Toward Integrated Tactical Operations for Red/Blue Cyber Defense Teams

Julie M. Haney*
National Institute of Standards and Technology
julie.haney@nist.gov

Celeste Lyn Paul
U.S. Department of Defense
clpaul@tycho.ncsc.mil

ABSTRACT

Red and Blue cyberdefense teams provide valuable cybersecurity assessment services to help prevent and defend against malicious intruders. Through interviews, we investigated the methods, tools, and challenges of two specific U.S. Government Department of Defense Red and Blue teams and how they work together during integrated operations. We found examples of successful integration, as well as opportunities for enhanced, shared situation awareness. Based on these findings, we discuss design implications for tools that can facilitate situation awareness among multiple cyberdefense teams by supporting data fusion, change detection, network mapping, and access tracking.

1. INTRODUCTION

The U.S. Department of Defense (DOD) utilizes cyberdefense teams that specialize in penetration testing and vulnerability assessment to provide comprehensive network security assessments. These services are offered through the traditional *Red Team/Blue Team* cybersecurity assessment models [8], trading off acting as or defending against an intruder to assess and harden defenses. Although several teams may support the same customer, each team typically works independently to complete their assessments. However, with an increase in malicious intruder sophistication and mission need, DOD has realized the benefit of having Red and Blue work concurrently, with each team bringing its own strengths to cooperate in a more integrated manner.

The increased need for integrated operations has led to new interactions between these teams. Within the past year, there have been several cases of DOD Red and Blue teams working side-by-side during incident responses during which they brought their own unique perspectives to the operation. With a goal of better understanding these collaborative efforts as well as the practices and tools employed by each of the teams individually, we conducted a semi-structured interview study of members of two DOD cyber defense teams. We found that the resulting collaborations, while ultimately successful, brought to light areas for improvement as the teams moved from a single-team mode of operation to a more integrated one. Specifically, the teams' progression towards integrated operations illuminated gaps in methods and capabilities to support *cooperative tactical decision-making* and *shared situation awareness* that effectively incorporates data and expertise. In this paper we focus on the theme of *integrated tactical situation awareness*: situation awareness that informs specific actions and that is shared and contributed to by collaborating teams.

Effective situation awareness is particularly critical to integrated team planning and execution. For instance, more effective situation awareness may help reveal anomalies to investigate further, allow team members to track parts of the network they have already explored, permit the documentation and sharing of discoveries, and provide flexible views on how systems relate to each other in the network. This is already a challenging task for the cyber teams we studied, and the integration of these teams may exacerbate shortcomings that could otherwise be worked around.

Our findings provide a rare view into the practices of government cyberdefense teams. Although other red and blue teams outside this context may be similar in purpose and overall methodology [15], the specific infrastructure and tools utilized by the DOD teams described here are unique. Nevertheless, the lessons learned and recommendations to support situational awareness during collaborative efforts can be applied to a variety of cyberdefense teams.

2. BACKGROUND

Cyber Defense Teams. A growing body of cybersecurity research explores incident response activities and tools from the defender perspective. For example, Goodall et al. [7] examined the work practices of intrusion detection analysts, providing tool design recommendations to support analysts' four core tasks: monitoring, triage, analysis, and response. Werlinger et al. [14] investigated incident response practices of security practitioners during preparation, detection, and analysis phases. They found that incident response is a highly collaborative effort that must involve contributions from different groups of information technology specialists. Work by Paul [9] also found that cyberdefense teams are highly collaborative, with major challenges to situation awareness stemming from knowledge sharing . Sundaramurthy et al. [12] took an anthropological approach to studying security operations centers, and found that analyst workflows were tightly coupled to available tools.

*Work was done while at the U.S. Department of Defense

SIW'18, August 12 2018, Baltimore, MD, USA.

Cyber Situation Awareness. Endsley's classic definition of *situation awareness*, perceive–comprehend–project [4], was first expanded to the cybersecurity context by Barford et al. [1]. *Perception* in cyber situation awareness is expressed as situation recognition and identification, i.e. recognizing the type of vulnerability or attack, a target, a misconfiguration, and/or opportunities for further exploration. *Comprehension* occurs when a cyber analyst becomes increasingly aware of an issue, gains understanding of why and how the situation came about and assesses the impact of the issue. Finally, *projection* involves tracking a situation as it unfolds and anticipating future actions or consequences based on what is currently understood.

Researchers have also examined the work of cyber situation awareness. By examining common questions that cyber security analysts ask during the course of their work, Paul and Whitley [10] identified two stages of cyber situation awareness: event detection and event orientation. D'Amico et al. [3] found that information assurance analysts face several significant cognitive challenges within the course of their work: the analysis of massive amounts of data; fusion of complex data; the need to quickly establish patterns of 'normal' network behavior; and the maintenance of multiple mental models of threats and intrusion patterns.

