Retail Cyber Intelligence Sharing Center (R-CISC)

Informational Webinar

Table of Contents

- **What is the Retail Cyber Intelligence Sharing Center (R-CISC)?**

- **Why Join?**

- **R-CISC Benefits**

- **Membership Eligibility and Associate Member Program**

- **R-CISC Operating Principles**

- **Join Now!**

R-CISC
Retail Cyber Intelligence Sharing Center

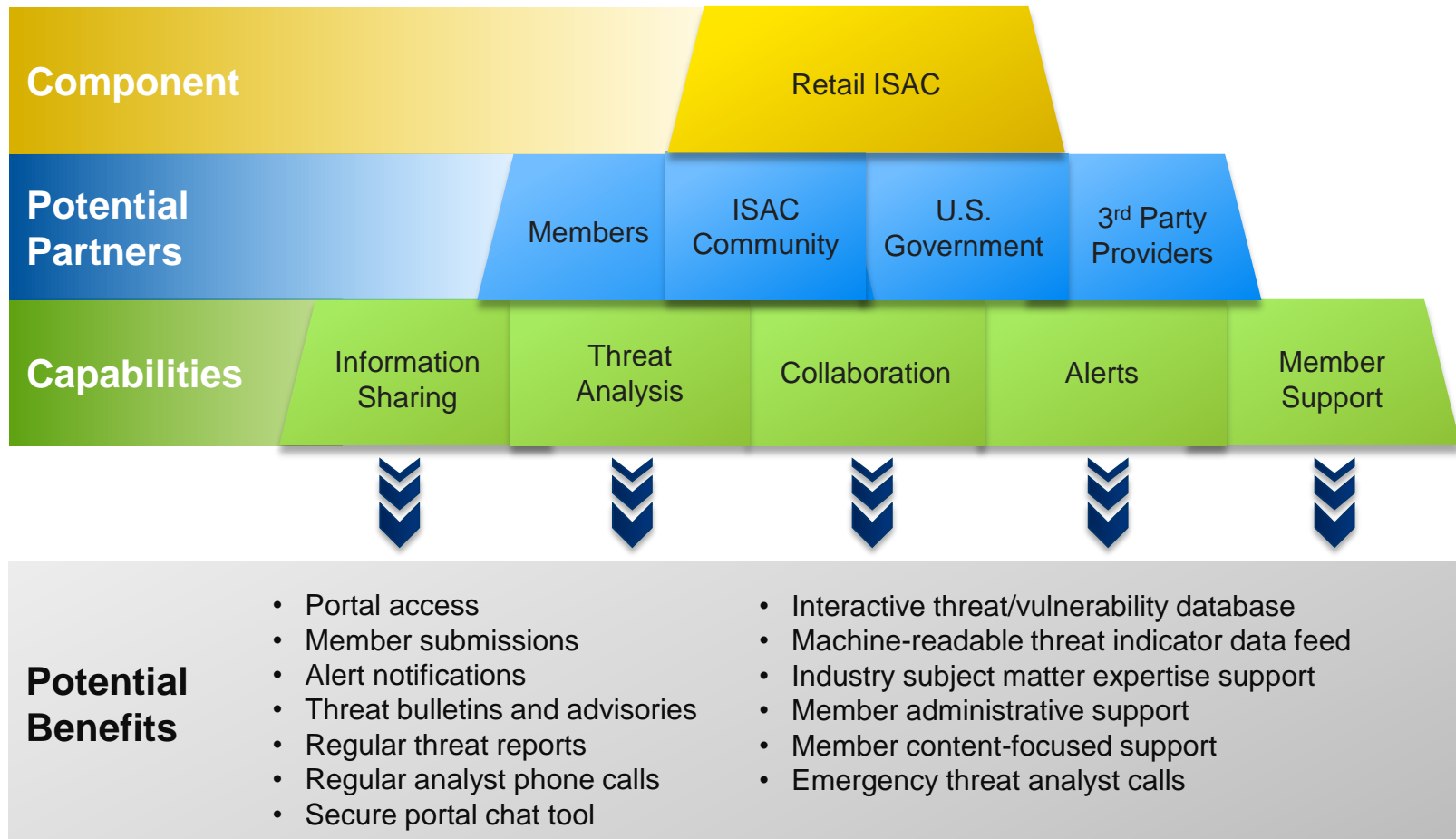# What is the Retail Cyber Intelligence Sharing Center (R-CISC)?

