From Evidence to Decisions: Interview-based Study of Reporting Practices in Defensive Cyber Operations

Justin Raynor[1], Bijesh Shrestha[2], Cody Dunne[1], Melanie Tory[1] and Lane Harrison[2]
[1]Northeastern University, Boston, USA
[2]Worcester Polytechnic Institute, Worcester, USA

raynor.j@northeastern.edu
bshrestha@wpi.edu
c.dunne@northeastern.edu
m.tory@northeastern.edu
ltharrison@wpi.edu

Abstract: Defensive cyber operations (DCO) missions demand rapid decision-making under active digital threats. Established doctrine and industry standards provide technical procedures for handling incidents. However, they offer little guidance on how reporting artifacts, such as data analytics, visualization, and briefs, are produced, adapted, and communicated for decision-making. To address this gap, we conducted an empirical investigation of reporting practices in DCO through semi-structured interviews with 15 cybersecurity practitioners (managers, analysts, infrastructure technicians, and developers) engaged in incident response and threat hunting. We derived a three-dimensional model of the reporting lifecycle structured around reporting roles, purpose, and operational timeline that characterizes how network data and analytic outputs are represented in reporting artifacts such as templates, risk matrices, and briefs under time pressure and organizational constraints. Our findings highlight how reporting is shaped by trust, audience language, and the balance of standardized and flexible templates. We point to the need for traceability-linked modules, audience-aware data analytics and visualization tools, and playbooks that incorporate reporting artifacts with flexible guidance in DCO.

Keywords: Incident response, Defensive cyber operation, Stakeholder, Human-dimension, Analytics, Reporting

1. Introduction

Defensive cyber operations (DCO), including incident response and threat hunting missions, place practitioners in environments where decisions must be made at speed, often under active adversary threat and incomplete information. Established doctrine and industry standards, such as NIST SP 800-61, MITRE ATT&CK framework, and Department of Defense (DoD) cyber operations guidance (2023), provide detailed technical procedures for detecting, analyzing, containing, and recovering from incidents. However, they offer comparatively limited direction on how reporting artifacts such as templates, briefs, and risk/impact visuals are produced, adapted, and communicated as decision products that leadership can trust and act upon, or how organizational structures and human factors shape the credibility and consumption of those reports. The challenge lies in understanding how technical evidence is translated into decision-ready reporting, and how human-factors, audience alignment, and time pressure influence that translation. Prior work leaves key aspects of reporting practice unexplored. Questions remain about how credibility is maintained or lost when evidence is transformed into reporting products.

To address this gap, we conducted an empirical study of reporting practices in DCO. We carried out semi-structured interviews with 15 cybersecurity practitioners, including managers, analysts, infrastructure technicians, and developers engaged in incident response and hunt missions to examine how reporting practices are shaped by technical, human, and organizational factors. We analyze how reporting and analytics are produced, adapted, and communicated in operational settings. From these interviews, we derived a three-dimensional model of the reporting lifecycle linking practitioner roles, goals, and operational timelines to contextualize practitioners' insights. *Figure 1* summarizes this three-dimensional model by mapping the reporting goals *(Section 3.2)* described in our interviews to phases of operation and primary work-role associations. The model explains how analytical and reporting practices unfold in context and surfaces the conditions under which reporting products are accepted or dismissed. These conditions span human dimensions and the translation of technical evidence into decision-focused artifacts.

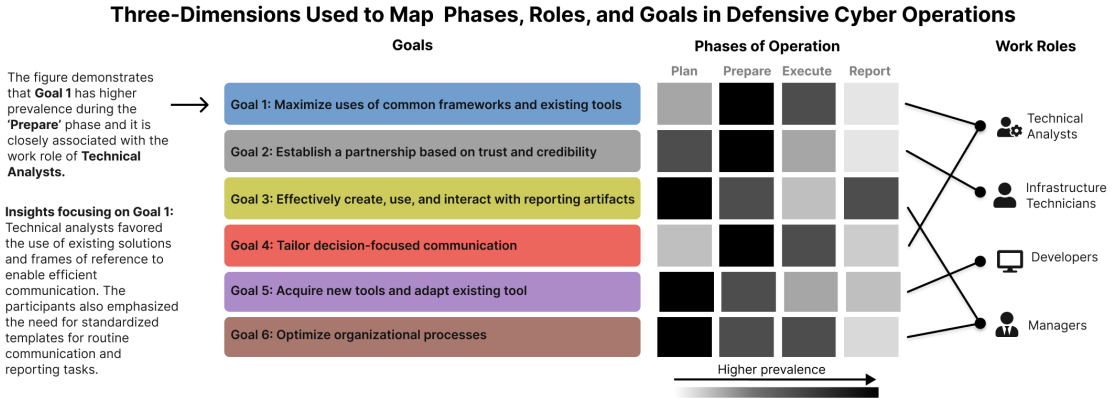

Figure 1: Three-dimensional model illustrating how practitioner goals align with operational phases and DCO work roles. Shading indicates prevalence across phases; connecting lines show primary role associations. Example insights (left) highlight how Goal 1 emerges during the 'Prepare' phase and is emphasized by technical analysts

