

EXECUTIVE WHITE PAPER

Threat Intelligence in Modern Cybersecurity

Insights from Government and Industry Leaders

Highlights from a recent roundtable, hosted by the Advanced Technology Academic Research Center (ATARC) Threat Intelligence Working Group, June 24, 2025



ATARC Threat Intelligence Working Group

Table of Contents

| | |
|---|----|
| Introduction | 3 |
| The Evolving Threat Landscape | 4 |
| Operational Challenges in Threat Intelligence | 5 |
| Technological Innovations and AI Integration | 7 |
| Strategies for Effective Threat Intelligence | 9 |
| The Role of Collaboration and Information Sharing | 11 |
| Case Studies and Real-World Examples | 12 |
| Conclusion | 16 |



Introduction

The digital transformation of government, industry, and society has fundamentally altered the nature of risk and security. As organizations become more interconnected and reliant on technology, the threat landscape has evolved in both complexity and scale. Cyber adversaries are leveraging advanced tools, automation, and artificial intelligence to exploit vulnerabilities across traditional IT, operational technology (OT), and even space-based assets. In this context, threat intelligence has become a cornerstone of effective cybersecurity strategy. This white paper synthesizes the insights of leading government and industry experts, as captured in a recent panel discussion, to provide a comprehensive overview of the current state, challenges, and future directions of threat intelligence.



The Evolving Threat Landscape

Expanding Attack Vectors and Surfaces

The modern threat landscape is characterized by a proliferation of attack vectors and an ever-expanding attack surface. No longer confined to traditional IT systems, cyber threats now target operational technology, Internet of Things (IoT) devices, and even assets in space. Drones, satellites, and edge devices have introduced new vulnerabilities, requiring defenders to rethink their approach to security. The shift to remote work and mobile operations has further complicated the security environment, as organizations must now protect users and assets that operate outside the traditional network perimeter. Supply chain vulnerabilities have become a focal point for attackers, with high-profile incidents such as the SolarWinds breach demonstrating the interconnectedness of modern risks. The convergence of IT and OT environments presents unique challenges, as defenders must secure systems with different protocols, lifecycles, and risk profiles.

The Role of Adversaries and Advanced Techniques

Attackers are increasingly leveraging artificial intelligence and automation to increase the speed, scale, and sophistication of their operations. This has led to a shift from reactive to proactive threat management,

with organizations seeking to anticipate and prevent attacks before they occur. The panel discussion highlighted the importance of understanding not only known threats, but also the “art of the possible”—identifying potential vulnerabilities and attack paths that have not yet been exploited. This requires a combination of technical expertise, threat modeling, and creative thinking. For example, as one panelist noted, the use of drones and satellite communications introduces new risks, such as the potential for adversaries to jam satellite uplinks or exploit location data from fitness tracking devices, as was the case with the Strava incident that exposed military base locations.

The Impact of Digital Transformation

Digital transformation has accelerated the adoption of cloud services, mobile devices, and remote work, further expanding the attack surface. Organizations must now contend with a diverse array of devices, platforms, and networks, each with its own set of vulnerabilities and security requirements. The panelists emphasized the need for a holistic approach to threat intelligence that encompasses not only traditional IT assets, but also OT, IoT, and emerging technologies such as artificial intelligence and machine learning.



Operational Challenges in Threat Intelligence

Data Overload and Alert Fatigue

One of the most significant operational challenges facing security teams is the sheer volume of data generated by modern networks. Telemetry from endpoints, network devices, cloud services, and OT systems can quickly overwhelm analysts, leading to alert fatigue and the risk of missed threats. While artificial intelligence and large language models (LLMs) have the potential to enhance detection and analysis, they can also increase the volume of alerts, requiring careful tuning and ongoing expertise to ensure that only the most relevant and actionable intelligence is surfaced.

The panelists discussed the challenge of balancing the need for comprehensive monitoring with the practical limitations of human analysts. As one expert noted, the introduction of AI and LLMs can actually increase alert fatigue, as these systems are capable of identifying more potential threats than traditional tools. This underscores the importance of developing effective filtering and prioritization mechanisms to ensure that analysts are focused on the most critical issues.

Data Accessibility and Attribution

Data accessibility and attribution present additional challenges. Privacy laws such as the General Data Protection Regulation (GDPR) and the increasing use of anonymization techniques have made it more difficult to attribute attacks and notify victims. Encryption, VPNs, and the proliferation of edge devices further complicate the task of tracking malicious activity across networks. Smaller agencies and organizations often lack access to the advanced tools and resources needed to keep pace with these challenges, making them attractive targets for adversaries.