The Retail Cyber Intelligence Sharing Center (R-CISC) is the cybersecurity resource for the retail industry.

Created by retailers in response to the increased number and sophistication of attacks against the industry, the R-CISC provides another tool in retailers' arsenal against cyber criminals by sharing leading practices and threat intelligence in a safe and secure way.
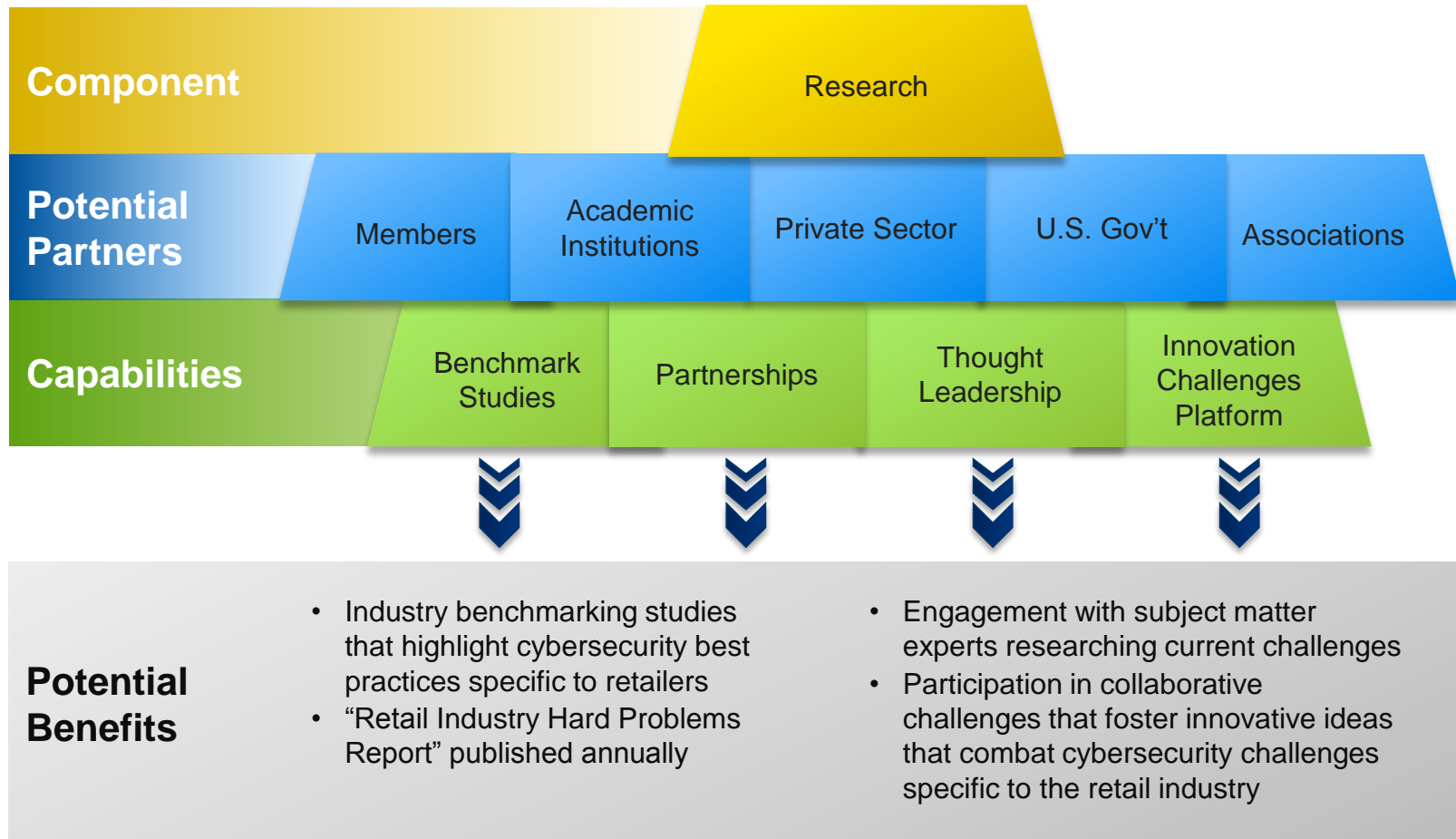
THE THREE COMPONENTS OF THE R-CISC:

1 **Retail Information Sharing & Analysis Center (ISAC)** – to identify real-time threats and share actionable intelligence to mitigate the risk of cyber attacks

2 **Training & Education** – to educate the retail community of leading practices for information sharing and protecting against cyber criminals

3 **Research** – to collaborate with academia, government and the private sector to provide retail-specific research on emerging technologies and potential future threats
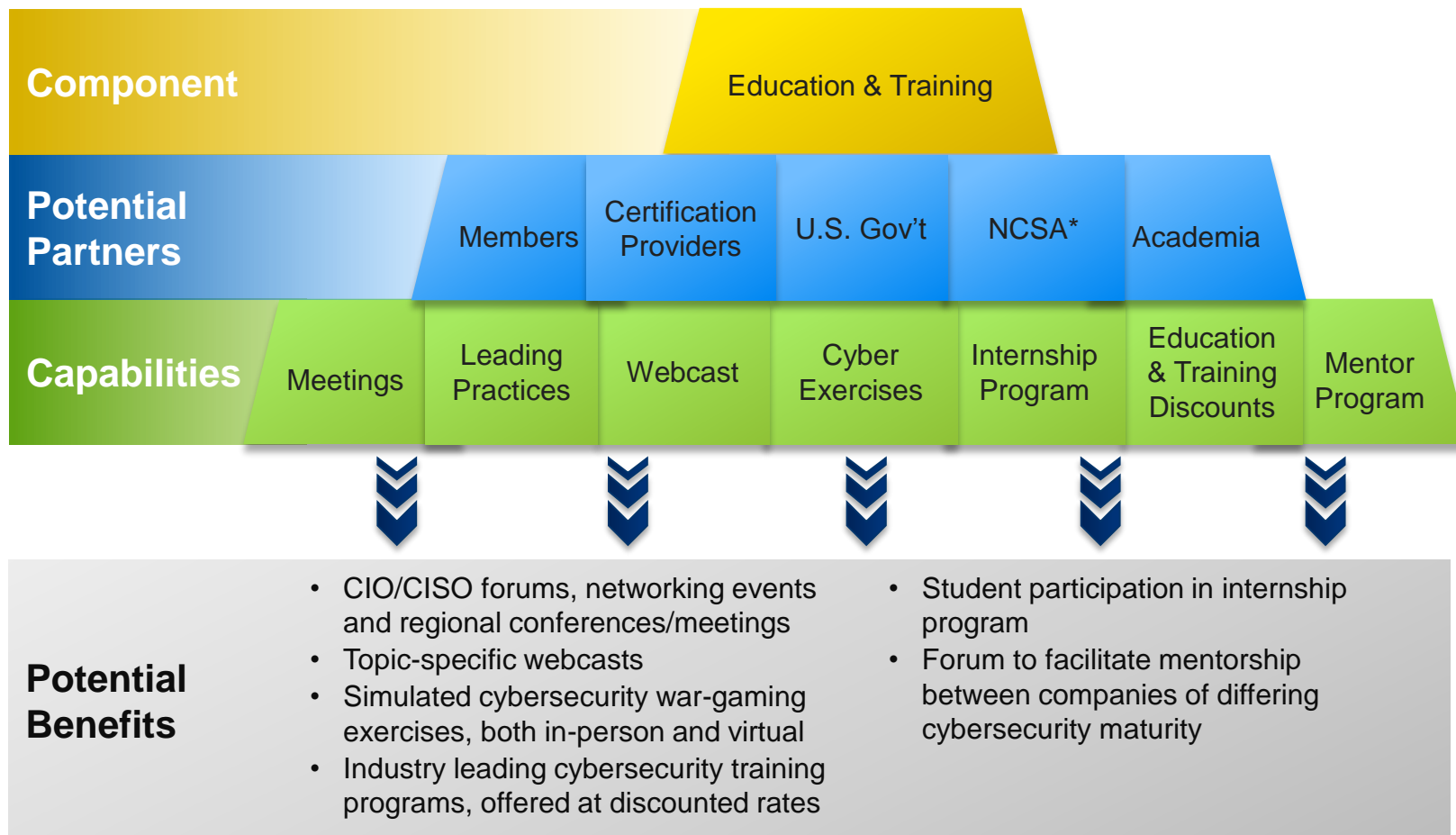
R-CISC
Retail Cyber Intelligence Sharing Center

