THREAT INTELLIGENCE
WORKING GROUP CHARTER

Mission Statement

To advance proactive cybersecurity by strengthening how organizations collect, analyze, and act on threat intelligence. The Working Group fosters collaboration across sectors to develop best practices, integrate AI and automation, and empower threat analysts to anticipate and outpace adversaries.

Context

As threat actors grow more sophisticated and well-resourced, traditional reactive cybersecurity approaches are no longer sufficient. Government and industry alike must shift toward a model of proactive cyber defense—one that leverages threat intelligence not just as a feed, but as a force multiplier.

In this evolving landscape, AI and automation offer new opportunities for speed, scalability, and decision support, but must be thoughtfully integrated with human expertise. Resource constraints—including the shortage of trained analysts and fragmented data environments—demand innovative models for sharing, operationalizing, and measuring the impact of intelligence.

Meanwhile, there is no one-size-fits-all model. The use of frontier models (e.g., GPT-4, Claude, Gemini) vs. cybersecurity-specific distilled models must be evaluated within the full AI security architecture. While smaller models may outperform in narrow tasks (e.g., phishing detection, log parsing), frontier models offer greater contextual reasoning and value in multi-agent threat hunting and intelligence synthesis.

Through real-world testing, working group participants have observed the need for a hybrid AI approach: combining lightweight models for task-specific roles with a larger reasoning model to guide overarching detection and response.

Scope

The Threat Intelligence Working Group will explore the end-to-end lifecycle of cyber threat intelligence, from data collection and fusion to operationalization and impact measurement. The group will focus on developing methods to produce timely, actionable intelligence across strategic, operational, tactical, and technical levels. Its scope includes both internal and external data sources, integrating telemetry, OSINT, and threat feeds into shared defense strategies.

The group will also explore the evolving role of AI and automation in analyst workflows, multi-model AI architectures, and agentic patterns that enable both precision and scale in threat detection. It will examine both the value and limitations of domain-specific models versus frontier models for context-rich threat hunting and decision-making.

Objective

The primary objective of the Threat Intelligence Working Group is to advance proactive cybersecurity by enhancing how organizations generate, integrate, and act on threat intelligence. The group aims to foster collaboration across government, industry, and academia to identify emerging threats, improve detection capabilities, and support timely, informed decision-making. Through shared research, events, and strategic discussions, the group will work to strengthen operational effectiveness and influence broader cybersecurity practices.

Key objectives include:

- Advancing methods to produce and operationalize intelligence across strategic, operational, tactical, and technical levels
- Exploring the use of automation, AI, and agentic models to support threat hunting and analyst workflows
- Facilitating trusted intelligence-sharing models and frameworks for joint cyber defense
- Promoting the development of outcome-based metrics to evaluate the maturity and impact of intelligence programs
- Supporting the development of repeatable practices and collaborative tools that enhance detection, response, and resilience

Deliverables

- **Use Cases and Best Practices Repository:**
  A collection of real-world applications of threat intelligence, data fusion, and AI-driven analysis.
- **Reference Models or Guidance Documents:**
  Draft guidance on evaluating threat intelligence tools, AI model integration, or sharing frameworks.
- **Metrics & Maturity Assessment Toolkit:**
  A proposed set of KPIs to assess intelligence program health and readiness.
- **Potential Events: Capture the Flag**
  Community-driven A virtual exercise focused on threat hunting with real or simulated threat intelligence inputs. CTF centered on open-source collection, validation, and triage.

Working Group Membership

Working Group Chairs

Rezaur Rahman, Advisory Council on Historic Preservation, Government Chair
Daniel Buchholz, Department of State, Government Vice Chair
John Polishuk, Recorded Future, Industry Chair

Working Group Chairs will:

- Attend and contribute to each Working Group meeting
- Prepare the meeting agenda, solicit topics for discussion, assign members to address discussion topics, and distribute meeting materials
- Share information of relevance; provide an update/introduction at the beginning of each meeting to encourage member engagement
- Define and oversee Working Group initiatives and activities
- Assist in all stages of the deliverable production process
- Advocate for government, academic, and industry involvement in the working group
- Referee requests and suggestions for working group membership regarding agenda, deliverables, and representation

Working Group Members

Group members are strictly voluntary, and we strive for a broad representation across government, private sector, and academia.

Working Group Members will:

- Participate in meetings, including exchanging technical information, experiences, and best practices to develop a shared understanding of the topic(s) discussed
- Gather information and work on group deliverables outside of meetings as needed
- Provide feedback on draft deliverables as requested
- Co-lead or participate in Sub-Working Groups (breakout teams/project teams) as needed
- Provide input on meeting agendas as requested

ATARC Support

Elizabeth Wyckoff, Associate Director, Working Groups
Amy Karpowicz, Working Groups Associate
Taylor Gibbs, Working Groups Associate

ATARC support will:

- Serve as program management for the Working Group
- Coordinate and drive group projects and deliverables forward
- Schedule Working Group meetings
- Develop Working Group meeting agendas along with the chairs
- Facilitate Working Group meetings along with the chairs
- Assist in distributing relevant documents and materials to Working Group members
- Record meeting minutes, post-meeting decisions, and action items, and distribute them to Working Group members after each meeting
- Assist in preparing final proposals/recommendations
- Provide marketing services for the Working Group (promoting completed deliverables, etc.)
- Develop strategies to improve Working Group engagement, including applicable cross-overs with other Working Groups and relevant events
- Coordinate Working Group Labs as applicable

Rules of Engagement

The Working Group rules of engagement are described as below:

- Meet bi-weekly from 2025 - 2026 or until amended by ATARC Support
- Join Working Group meetings prepared and with requested action items completed
- Provide respectful and constructive feedback to yield the best decisions for the Working Group's objectives
- Endeavour to balance time among members so that all may contribute. All members of the Working Group have a voice and will be listened to.
- Final decisions are made by the Working Group Co-Chairs and ATARC Support
- If a Working Group member misses a meeting, decisions will be made in their absence. The Working Group will consider on a case-by-case basis at the request of the absentee if a decision made in the absence of a member shall be revisited.
-

The Working Group will:

- Meet every other Tuesday from 11:00 AM - 12:00 PM EST.
- Form Sub-Working Groups (breakout teams/project teams) as needed
- Follow the group's ground rules as developed in the charter
- Meet critical deadlines in the creation of deliverables by mutual and balanced effort
- Keep in confidence draft versions of deliverable, off-the-record conversations, and non-public Working Group or ATARC plans to the extent disclosure is not required by law, regulation, or valid court order

File Sharing and Collaboration Tools

Access to the ATARC Box Account is managed by ATARC Support.

Disclaimer: Products and communications by ATARC's Threat Intelligence Working Group do not necessarily represent the plans or preferences of any company or government agency.