The panelists highlighted the difficulties associated with open-source attribution, noting that the use of proxies and anonymization services can obscure the true origin of attacks. This is particularly problematic for law enforcement and national security agencies, which rely on accurate attribution to investigate and respond to incidents. The increasing use of encryption and privacy-enhancing technologies, while beneficial for legitimate users, also provides cover for malicious actors.

Talent and Resource Constraints

Talent and resource constraints are a persistent issue, particularly in the public sector. Government agencies face a growing knowledge gap as experienced professionals retire or leave for the private sector, and budget cuts make it difficult to attract and retain new talent. The panelists emphasized the importance of continuous training, knowledge sharing, and the development of innovative approaches to compensate for limited resources. Smaller organizations, in particular, must find ways to automate routine tasks and leverage technology to maximize the impact of their limited staff.

The loss of institutional knowledge and expertise can have a significant impact on the effectiveness of threat intelligence programs. As one panelist observed, the departure of experienced personnel can create a “huge knowledge gap” that is difficult to fill. This challenge is compounded by the increasing complexity of the threat landscape and the need for specialized skills in areas such as OT security, data analytics, and AI.

Organizational Silos and Information Sharing

Another operational challenge is the existence of organizational silos that hinder the flow of information and collaboration. Threat intelligence teams may operate in isolation from other parts of the organization, limiting the impact of their work. The panelists stressed the importance of breaking down these silos and ensuring that threat intelligence is integrated into all aspects of the organization, from supply chain management to incident response.



Technological Innovations and AI Integration

Artificial Intelligence and Machine Learning

Artificial intelligence and machine learning are transforming the field of threat intelligence. AI-powered tools are now used for real-time threat detection, behavioral analysis, and anomaly detection, enabling organizations to identify and respond to threats more quickly and accurately. The panel discussion highlighted the potential of specialized, distilled language models that are focused on cybersecurity, which can match the performance of much larger models while being more efficient and easier to deploy.

For example, one panelist described the use of a distilled language model trained specifically on cybersecurity data, which was able to achieve performance comparable to a much larger general-purpose model. This approach enables organizations to deploy AI-powered threat detection at the edge, providing real-time insights and reducing the burden on central analysis teams.

Automation and Orchestration

Automation and orchestration are also playing a critical role in modern security operations. By automating routine investigation and response tasks, organizations can reduce the time required to analyze incidents and free up analysts to focus on more complex threats. Security Orchestration, Automation, and Response (SOAR) platforms are evolving to integrate with LLMs and advanced analytics, enabling more intelligent and adaptive workflows. Automation is particularly important for smaller agencies, which may lack the staff to manually investigate every alert.

The panelists discussed the use of automation to streamline incident response, from initial detection to containment and remediation. Automated playbooks can be used to investigate alerts, correlate data from multiple sources, and generate detailed reports for analysts. This not only improves efficiency, but also helps ensure consistency and accuracy in incident response.

Data Correlation and Enrichment

Data correlation and enrichment are essential for effective threat intelligence. Integrating multiple sources of threat data—ranging from commercial feeds to open-source intelligence and internal telemetry—improves coverage and accuracy. Graph and vector databases facilitate complex relationship mapping and vector searches, enabling analysts to identify patterns and connections that would be difficult to detect manually. Local intelligence, including detailed inventories of assets, user roles, and network configurations, provides the context needed to make sense of threat data and prioritize response efforts.

The panelists emphasized the importance of building and maintaining comprehensive local intelligence databases, which can be used to enrich threat data and support more effective analysis. For example, maintaining up-to-date information on user roles, department affiliations, and asset configurations can help analysts quickly identify anomalous behavior and assess the potential impact of incidents.

The Role of Edge Computing

Edge computing is becoming increasingly important in the context of threat intelligence. By deploying AI-powered detection and analysis capabilities at the edge, organizations can reduce latency, improve responsiveness, and enhance the security of remote and distributed assets. The panelists discussed the challenges and opportunities associated with edge computing, including the need for lightweight, efficient models and the importance of securing edge devices against tampering and compromise.



Strategies for Effective Threat Intelligence

Prioritization and Risk Assessment

Effective threat intelligence begins with prioritization and risk assessment. Organizations must identify the most critical assets, data sources, and intelligence streams, and focus their efforts on the threats that pose the greatest risk. This requires a deep understanding of the organization's mission, business processes, and risk tolerance. Regular risk assessments and threat modeling exercises help ensure that defenses are aligned with the most pressing threats.