In addition to the framework, we also offer reflections and practices for improving reporting credibility and effectiveness, emphasizing conditions such as trust and acceptance that determine whether reports succeed in practice. We emphasize the importance of reporting technologies, such as traceability-linked modules, that connect data to decision artifacts and make their sources transparent. We also highlight the value of audience-aware analytics and visualization tools that allow tailoring and scoping to different stakeholders. Finally, we call for updates to playbooks and doctrine that provide flexible guidance on producing and adapting reporting artifacts in DCO.

2. Related Work

We consider three main areas of prior work: input and tool credibility, playbook requirements, and decision-making during analysis. Our interest lies in how DCO experts create and use reporting artifacts, examining how reports are adapted and communicated across operational phases. We also consider how reporting practices are shaped by organizational hierarchies and complex analytical workflows.

Kassim et al.'s study of national CSIRTs, which examined how teams evaluate tools and data for incident response, argued for systematic evaluation, but no shared procedure exists (Kassim et al., 2023). They proposed candidate criteria for assessing tools (usability, maintainability, security) and data (credibility, timeliness, structure), but their work remains at the input level. Like doctrines such as NIST SP 800-61 and ISO/IEC 27035, Kassim et al.'s work does not examine how credibility carries into reporting. This focus on inputs is also reflected in adjacent studies of analysts' practices. D'Amico et al.'s cognitive task analyses show that analysts under time pressure often rely on heuristics and struggle to judge the reliability of feeds and tools (D'Amico et al., 2005). Parsons similarly observes that evaluation practices are typically ad hoc rather than systematic (Parsons 2022). Gutzwiller et al., extend this point in the situational awareness literature, noting that analysts' ability to act depends heavily on whether inputs are trusted, and in later work, they identified differences in cyber operator roles and called on the research community to further develop situational awareness from the perspective of end-users (Gutzwiller et al., 2016, Gutzwiller et al., 2020). Together, these works underscore the role of input credibility in analysis and decision-making, while leaving open questions about its role in the reporting artifacts used across organizations.

Works on structured playbooks and doctrines extend beyond inputs to formalize incident handling steps, including reporting. Doctrine and standards such as NIST SP 800-61 (Nelson et al., 2024) and ISO/IEC 27035 define phases of incident response and prescribe procedures for detection, analysis, containment, and recovery. Similarly, DoD doctrine (Staff 2018) codifies cyber operations at the organizational level. Frameworks such as MITRE ATT&CK (MITRE 2025) provide taxonomies of adversary tactics that can be embedded into playbooks. These sources emphasize structure, standardization, and technical coverage, but often treat reporting as compliance documentation or post-incident summaries. They offer little guidance on how reporting artifacts should be produced, adapted for different audiences, or evaluated for credibility in practice. Recent work on playbooks reflects the same limitation, identifying reporting as a feature but not addressing how it is enacted in real-world settings. Akbari et al. identified sixteen requirements for playbook-assisted incident response,

including reporting ability, adaptability, and confidentiality (Gurabi et al., 2024). They proposed a framework and prototype tool that support established process-modeling and machine-readable playbook standards, enabling interoperability and reuse across platforms. Gurabi et al. (2024) fill part of the standards gap by formalizing playbook requirements and creating a specification that includes reporting. We build on their framework by using their categories to structure our coding related to reporting tasks and extending it with evidence of reporting practice in DCO.

Other research illustrates why these requirements are difficult to realize in practice. Nyre-Yu et al. describe the conflicting priorities of mission, policy, and organizational processes within incident response teams, showing how a lack of contextual understanding can bias operations (Nyre-Yu et al., 2019). In our study, we view these findings through the lens of decision-making and reporting in operational environments, where such biases can shape how reporting artifacts are created and used. Gao highlights how cyber defense is constrained by organizational policies and the limits of monitoring technologies, reinforcing the tension between formalized procedures and practice in ways that can also shape how reporting artifacts are produced and how decisions are made under operational pressure (Gao et al., 2021). Mathews et al. propose collaborative approaches for integrating cyber threat data from traditional and non-traditional sources, highlighting the challenges of structuring and interpreting heterogeneous information across organizations (Mathews et al., 2012). We see similar challenges in how reporting artifacts are adapted and understood across organizational boundaries.