Retail ISAC benefits will be determined by retail industry needs and the desired level of ISAC maturity

Component			Retail ISAC		
Potential Partners		Members	ISAC Community	U.S. Government	3rd Party Providers
Capabilities	Information Sharing	Threat Analysis	Collaboration	Alerts	Member Support

Potential Benefits

- Portal access
- Member submissions
- Alert notifications
- Threat bulletins and advisories
- Regular threat reports
- Regular analyst phone calls
- Secure portal chat tool

- Interactive threat/vulnerability database
- Machine-readable threat indicator data feed
- Industry subject matter expertise support
- Member administrative support
- Member content-focused support
- Emergency threat analyst calls

R-CISC
Retail Cyber Intelligence Sharing Center

Research benefits will be defined by examining existing industry services and resulting retail industry needs

Component			Research		
Potential Partners	Members	Academic Institutions	Private Sector	U.S. Gov't	Associations
Capabilities	Benchmark Studies	Partnerships	Thought Leadership	Innovation Challenges Platform	

Potential Benefits

- Industry benchmarking studies that highlight cybersecurity best practices specific to retailers
- "Retail Industry Hard Problems Report" published annually

- Engagement with subject matter experts researching current challenges
- Participation in collaborative challenges that foster innovative ideas that combat cybersecurity challenges specific to the retail industry

R-CISC
Retail Cyber Intelligence Sharing Center

Education & Training benefits will be determined based on current industry services and resulting retail industry needs

Component				Education & Training			
Potential Partners		Members	Certification Providers	U.S. Gov't	NCSA*	Academia	
Capabilities	Meetings	Leading Practices	Webcast	Cyber Exercises	Internship Program	Education & Training Discounts	Mentor Program

Potential Benefits

- CIO/CISO forums, networking events and regional conferences/meetings
- Topic-specific webcasts
- Simulated cybersecurity war-gaming exercises, both in-person and virtual
- Industry leading cybersecurity training programs, offered at discounted rates

- Student participation in internship program
- Forum to facilitate mentorship between companies of differing cybersecurity maturity

R-CISC
Retail Cyber Intelligence Sharing Center

Why Join?

- We're stronger through collaboration.

- Through the existing Retailers Against Threat Actors listserv, retailers have already:

  — Identified prospective malware threats

  — Identified infested hosts based on shared IOCs

  — Blocked bad IP addresses

  — Refined approach to possible POS breaches

  — Prevented reshipping schemes

- Sharing threat intelligence with peers helps improve security posture and situational awareness.

- R-CISC will provide access to services that may be out of reach to many retailers:

  — Certification programs

  — 3rd party intelligence feeds

YOUR PERFORMANCE ADVANTAGE

⚠ **DETECT**
Quickly detect or respond to threats before they impact your enterprise

LEARN
Learn from others to decrease your risk, increase safety, and avoid loss of revenue

🔒 **PROTECT**
Protect your reputation and position your organization ahead of attackers

IMPROVE
Avoid data overload and improve critical decision making

In 2013, 3,000 U.S. companies – large and small firms from local banks to major defense contractors to national retailers – **were hacked.**

R-CISC
Retail Cyber Intelligence Sharing Center

R-CISC Benefits

- Member benefits are organized across the three R-CISC components and include access to:
  - Secure web portal
  - Reports on keyword searches using retail industry-specific terms
  - Regular teleconferences with security analysts
  - Retail-focused cyber table-top exercises
  - Threat bulletins and advisories
  - Sharing of retail industry leading practices

