthly interviews of strategic leaders who share their journey in building their information security program. Each interview includes time for discussion.

Software Security

This working group meets to discuss challenges in product security, application security, and software security fields. Topics include: DevSecOps, cloud security, security by design, shifting left, and security automation tooling (e.g., DAST, SAST, IAST).

Third-Party Risk Management

This working group shares insights and information for building a third-party risk management program, including how to work with internal teams to identify and assess suppliers and verify what vendors have elevated levels of privilege within your networks.

Vulnerability Management

This group is dedicated to the exchange of best practices for identifying, evaluating, prioritizing, and mitigating vulnerabilities to protect the modern expanded attack surface. A proactive approach to security allows for appropriate prioritization of potential risks so companies can allocate resources to mitigate vulnerabilities before they become exploited.

Industry or Attribute Groups

Franchise

The Franchise Working Group addresses cybersecurity issues within the franchisee operating model, vendor outsourcing/solution provider support, cybersecurity framework models, and shares best practices to address challenges and increase awareness among franchisees to collectively mitigate risks.

Hospitality & Gaming

Information shared through this special interest group will translate to detection, mitigation, and improved response capabilities to reduce business risks, protect customer accounts, and create safer experiences within this sector's ecosystem.

Operational Technology

This group offers collaboration for those retailers who may have manufacturing or plant capabilities and are concerned with the unique security challenges of enabling internet of things (IoT), connective devices and technology that supports retail production operations.

Pharmacy Retailers

The Pharmacy Retailers Special Interest Group provides a forum to discuss concepts, processes, and best practices of pharmacy retailers. Recent collaboration revolved around delivery of COVID vaccines.

Tool-Based Groups

Crowdstrike Falcon EDR

A place for users of the Crowdstrike Falcon EDR tool to ask each other questions, discuss use cases, and share best practices.

MISP

The goal of the MISP Working Group is a steady-state collaborative environment for RH-ISAC members to exchange experiences in MISP development, and to jointly mature their current MISP implementations.

SOAR

The SOAR (Security Orchestration, Automation, and Response) group provides a forum for members to learn how others are effectively using software solutions and tools to streamline and automate security operations.

Splunk

Group participants learn how other members are making the most effective use of Splunk. This includes ingesting RH-ISAC threat intel from TruSTAR, building detections, managing alerts, configuring custom dashboards, and integrating with other tools to increase automation.

YARA

The YARA group provides a collaborative community where YARA users can learn from other malware detectives, and build and share techniques and descriptions (a.k.a rules).

Frequently Asked Questions

How often do groups meet?

Groups meet on a regular basis as determined by the respective group chairs and RH-ISAC program lead. Some groups have a regular monthy meeting schedule, and others meet on an adhoc basis.

What’s the time commitment to participate?

Time commitment varies by group based on the meeting schedule. RH-ISAC is heavily involved with each group, providing a designated RH-ISAC staff member to assist with administrative tasks, deliverables, and products. RH-ISAC group members are expected to participate regularly, contribute openly, and assist with deliverables in support of the goals and objectives of the group.

Can I create a new group?

Yes! RH-ISAC establishes new groups as needed to meet member interests. Members may submit a request to start a new working group by contacting {TK}.

Who are the group chairs?

Leadership from the respective group chairs is vital to each group’s effectiveness. Effective group chairs have a clear understanding of the group’s goals, objectives, and scope; should be able to commit the necessary time to their participation; be available to provide guidance on decisions needed; be willing to serve as the face and the voice of the group in order to gain support from group members, expand member participation, and providing key insights and leadership guidance which drives achievement of the group objective