Spring and Illari review how analysts make decisions during incident analysis, highlighting three persistent challenges: how to prioritize tasks and tactics, when to generalize from incomplete evidence, and how to craft persuasive reports that others trust (Spring and Illari 2021). These challenges underscore the human dimension of incident response, showing that decision-making is not only technical but also social and communicative. We used this contribution in how we approached findings of our own study, interpreting participants' accounts of prioritization, uncertainty, and persuasion through this lens. In doing so, we extend Spring and Illari's framing with empirical evidence of how these challenges unfold under operational tempo and organizational constraints.

Prior work in this area highlights the importance of these challenges. D'Amico et al. describe how analysts escalate evidence under time pressure and struggle to communicate uncertainty with credibility (D'Amico et al., 2016). Dimara et al. emphasize that visualization and communication in cyber defense are shaped by human-centered constraints in time-sensitive contexts (Dimara et al., 2022). Gutzwiller et al. extend this perspective by showing how situational awareness depends on how inputs are trusted, and later call for research that attends more directly to operator roles and perspectives (Gutzwiller et al., 2016; Gutzwiller et al., 2020). Classic situational awareness frameworks, such as Endsley's three-level model (Endsley 1995), and subsequent elaborations (e.g., Coufalíková et al., 2021; Malviya et al.,2011), also stress that analysts' ability to act depends on how information is represented and interpreted.

Prior work converges on the importance of credibility, structure, and communication in incident response, but the practices of reporting remain insufficiently understood.

3. Methodology

To contextualize practitioner perspectives on the topic of DCO reporting and communication to decision makers, we conducted a qualitative study using semi-structured interviews. The goal of this study is to understand how practitioners in DCO create, use, and communicate data and artifacts while working under operational constraints. We aimed to capture how reporting practices unfold in real settings and what factors influence whether reporting artifacts are trusted and acted upon.

Participants: We interviewed 15 cybersecurity practitioners across three government organizations who play key roles in DCO reporting and decision-making, including managers, technical analysts, infrastructure technicians, and developers (Table 1). We identified participants through professional networks across organizations. From an initial group of 24 qualified candidates, we selected participants to ensure a mix of roles and experience levels. We did not provide monetary compensation.

Data Collection: We conducted interviews either virtually or in person, depending on participant availability. Each session lasted about an hour. Given the sensitive nature of the domain, we maintained strict confidentiality and avoided collecting any identifying operational details. We stored audio recordings locally for analysis and then removed them. This approach builds on prior interview-based studies that examine data work and communication practices in context (Tory et al., 2023; Liu et al., 2020; Erete et al., 2016).

Data Analysis: We analyzed the interview data using an iterative qualitative coding approach informed by grounded theory (Strauss and Corbin, 1997; Glaser and Strauss, 2017). We focused on identifying recurring practices and conditions that shape how practitioners use reporting and visualization across roles and operational phases. Two researchers reviewed and coded the data together and resolved differences through discussion until reaching agreement. We then grouped the codes into higher-level themes, which informed the three-dimensional framework below and contextualized practitioner insights.

Framework: How practitioners create, use, and communicate data varies based on work role, operational phase, and immediate goals, influencing how artifacts are adapted, trusted, and acted upon.

Table 1: Participant demographics and work roles, with reported uses of data artifacts

Participants	Job titles held	No. of years (Experience)	Education	Workrole	Use of Data Artifacts
P1	Element Lead, Capability Manager, Network Engineer	5	Bachelor's	Managers	Aggregate; Tailor to audience; Seek decision and support; Disseminate information
P4	Element Lead, Operations Officer	10	Master's		
P7	Element Lead	6	Master's		
P14	Operations Officer, Executie Officer	5	Bachelor's		
P3	Network Analyst, Host Analyst, Hardware Engineer	8	Bachelor's	Technical Analysts	Gain situational understanding; Communicate scheme of maneuver; Support decision making
P5	Analyst, Instructor	15	Bachelor's		
P10	Host Analyst, Cyber Planner, Technical Advisor	11	Master's		
P13	Network Analyst, Host Analyst, Technical Advisor	5	Master's		
P2	Network Analyst, Cyber Planner, Hardware Engineer	8	Master's	Infrastructure Technicians	Gain situational understanding,; Understand network infrastructure, and highlight hardware, connection and operational capability
P6	Network Analyst	6	Master's		
P8	Network Analyst, Host Analyst, Data Engineer	11	Master's		
P11	Network Analyst, Host Analyst	6	Bachelor's		
P9	Software Developer	8	Master's	Developers	Understand requirements; Delegate tasks; Demonstrate capability
P12	Software Developer, Traninee Advisor	10	Master's		
P15	Software Developer	6	Master's		

Based on our interviews, we developed a three-dimensional framework to contextualize practitioner insights focusing on work roles, phases of operation, and practitioner goals. The framework explains how reporting and communication artifacts evolve as work progresses, and information is translated for different audiences.