- Retailers have the opportunity to buy up to Core+ benefits that provide further enhancements to their operations:
  - Automated threat information feeds
  - Reports on keyword searches on company-specific information
  - Free passes to R-CISC educational events

Capabilities Across the R-CISC Components

Retail ISAC	Research	Education & Training
Information Sharing	Benchmark Studies	Conferences
Threat Analysis	Partnerships	Leading Practices
Collaboration	Industry Leading Practices	Webcast
Alerts	Thought Leadership	Cyber Table Top Exercises
Analyst Calls		Internship Program
Member Support	Innovation Platform	Discounts
		Mentorship Program

R-CISC
Retail Cyber Intelligence Sharing Center

Benefits will phase-in over the first 18 months

Retail ISAC Component	Core	Core+
Governance. Voting position on the R-CISC Board of Directors		✔
Machine-Readable Threat Indicator Data Feed. Core⁺ members will receive machine-readable threat indicators to import into their systems		✔
Keyword Search- Core+ Analysts will conduct keyword searches to collect company-specific information on Core+ members and deliver tailored and personalized analysis to Core+ members two times/quarter.		✔
Security Conferences. Invitations to an annual security conference to discuss threats and vulnerability trends seen across the industry, as well as successful mitigations and solutions.	✔	3 Free
CIO/CISO Forum. Invitations to a virtual or physical forum for leaders to come together and discuss/understand current cyber threats facing the industry, as well as leading practices.	✔	3 Free
Access Credentials. Number of portal user access credentials per member institution.	4	12
Regular Security Analyst Phone Calls. Regularly scheduled calls with security analysts to address current challenges.	✔	✔
Keyword Search- Core. Analysts will conduct keyword searches using retail industry-specific terms to collect information and tailor reports to the retail industry.	✔	✔
Secure Web Portal. A centralized, confidential system to can post and access information on threats and attacks.	✔	✔
Member Submissions. All members will have the ability to share information with the greater membership.	✔	✔
Threat Bulletins and Advisories. Regular summary reports of analysis on the most significant reported threats.	✔	✔
Emergency Alert Notifications. Emergency alert notifications, as well as relevant technical details.	✔	✔
Secure Chat Tool. Access to a secure, online chat room or forum to discuss threats and events.	✔	✔
Interactive Threat/Vulnerability Database. Catalogue of identified threats and specific indicators, documented by R-CISC.	✔	✔
CISCP Information. Cyber threat indicators from government partner DHS CISCP.	✔	✔

Research Component	Core	Core+
Personalized Reports on Topic. Core⁺ members can annually commission two personalized reports on their company's cyber challenges.		✔
Personalized Consultations and Engagements with Subject Matter Experts. Core⁺ members can engage with subject matter experts up to three times a quarter.		✔
Industry Leading Practices. R-CISC will work with partner organizations to develop retail industry leading practices and disseminate to all members.	✔	✔
Annual "Retail Industry Hard Problems Report". R-CISC will publish an annual "Retail Industry Hard Problems Report"; the report will include content such as: cross-industry studies, leading practices and lessons learned, and technical advice.	✔	✔
Cybersecurity Benchmarking Studies. R-CISC will leverage partner organizations' expertise to conduct cybersecurity benchmarking studies on information security risks specific to the retail industry.	✔	✔
Open Innovation Challenges Platform. R-CISC will establish an open-innovation platform where members can post challenges to creatively solve specific problems facing the retail industry.	✔	✔