The panelists discussed the importance of aligning threat intelligence with organizational priorities, noting that not all threats are equally relevant or impactful. By focusing on the most significant risks, organizations can make more effective use of their resources and improve their overall security posture.

Actionable Intelligence and Communication

Actionable intelligence is essential for both technical and non-technical stakeholders. Intelligence must be relevant, timely, and presented in a format that supports decision-making. Plain-language reporting and context-aware alerts improve the ability of security teams and leadership to understand and respond to threats. Tabletop exercises and red team drills are valuable tools for aligning leadership and operational teams, ensuring that everyone understands their roles and responsibilities in the event of an incident.

The panelists highlighted the importance of effective communication, both within the organization and with external partners. Clear, concise reporting helps ensure that intelligence is understood and acted upon, while regular exercises and drills help build trust and coordination among team members.

Continuous Improvement and Adaptation

Continuous improvement is a hallmark of mature threat intelligence programs. Organizations must adapt to evolving threats and technologies, regularly updating their processes, tools, and training. Feedback loops between intelligence, operations, and leadership drive ongoing improvement and help ensure that lessons learned from incidents are incorporated into future defenses.

The panelists emphasized the need for a culture of continuous learning and adaptation, noting that the threat landscape is constantly changing. Regular reviews of incident response processes, threat models, and intelligence sources help organizations stay ahead of emerging risks.

Integration with Business Processes

Integrating threat intelligence with business processes is essential for maximizing its impact. The panelists discussed the importance of embedding threat intelligence into supply chain management, procurement, and other critical functions. By ensuring that threat intelligence informs decision-making across the organization, agencies can better anticipate and mitigate risks.

The Role of Collaboration and Information Sharing

Public-Private Partnerships

Collaboration and information sharing are critical to the success of threat intelligence programs. Public-private partnerships, working groups, and information sharing platforms enable organizations to pool resources, share insights, and respond more effectively to emerging threats. The panelists emphasized the value of building relationships with industry, academia, and other government agencies, as these partnerships can provide access to advanced tools, expertise, and threat data that may not be available internally.

For example, the panelists discussed the benefits of participating in working groups and industry associations, which provide opportunities to share best practices, learn from peers, and stay informed about the latest threats and trends. These partnerships also facilitate the development of joint solutions and coordinated responses to large-scale incidents.

Overcoming Classification and Sharing Barriers

Overcoming classification and sharing barriers is an ongoing challenge. Classified intelligence must be translated into actionable, shareable insights that can be used by a wide range of stakeholders. Open-source and commercial

intelligence often provide the context needed to make sense of classified data and inform operational decisions. Building trust and communication channels is essential for effective collaboration, as is the willingness to share both successes and failures.

The panelists noted that information sharing is often hindered by concerns about confidentiality, liability, and competitive advantage. Developing clear policies and protocols for information sharing, as well as fostering a culture of trust and collaboration, can help overcome these barriers.

The Importance of Local Intelligence

Local intelligence—detailed knowledge of an organization's assets, users, and configurations—is a critical component of effective threat intelligence. The panelists discussed the importance of maintaining up-to-date inventories, network maps, and user profiles, which can be used to enrich threat data and support more effective analysis. Local intelligence also supports the development of tailored detection and response strategies, enabling organizations to focus on the threats that are most relevant to their environment.



Case Studies and Real-World Examples

Edge Device and Identity-Based Attacks

Recent trends in cyberattacks highlight the need for continuous reprioritization of defenses. For example, while phishing has long been considered the primary attack vector, recent data shows a shift toward edge device and identity-based attacks. Organizations must be prepared to adapt their defenses in response to changing tactics, techniques, and procedures (TTPs).

The panelists shared examples of attacks targeting edge devices, such as SSL VPNs and remote access gateways, as well as identity-based attacks involving stolen credentials and session tokens. These incidents underscore the importance of monitoring for anomalous behavior, implementing strong authentication controls, and maintaining visibility into remote and distributed assets.

Supply Chain and OT Vulnerabilities

Supply chain and OT vulnerabilities have been exploited in high-profile incidents, demonstrating the interconnectedness of modern risks. The SolarWinds breach, for example, underscored the importance of securing third-party relationships and monitoring for signs of compromise across the supply chain. OT environments require specialized approaches, as defenders must secure systems that were not designed with cybersecurity in mind and may have long lifecycles and limited patching options.

The panelists discussed the challenges of securing OT systems, including the need for specialized training, the difficulty of applying traditional IT security controls, and the importance of collaboration with vendors and manufacturers. They also highlighted the value of building virtual replicas of OT networks to support testing, analysis, and incident response.