3.1 Phases of Defensive Cyber Operations

Our analysis showed that reporting in DCO is organized around recurring operational phases that practitioners use to orient themselves. These phases shape when information is collected, how it is refined, and when it is communicated, even when real operations involve iteration, overlap, or exceptions. Prior work has similarly examined how data and cybersecurity practitioners rely on phases and processes to structure their work (Muller et al., 2019; Muckin and Fitch, 2014).

Across interviews, we observed that reporting artifacts changes based on who owned the work, how mature the evidence was, and what the reporting output needed to achieve, rather than movement through a rigid procedure. Naming the phases let us track how reporting artifacts evolve over time, from early alignment and readiness to real-time operational updates, and finally to decision-focused products.

We identified four phases that consistently emerged across interviews:

Plan: The team works with stakeholders and technical experts to clarify mission scope and requirements, define responsibilities, identify gaps, and establish initial communication with the customer organization.

Prepare: The team turns the plan into operational readiness by securing support and authority, validating personnel and tools, establishing access and connectivity, and rehearsing key procedures before mobilization.

Execute: The team carries out the defensive task while adapting to new findings, maintaining access to the customer environment, and providing periodic updates to sustain shared understanding and situational awareness.

Report: The team consolidates findings into a formal report that explains impacts and provides recommendations for mitigating identified vulnerabilities and threats.

3.2 Work Roles

In large hierarchical organizations, roles shape what information people see, what they are responsible for, and what they need from data and visualizations (Rajan et al., 2021). This is consistent with prior observations that

job titles vary across organizations while underlying duties and separation of work remain similar (D'Amico, Whitley, et al., 2005), and that role boundaries create real handoff and coordination challenges when analytic and visualization work is distributed across teams (Walny et al., 2020, Crisan et al., 2021). We also ground our role grouping in common cybersecurity functions noted in prior research (Sabillon et al., 2017).

We grouped interview participants into four work roles based on function, since job titles alone were not reliable indicators of responsibilities:

Managers: Oversee the operation and translate technical findings into updates and products that enable decisions and shared understanding across stakeholders.

Technical Analysts: Work directly with mission data to identify and investigate malicious activity, then communicate technical assessments that shape what gets reported and how evidence is framed.

Infrastructure Technicians: Establish and sustain the access and connectivity needed for the team to operate in the customer environment, often relying on infrastructure views (for example network diagrams) to communicate dependencies and operational constraints.

Developers: Build or adapt scripts, analytics, and applications to close technical gaps, then demonstrate and explain tool capabilities to audiences with mixed technical backgrounds.

Table 2: Key tasks involving interactions with data artifacts, with specific examples of data and visualization products within different phases of operations

Phases	Data	Reporting Arctifacts	Key tasks per phase

Plan	• Task orders
	• Network logs and data
	• Threat intelligence
		• Organizational chart and hierarchy map
		• Network map (initial ingest)
			• Identify needs, gaps, and requirements
			  • Pair tools and techniques
			  • Establish hardware requirement
			  • Establish development requirement

Prepare	• Authority
	• Credentials and access
	• Additional network logs and data
	• Additional threat intelligence
		• Decision template
		• Infrastructure and topology related visualization products
		• Scheme of maneuver
			• Build relationships
			  • Conduct on-site visits
			  • Establish lines of communication
			• Communicate for decision and support

Execute	• Collect
	• Network data
	• Updated threat intelligence
		• Reporting template
		• In-progress reports
			• Communicate with decision makers and stake holders
			  • Provide in-progress and periodic reports
			  • Ensure shared understanding

Report	• Technical notes	• Updated reports	• Report findings to stake holders

3.3 Practitioner Goals

Practitioner goals were grouped and summarized from our interviews. We analyzed interview transcripts using a grounded theory-informed, multi-pass coding approach using open, axial, and selective coding. Two researchers reviewed and coded the data together and resolved differences through discussion until reaching agreement. We then grouped recurring codes into higher-level themes and consolidated those themes into a small set of practitioner goals and sub-goals that capture what participants were trying to achieve through reporting and communication across roles and operational phases. These goals give us a practical way to link reporting artifacts to intent and success criteria, and by showing how priorities shift across roles and phases.

Common Framework *Goal 1: Maximize use of common frameworks and existing tools:* Use shared language, templates, and standard products to coordinate work, while adapting them when context demands it. Participants emphasized using common language for effective communication and relying on standardized tools. This often meant a shared lexicon and *"common frame of reference"* that helps teams establish and maintain communication across customer and home organizations and translate evidence into brief-ready outputs. Templates and standard products supported routine reporting, but practitioners emphasized the need to adapt details and framing to the case context and the audience.

Trust *Goal 2: Establish partnerships based on trust and credibility:* Build working relationships that make findings believable and actionable, especially early in an operation. Participants described trust and credibility as a condition that develops between the customer and the enabling entities supporting the mission. They emphasized that early interactions shape whether later reporting is accepted, including "dos and don'ts" that influence credibility during initial engagement and coordination.