Training & Education	Core	Core+
Participation in Simulated Cybersecurity Exercises. Virtual and in-person cyber simulations will engage Core⁺ members in reacting to a series of business-impacting cyber events.		✔
Invitation to Forums, Networking Events and Regional Conferences/Meetings. R-CISC will organize a variety of meetings to educate members and share knowledge on current/emerging trends that impact retail operations.		3 Free
Training Programs, at discounted rates. R-CISC members can benefit from discounted education, training, and certification programs offered through industry leading organizations (e.g., SANS, ISC2, ISACA).	✔	✔
Topic Specific Webcasts. R-CISC webcasts designed to provide members with timely information on topical areas.	✔	✔
Mentorship Program. R-CISC will establish a forum for members to ask questions to the broad membership in order to benefit from a range of ideas and solutions.	✔	✔
Internship Program Recruitment Support. R-CISC will fund and sponsor a summer program to connect college juniors with members.	✔	✔

R-CISC
Retail Cyber Intelligence Sharing Center

Membership Eligibility

R-CISC Eligibility Criteria

- Recognized by trade associations with a presence in North America (but membership in R-CISC is not dependent upon membership in any trade association)
- Any firm, corporation, or other enterprise that:
  - •(i) is engaged in the operation of a retail presence;
  - •(ii) is directly or indirectly connected with the retail merchandising industry

Joint Venture Process

- Member agreement highlights confidentiality and sharing protocols where a potential member has operations in the U.S. and in one of the restricted areas.

Restrictions

- No state-owned retailer
- Not subject to U.S. economic sanctions
- Fails to promote the cybersecurity interests of the retail industry
- No head office or primary business in a country:
  - On OFAC list or subject to U.S. economic sanctions
  - DHS will not allow information to be shared
  - Without cybercrime laws
  - Supporting terrorist activities or corporate espionage against the U.S.

Associations

- Access to threat intelligence and analysis to protect their organizations; however, they are not permitted to distribute R-CISC information with broader membership.

R-CISC membership is open to retailers and merchants of all segments and sizes.*

*All applications are subject to R-CISC Membership Committee approval

R-CISC
Retail Cyber Intelligence Sharing Center

Associate Member Program

Eligibility	Associate Benefits
• Engaged in the business of providing services to retailers or retail product manufacturers • Subject matter expertise in cybersecurity and privacy issues	• Increased insight into retail concerns • Website branding • Conference and webinar participation • Access to industry leadership
Member Benefits	**Limitations**
• Additional threat information • Potential discount on services • Partners with cyber threat knowledge • Better security controls from providers	• No voting governance rights • Limited LISTSERV/portal access • No member directory access • No unchecked promotion • Board option to terminate participation