Automation in Small Agencies

Smaller agencies and organizations are leveraging automation and LLMs to compensate for limited staff and resources. By building local intelligence databases and virtual

replicas of their networks, these organizations can enhance their ability to detect and respond to incidents. Automation enables them to conduct broad investigations, correlate data from multiple sources, and generate detailed reports with minimal manual effort.

The panelists shared examples of using automation to streamline investigations, reduce manual workload, and improve the accuracy and consistency of incident response. They also discussed the challenges of implementing automation, including the need for careful tuning, ongoing maintenance, and the development of custom playbooks and workflows.

Recommendations for Agencies and Organizations

Based on the insights of the panelists, several key recommendations emerge for agencies and organizations seeking to enhance their threat intelligence capabilities.

First, invest in AI and automation for threat detection and response. These technologies can help organizations keep pace with the volume and complexity of modern threats, while freeing up analysts to focus on higher-value tasks. AI-powered tools can provide real-time insights, automate routine investigations, and support more effective decision-making.

Second, prioritize actionable, relevant intelligence over sheer volume. Security teams should focus on the threats that matter most to their organization, rather than trying to address every possible risk. Effective filtering, prioritization, and communication are essential for ensuring that intelligence is understood and acted upon.



Third, foster cross-organizational collaboration and information sharing. Building relationships with industry, academia, and other agencies can provide access to advanced tools, expertise, and threat data. Participation in working groups, industry associations, and information sharing platforms can help organizations stay informed about the latest threats and trends.

Fourth, maintain comprehensive local intelligence on assets, users, and configurations. This context is essential for effective detection, analysis, and response. Regularly updating inventories, network maps, and user profiles helps ensure that analysts have the information they need to assess the impact of incidents and prioritize response efforts.

Fifth, regularly conduct tabletop exercises and red team drills to ensure that leadership and operational teams are aligned and prepared to respond to incidents. These exercises help build trust, improve coordination, and identify gaps in processes and capabilities.

Sixth, address talent gaps through training, recruitment, and retention initiatives. Organizations must invest in their people, providing opportunities for continuous learning and professional development. Developing specialized skills in areas such as OT security, data analytics, and AI is particularly important.

Seventh, continuously evaluate and update risk assessments and defense strategies to ensure that they remain aligned with the evolving threat landscape. Regular reviews of incident response processes, threat models, and intelligence sources help organizations stay ahead of emerging risks.

Finally, leverage public-private partnerships for access to advanced tools and expertise, and to stay informed about emerging threats and best practices. Collaboration with vendors, manufacturers, and other stakeholders is essential for addressing complex, cross-cutting risks.

Future Outlook

The future of threat intelligence will be shaped by continued advances in artificial intelligence, automation, and data analytics. AI-powered tools will become increasingly sophisticated, enabling organizations to detect and respond to threats in real time. Identity-based security and behavioral analytics will play a growing role, as attackers seek to exploit user credentials and bypass traditional defenses. Agencies and organizations must remain agile, continuously adapting their strategies and technologies to keep pace with evolving threats.

Collaboration and information sharing will be more important than ever, as no single organization can address the full spectrum of cyber risks alone. Public-private partnerships, working groups, and information sharing platforms will play a critical role in building collective defense. As the threat landscape continues to evolve, organizations must be prepared to invest in new technologies, develop innovative approaches, and foster a culture of continuous improvement.

The panelists also highlighted the importance of developing specialized, domain-specific AI models that can provide more accurate and relevant insights for specific environments, such as OT, IoT, and cloud. The integration of AI with edge computing, automation, and advanced analytics will enable organizations to respond more quickly and effectively to emerging threats.

As the workforce continues to evolve, organizations will need to invest in training and development to ensure that they have the skills and expertise needed to manage complex, technology-driven environments. The loss of institutional knowledge and the increasing demand for specialized skills will require new approaches to talent management and professional development.



Conclusion

The complexity and scale of modern cyber threats require a holistic, adaptive approach to threat intelligence. By leveraging advanced technologies, fostering collaboration, and prioritizing actionable intelligence, organizations can enhance their resilience and better protect critical assets. The insights and recommendations captured in this white paper provide a roadmap for agencies and organizations seeking to strengthen their threat intelligence capabilities and stay ahead of emerging threats.

The panel discussion underscored the importance of continuous learning, adaptation, and collaboration in the face of an ever-changing threat landscape. By investing in people, processes, and technology, organizations can build the capabilities needed to anticipate, detect, and respond to the threats of today and tomorrow.