Visualization *Goal 3: Effectively create, use, and interact with visualization:* Use visual representations to build shared understanding, communicate updates, and make technical work legible to different audiences. In this paper, visualization includes common reporting visuals and artifacts used in DCO products, such as risk or impact visuals and brief-ready representations that help translate technical evidence into decision-focused reporting. This goal emphasizes visualization as part of the reporting workflow, supporting coordination and communication across roles under time pressure.

Communicate *Goal 4: Tailor decision-focused communication:* Produce outputs designed to drive a decision, with careful framing of impact, urgency, and what to do next. Practitioners emphasized that reporting must be shaped around the stakeholder who will act on it, since communication often moves *"up the chain"* to audiences with different technical backgrounds. They described tailoring as translating technical evidence into decision-ready language and levels of detail that support timely action and acceptance.

Acquire and Adapt *Goal 5: Acquire new tools and adapt existing tools:* Identify capability gaps and integrate new methods (including automation) into existing environments and constraints. Participants described the need for decision-support capabilities such as automation and AI/ML, while also emphasizing the practical work of adapting current tools to fit operational needs. They specifically pointed to emerging requirements like automating parts of the workflow, piping data into reporting systems, and improving interoperability across tools to support faster reporting and coordination.

Process *Goal 6: Optimize organizational processes:* Reduce friction from coordination, handoffs, and knowledge management across a multi-tier organization. Participants emphasized that reporting success depends not only on analysis quality, but also on how work is coordinated across roles and organizational tiers. They described recurring process challenges such as collaboration overhead, role handoffs, and knowledge management gaps that slow reporting and reduce consistency in decision-focused outputs.

We overlay our three framework dimensions into a single representation to connect roles, phases, and goals in one view. Building on our qualitative coding, we identified key tasks and events described across interviews and mapped each to the goals above. We then placed these tasks within the phases and roles where participants most often described them occurring, and color-coded them by goal to show how practitioner intent aligns with operational work. *Figure 2* shows this mapping; for readability, it highlights the most prominent tasks that relate to reporting and communication artifacts, including the subset involving interactions with data artifacts that we expand in *Table 2*. Although we label phases for clarity, participants described time-critical operations where phases often overlap or compress. Here, "customer/home" indicates defended vs supporting organizations; "teams" are functional sub-teams; "rehearsals" are brief pre-execution checks; and "threat intelligence integration" applies external indicators to interpret current evidence.

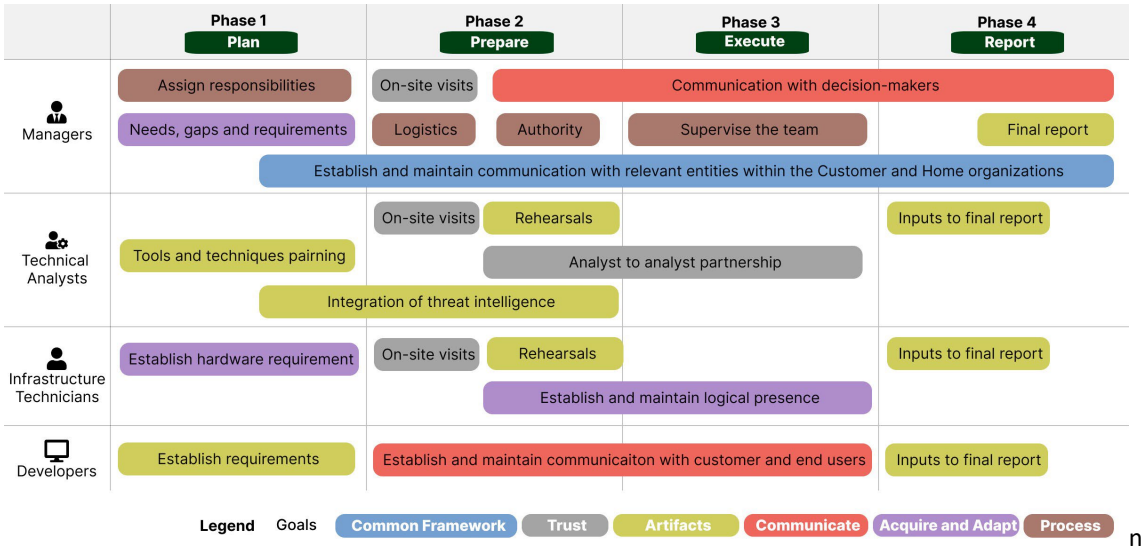

Figure 2: This figure combines all three DCO framework dimensions, overlaying key tasks and events for each work role. The key tasks are nested within various phases of operation and coded based on their associated goals. We expand the identified key tasks that apply to interactions with data artifacts in Table 2

4. Insights

In this section, we share the key insights we garnered from our participants listed in *Table 1* and using our framework in Section 3 for context.