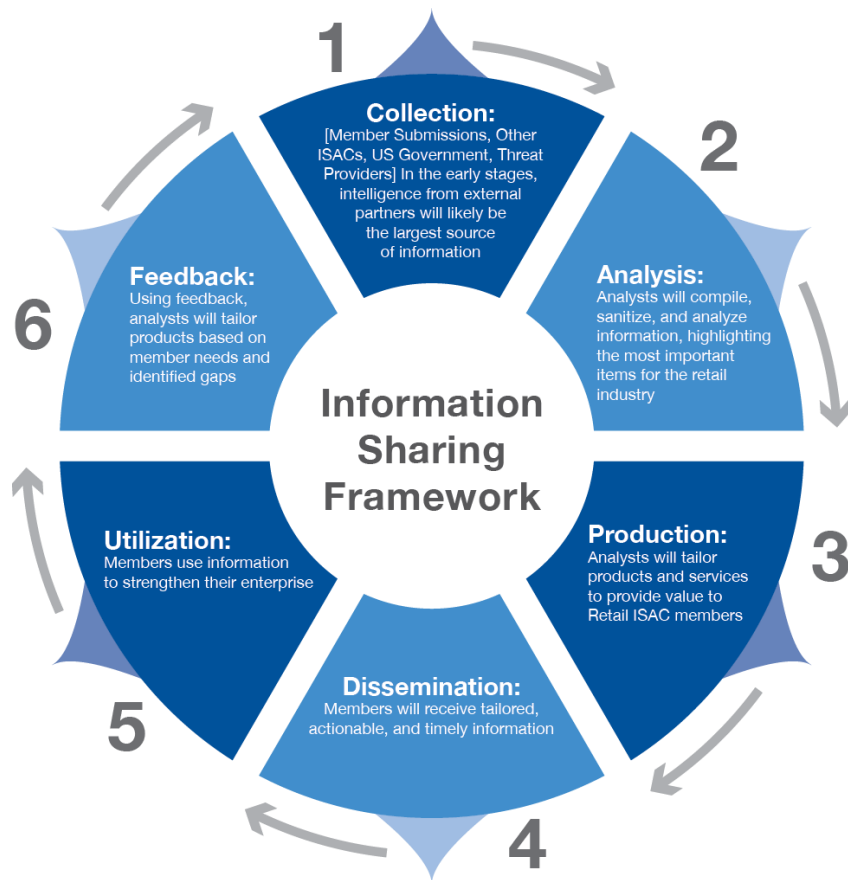**$50K** Platinum Associate

$20K Premier Associate

$5K Associate

R-CISC
Retail Cyber Intelligence Sharing Center

R-CISC Operating Principles

R-CISC's Information Sharing Framework

Information Sharing Framework

1 — Collection: [Member Submissions, Other ISACs, US Government, Threat Providers] In the early stages, intelligence from external partners will likely be the largest source of information

2 — Analysis: Analysts will compile, sanitize, and analyze information, highlighting the most important items for the retail industry

3 — Production: Analysts will tailor products and services to provide value to Retail ISAC members

4 — Dissemination: Members will receive tailored, actionable, and timely information

5 — Utilization: Members use information to strengthen their enterprise

6 — Feedback: Using feedback, analysts will tailor products based on member needs and identified gaps

Submission Type
- Incidents
- Threats
- Vulnerabilities
- Resolutions/Solutions
- Best Practices

Criticality
- Urgent
- Elevated
- Normal

Representative Outputs
- Emergency Alert Notification
- Weekly Trend Analysis
- Mitigation/Management Best Practices
- Analyst Phone Calls
- Threat/Vulnerability Catalogues

Traffic Light Protocol

🔴 **Red**: Restricted to a defined group (i.e. those present in a meeting). Information labeled 'Red' should not be shared with anyone outside the group.

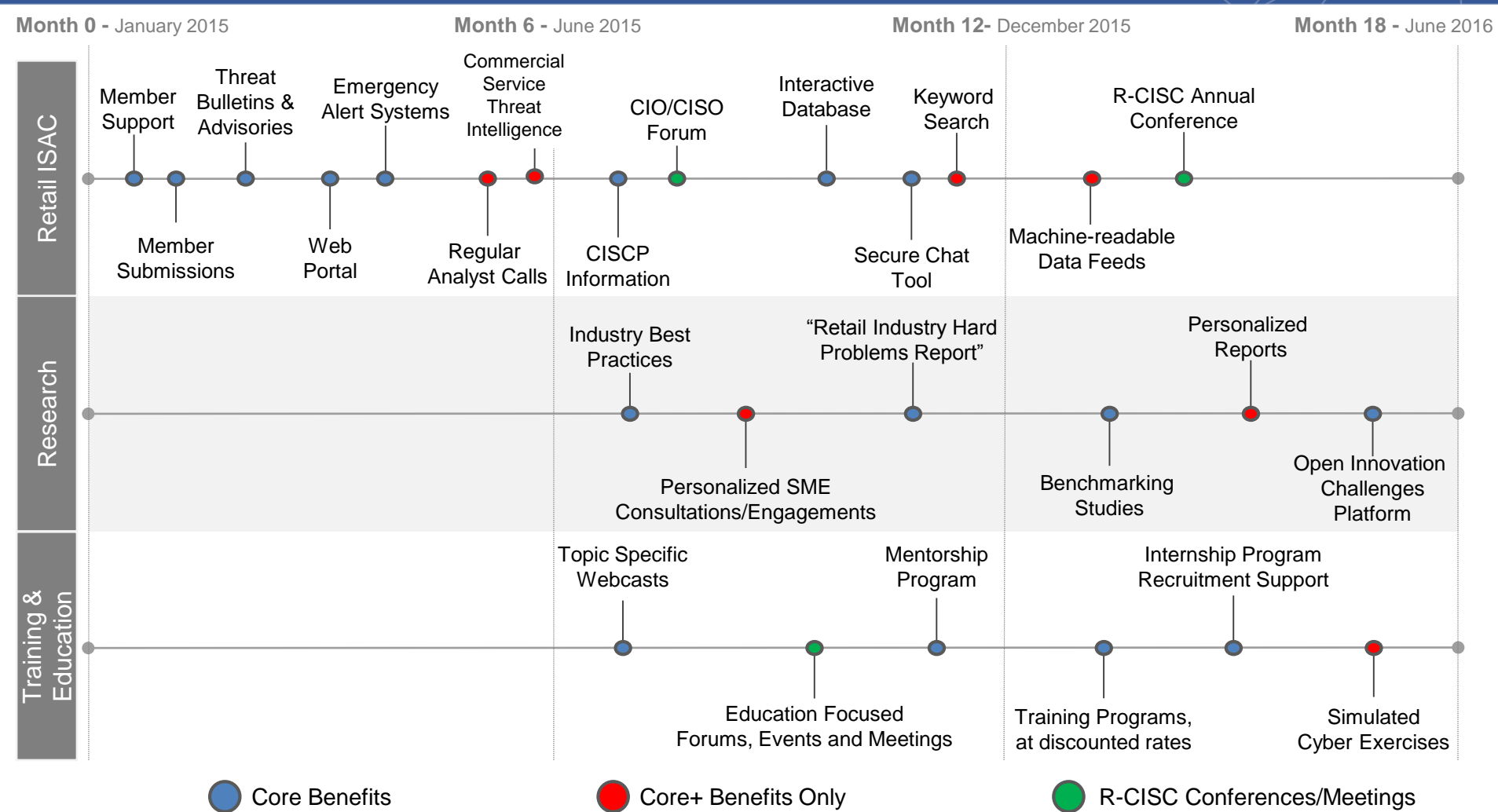🟡 **Amber**: This information may be shared with R-CISC Members.