4.1 Socio-technical: Early Coordination and Trust Groundwork

When a mission begins, participants describe early work as heavily shaped by coordination, relationship-building, role clarification, and resolving access and integration issues. Multiple participants emphasized that people and process dynamics can be more challenging than the technical work itself. P8 noted that "The biggest obstacle is not the technical, it is the personnel in that network space" (P8). P11 explained that supporting personnel are often balancing their own responsibilities while also helping the incoming team, making the work "very people heavy" and "very relationship driven" (P11). Participants also pointed to the value of identifying the right people early to build situational awareness and reduce avoidable breakdowns in communication (P12).

Early-phase progress is often shaped by socio-technical work, especially building trust and coordinating across organizations. Participants emphasized the need to clarify who to engage, who owns which actions, what information is missing, and which access or integration steps are blocking progress.

4.2 Standardization: Templates with Room to Adapt

Participants were very direct about how much time routine communication and reporting during operation takes, especially when teams have to recreate products and visuals from scratch. P6 described this as "reinventing the wheel" (P6). P4 emphasized that expectations shift across units and leaders, noting, "You have to make a new standard every time you do something, and every unit and every leader has a different standard. Makes it very tough" (P4). At the same time, participants described the value of modularity. P13 argued for "modular standardized products" that facilitate adjustments when mission conditions change, articulating an idea of "plug and play" (P13).

Participants also cautioned that standardization can become harmful when it turns into a checklist. P6 noted, "I think it definitely kind of kills creativity," and warned that analysts may stop looking for issues that are not captured by the template, even if something important occurred earlier (P6). Participants also described the burden of constantly tailoring products to different audiences. P13 pointed out that different leaders expect different standardized products, which can result in reporting the same information multiple ways, calling this "not great" (P13). P3 similarly observed that "sometimes the format becomes more important than the information you're trying to convey" (P3). Finally, P14 raised the challenge of handling non-standard details, asking how teams can "ingest that properly and make that viewable by analysts in a meaningful way" and then communicate it back to the larger organization (P14).

Standardization helps when it speeds recurring operational updates, but participants cautioned that rigid checklist-style templates can narrow attention and make it harder to surface non-standard details, motivating modular products that balance consistency with adaptation.

4.3 Communication: Audience-aware Translation and Decision-focused Reporting

Participants emphasized knowing their audience and tailoring how information is presented because the same evidence must be translated into different levels of detail, terminology, and impact framing depending on who is making the decision and what authority they hold. P7 stated, "[...] You have to know your audience" (P7), and P4 noted, "The key difference is how the commander perceives information and how we tailor it to them" (P4). Participants also highlighted credibility-building through language. P4 stated, "So, the biggest thing that helped us build credibility was knowing the right terms to use and incorporating that into our products" (P4), and P7 emphasized communicating intent and reassurance ("I'm here to help") when engagement becomes combative (P7).

Participants described using common frames of reference to support communication across organizations. P3 discussed using the MITRE framework (Xiong et al., 2022) and noted, "We have a common understanding in terms of down to the level of the MITRE techniques [...]" (P3). P6 described using MITRE as a common lexicon and presenting non-MITRE techniques in the same tactic-technique-procedure style so they are understood in a familiar way (P6). Participants also described using analogies to communicate technical details to non-technical leadership (P5, P12). Participants emphasized that decision-makers want clear risk and impact analysis, and that communication becomes less technical as it moves up a chain of command (P12, P15).

These themes highlight the need to support audience-specific lexicon, bridge technical and non-technical communication, and convey risk and impact while preserving confidence in the reporting.

4.4 Adoption: Tool fit, Automation Limits, and how Reporting Lands in Practice

Participants cautioned that automated solutions and new tools are not always trusted or helpful in practice. P13 described analysts getting overwhelmed by "big data" and questioned whether automation can be trusted "if there's no standardization," noting that "the human element is messing it up at the ground level" (P13). P10 similarly stated that tools can hinder productivity when analysts spend time following what a tool tells them rather than doing the work, and when the tool requires everyone to use it, "consuming their bandwidth" (P10). This illustrates that simply replacing a process with a tool does not necessarily fix problems, and aligns with the need to design tools that "meet them where they are" (Tory et al., 2023).

5. Reflection

Reporting and communication in DCO are shaped by more than technical work. Audience, organizational context, and trust affect what gets reported and how it is received. Across interviews, we observed that reporting artifacts changed as they moved across roles and phases. Participants described how the same evidence gets explicitly tailored to the audience to support a decision. This sheds light on why teams use standard formats yet still adapt them, and why language, trust, and credibility emerge as practical constraints.

We also note growing pressure on evidence-to-decision translation as threats become more automated and operational timelines compress, making it harder to turn evolving evidence into decision-ready reporting fast enough. This issue motivates bounded uses of automation and AI in decision-support tools to speed up evidence-to-artifact translation and support analysis in the workflow, while preserving traceability so outputs from AI-infused workflows remain auditable and accountable.

Conducting and sharing research in security-sensitive settings also raised practical challenges. Designing the interviews was especially challenging because we were most interested in real personal stories that would provide rich insights, rather than generalizations and hypotheticals. We also iterated on question phrasing and categories to reduce the risk that small details could combine into something more sensitive.

We recognize limitations in our study. Our interview sample is small and may not fully represent the broader DCO community; participant selection also affects generalizability. In addition, given the sensitive nature of DCO, participants may not have been able to expand on their responses as much as they would have liked.

Finally, many participant recommendations emphasized visualization and reporting for *communicating* findings to decision-makers, not only for *understanding* the technical picture. Future work can validate these findings with additional teams and settings, and examine how the reporting lifecycle varies across organizations.

6. Conclusion

In this study, we present a descriptive framework that organizes reporting and visualization practices in DCO along three dimensions: work roles, operational phases, and practitioner goals. We use this framework to contextualize themes from our interviews and show how human and organizational factors, including trust, audience expectations, and communication practices, shape how data and visualization artifacts are created, adapted, and used in practice. The DCO study highlights how evaluation, feedback, and design decisions are intertwined in practice, often in ways that existing frameworks leave implicit. While these dynamics are not unique to cyber operations, they become especially visible in settings where decisions are time-sensitive and accountability matters.

Acknowledgements

Justin Raynor and Bijesh Shrestha are co-first authors and contributed equally to this work. We thank the interview participants for sharing their time, experiences, and perspectives.

Ethics Declaration: This study involved semi-structured interviews with human participants. Worcester Polytechnic Institute's IRB reviewed the study and granted an exemption.

AI Declaration: We used generative AI tools to assist with grammar and rephrasing.

References

Akbari Gurabi, M., L. Nitz, A. Bregar, J. Popanda, C. Siemers, R. Matzutt, and A. Mandal (2024). "Requirements for playbook-assisted cyber incident response, reporting and automation". *Digital Threats: Research and Practice* 5.3, pp. 1–11.

Coufalíková, A., I. Klaban, T. Šlajs, and A. Štefek (2021). "Concept of Solution for Cyber Common Operational Picture Gaining", Proceedings of the *2021 Communication and Information Technologies (KIT)*, pp. 1–4. DOI: 10.1109/KIT52904. 2021.9583758.

Crisan, A., B. Fiore-Gartland, and M. Tory (2021). "Passing the Data Baton: A Retrospective Analysis on Data Science Work and Workers". *IEEE Transactions on Visualization and Computer Graphics* 27.2, pp. 1860– 1870. DOI: 10.1109/TVCG.2020.3030340.

D'Amico, A., L. Buchanan, D. Kirkpatrick, and P. Walczak (2016). "Cyber Operator Perspectives on Security Visualization". In *Advances in Human Factors in Cybersecurity*. *Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World®, Florida, USA* (pp. 69-81). Cham: Springer International Publishing.

D'Amico, A., K. Whitley, D. Tesone, B. O'Brien, and E. Roth (2005). "Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts". In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 49.3, pp. 229–233. DOI: 10.1177/154193120504900304.

US Department of Defense (2023) *DoD Instruction 8530.03: Cyber Incident Response*. Available at: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853003p.pdf (Accessed: 1 September 2023)

Dimara, E., H. Zhang, M. Tory, and S. Franconeri (2022). "The unmet data visualization needs of decision makers within organizations". *IEEE Transactions on Visualization and Computer Graphics*, *28*(12), pp.4101-4112.

Endsley, M. R. (1995). "Toward a Theory of Situation Awareness in Dynamic Systems". In *Human Factors* 37.1, pp.32–64.DOI:10.1518/001872095779049543.

Erete, S., E. Ryou, G. Smith, K. M. Fassett, and S. Duda (2016). "Storytelling with Data: Examining the Use of Data by Non-Profit Organizations". In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. CSCW '16. San Francisco, California, USA: Association for Computing Machinery, pp. 1273–1283. ISBN: 9781450335928. DOI: 10.1145/2818048.2820068.

Gao, P., F. Shao, X. Liu, X. Xiao, Z. Qin, F. Xu, P. Mittal, S. R. Kulkarni, and D. Song (2021). "Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence". In *2021 IEEE 37th International Conference on Data Engineering (ICDE)*, pp. 193–204. DOI: 10.1109/ICDE51399.2021.00024.

Glaser, B. and A. Strauss (2017). *Discovery of grounded theory: Strategies for qualitative research*. Routledge.

Gutzwiller, R., J. Dykstra, and B. Payne (Sept. 2020). "Gaps and Opportunities in Situational Awareness for Cybersecurity". In *Digital Threats* 1.3. ISSN: 2692-1626. DOI: 10.1145/3384471.