🟢 **Green**: Information may be shared with R-CISC Members and partners (e.g. DHS, DOE, and other ISACs), but is not to be shared in public forums.

⚪ **White**: This information may be shared freely subject to standard copyright rules.

R-CISC
Retail Cyber Intelligence Sharing Center

Phasing in capabilities over 18 months will allow for prioritized implementation of R-CISC benefits

Month 0 - January 2015   Month 6 - June 2015   Month 12- December 2015   Month 18 - June 2016

Retail ISAC

- Member Support
- Threat Bulletins & Advisories
- Emergency Alert Systems
- Commercial Service Threat Intelligence
- CIO/CISO Forum
- Interactive Database
- Keyword Search
- R-CISC Annual Conference
- Member Submissions
- Web Portal
- Regular Analyst Calls
- CISCP Information
- Secure Chat Tool
- Machine-readable Data Feeds

Research

- Industry Best Practices
- "Retail Industry Hard Problems Report"
- Personalized Reports
- Personalized SME Consultations/Engagements
- Benchmarking Studies
- Open Innovation Challenges Platform

Training & Education

- Topic Specific Webcasts
- Mentorship Program
- Internship Program Recruitment Support
- Education Focused Forums, Events and Meetings
- Training Programs, at discounted rates
- Simulated Cyber Exercises

Legend:
- ● Core Benefits (blue)
- ● Core+ Benefits Only (red)
- ● R-CISC Conferences/Meetings (green)

13

R-CISC
Retail Cyber Intelligence Sharing Center

Join Now!

- R-CISC members may join at the Core or Core+ levels. Fees are based on annual corporate revenue. All organizations are eligible to purchase a Core+ membership upgrade that includes access to exclusive benefits.

ANNUAL CORPORATE REVENUE	CORE FEES
> $10B	$35,000
$5B - $10B	$20,000
$1B - $5B	$10,000
$250M-$1B	$5,000
<$250M	$2,000
Upgrade to Core+	+$15,000

- Companies who purchase a two-year membership will receive a 10% discount on annual Core membership fees.

- Find out more and join the R-CISC today. Visit www.r-cisc.org to complete a membership application or email membership@r-cisc.org for more information.

R-CISC
Retail Cyber Intelligence Sharing Center