Gutzwiller, R. S., S. M. Hunt, and D. S. Lange (2016). "A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts". In *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 14–20. DOI: 10.1109/ COGSIMA.2016.7497780.

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) (2023a). *Information technology — Information security incident management — Part 1: Principles and process*. Available at: https://www.iso.org/standard/78973.html.

ISO (2023b). *Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*. URL: https://www.iso.org/standard/78974.html.

Kassim, S. R. B. M., S. Li, and B. Arief (2023). "*Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions". Digital Threats: Research and Practice 4, 3 (Sept. 2023), 1–24*.

Liu, J., N. Boukhelifa, and J. R. Eagan (2020). "Understanding the Role of Alternatives in Data Analysis Practices". In *IEEE Transactions on Visualization and Computer Graphics* 26.1, pp. 66–76. DOI: 10.1109/TVCG.2019. 2934593.

Malviya, A., G. A. Fink, L. Sego, and B. Endicott-Popovsky (2011). "Situational Awareness as a Measure of Performance in Cyber Security Collaborative Work". In *Proceedings of the 2011 Eighth International Conference on Information Technology : NewGenerations*. ITNG'11. USA : IEEE Computer Society, pp.937–942. DOI: 10.1109/ITNG.2011.161.

Mathews, M. L., P. Halvorsen, A. Joshi, and T. Finin (2012). "A collaborative approach to situational awareness for cybersecurity". In: *8th International Conference on Collaborative Computing: Networking, Applications and Work sharing (CollaborateCom)*, pp. 216–222. DOI: 10.4108/icst.collaboratecom.2012.250794.

MITRE (2025). *MITRE: Cybersecurity Thought Leadership*. Available at: https://www.mitre.org/ (Accessed: 1 March 2024).

Muckin, M. and S. C. Fitch (2014). "A threat-driven approach to cyber security". In *Lockheed Martin Corporation*.

Muller, M., I. Lange, D. Wang, D. Piorkowski, J. Tsay, Q. V. Liao, C. Dugan, and T. Erickson (2019). "How Data Science Workers Work with Data: Discovery, Capture, Curation, Design, Creation". In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. CHI '19. Glasgow, Scotland Uk: Association for Computing Machinery, pp. 1–15. DOI: 10.1145/3290605.3300356.

Nelson, A., S. Rekhi, M. Souppaya, and K. Scarfone (2024). *Incident response recommendations and considerations for cybersecurity risk management: a CSF 2.0 community profile*. National Institute of Standards and Technology. *NIST special publication*.

Nyre-Yu, M., R. S. Gutzwiller, and B. S. Caldwell (2019). "Observing Cyber Security Incident Response: Qualitative Themes From Field Research". In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 63.1, pp. 437–441. DOI: 10.1177/1071181319631016.

Parsons, P. (2022). "Understanding Data Visualization Design Practice". In *IEEE Transactions on Visualization and Computer Graphics* 28.1, pp. 665–675. DOI: 10.1109/TVCG.2021.3114959.

Rajan, R., N. P. Rana, N. Parameswar, S. Dhir, Sushil, and Y. K. Dwivedi (2021). "Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management". In *Technological Forecasting and Social Change* 170, p. 120872. DOI: https://doi.org/10.1016/ j.techfore.2021.120872.

Sabillon, R., J. Serra-Ruiz, V. Cavaller, and J. Cano (2017). "A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM)". In *2017 International Conference on Information Systems and Computer Science (INCISCOS)*, pp. 253–259. DOI: 10.1109/INCISCOS.2017.20.

Spring, J. M. and P. Illari (2021). "Review of human decision-making during computer security incident analysis". In *Digital Threats: Research and Practice* 2.2, pp. 1–47.

Staff, J. (2018). "Joint publication 3-12 cyberspace operations". In:*Retrieved September* 16, p. 2019.

Strauss, A. and J. M. Corbin (1997). *Grounded theory in practice*. Sage.

Tory, M., L. Bartram, B. Fiore-Gartland, and A. Crisan (2023). "Finding Their Data Voice: Practices and Challenges of Dashboard Users". In *IEEE Computer Graphics and Applications* 43.1, pp. 22–36. DOI: 10.1109/MCG.2021. 3136545.

Walny, J., C. Frisson, M. West, D. Kosminsky, S. Knudsen, S. Carpendale, and W. Willett (2020). "Data Changes Everything: Challenges and Opportunities in Data Visualization Design Handoff". In *IEEE Transactions on Visualization and Computer Graphics* 26.1, pp. 12–22. DOI: 10.1109/TVCG.2019.2934538.

Xiong, W., E. Legrand, O. Åberg, and R. Lagerström (2022). "Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix". In *Software and Systems Modeling* 21(1), pp. 157–177.