Cyber situation awareness can also be described in terms of technical and cognitive components [6], that involves compiling, processing, fusing, evaluating, and relating data obtained from network sensors, physical sensors, and human-contributed knowledge. Having the right tools is critical to success in these activities. For example, Ruefle and Murray [11] proposed requirements for situation awareness services for computer security incident response teams (CSIRTs) that leverage visualization. Erbacher et al. [5] suggested that cyber situation awareness focus on immediate comprehension versus deep analysis, and recommended visualizations to facilitate quick overall assessments. Additionally, D'Amico and Whitley [2] argue that visualization helps with understanding the environment, shows the relationships between multiple interconnected events, reveals patterns and supports data exploration, and provides a sequential view of events. Trent et al. [13] advocated visual network maps that illustrate both physical and logical relationships to support sharable products that support decision-making.

DOD Red/Blue Team Operations. Red/Blue team network security assessments are a common model for network security evaluations of corporations, universities, and governments. Members of the Red team act as white hats to test the security of a network while members of the Blue team act as defenders to harden the network. In practice, these two teams are often at odds with each other, and it is not typical for them to work together. Although they both aim to improve the security posture of their customers' networks, they have different approaches to accomplish this. We provide an overview of Red and Blue team operations in a single organization in the DOD.

The Blue team conducts their operations at a customer site. These operations include vulnerability assessments (VA) and incident responses (IR). VAs involve the identification of vulnerabilities on a customer network and a resulting report detailing how to mitigate. During an IR, the Blue team determines the extent of an incident and provide countermeasure recommendations to assist the customer in incident recovery and prevent similar incidents from occurring again. The Blue team is divided into four technology areas: Windows Systems, Unix Systems, Network Infrastructure, and Forensic Analysis. Each technology team has their own methodology and suite of tools; however, all teams currently consolidate their collected data into a common tool that allows for ingesting, searching, monitoring, and analyzing.

The Red team primarily conducts assessments from an adversarial perspective, acts as an opposing force during military exercises, and demonstrates the operational impact of network security vulnerabilities. Typical Red operations are conducted remotely from the Red home base. However, it is not uncommon for Red to conduct on-site operations, including IRs. During an on-site IR, Red may look for evidence of the intrusion in a stealthy manner, or go in as a consultant with an intruder mindset to identify potential avenues of attack or perform penetration testing. Red tools primarily consist of publicly-known exploits, built-in Windows commands, and logging tools.

3. METHODOLOGY

We conducted a series of interviews with Blue and Red team operators and tool developers. Fourteen semi-structured interviews with nine Blue and five Red operators focused on in-depth queries about the tools and methodologies employed during their work, collaborations with other teams, and their challenges. Three interviews were with Red/Blue tool developers and were focused on learning about specific tools used by the teams. Three group interviews with two Blue teams and one Red team focused on group roles, goals, and challenges. One group interview with a Red/Blue tool development team focused on understanding how they developed capabilities to support their teams.

Demographic information was collected only in the 14 individual interviews. The nine Blue team participants had an average of four years experience (High = 10 years, Low = 9 months). The five Red team participants had considerably less experience with an average of 1.2 years (High = 1.5 years, Low = 1 year). Note that the years of experience only reflects participants' time in their respective teams, not necessarily overall computer or security experience. Members of both the Blue and Red team complete about a month of intensive training before being able to participate in operations, with subsequent training encouraged.

All interviews were conducted in-person at the facility housing both teams. Interviews lasted an hour on average. Because the facility's security policy prohibited audio recording, detailed, hand-written notes were taken of all interviews. Notes were then typed soon after each interview. Additional information was gathered from email correspondence between researchers and Red/Blue personnel, reading Red and Blue process documents and reports, and 18 hours of attendance in a Red team training course.

Interview notes were analyzed using open, inductive coding. Two researchers coded approximately one quarter of the interview notes separately, then met to discuss areas of agreement and disagreement to develop a final codebook. The first author then used the codebook to code all remaining interviews. Analysis was then conducted on the coded notes to identify emerging themes.

4. INTEGRATED INCIDENT RESPONSE

Many of our interview participants described cases of IRs where both Red and Blue teams worked together. Both Red and Blue members found the experience to be valuable, but not without its challenges. Based on three different cases of integrated operations discussed during interviews, we describe a typical integrated IR workflow.

An IR is initiated when Red and Blue services are requested after an incident is reported on a customer network. The integrated team may be provided limited information about the network and specific threat prior to the start of the operation. Once an operation begins, members shed their typical Red and Blue roles and shift into an operator/analyst relationship. Red takes on an *operator* role to actively access systems, while Blue carries out an *analyst* role to examine collected data and discover indicators of compromise. For instance, Red in effect assumes the on-network role of Blue Windows analysts since they have a similar technology skillset. However, Blue Windows analysts may assist in conducting more robust off-line analysis.

Blue Network analysts begin by looking for suspicious traffic coming from hosts. Red operators will investigate these hosts one by one, retrieving system and process information and consolidating the results into output files. They also periodically capture snapshots of host data to establish and maintain situation awareness for establishing a baseline for later comparison, identifying vulnerabilities, and finding evidence of new exploitations. Red operators frequently perform collection activities for situation awareness because an intruder may still be on the network.

Red manually examines the output files to identify more obvious issues. They may then forward the files to Blue analysts for deeper investigation. Red operators will also look for and retrieve suspicious files and artifacts, passing them on to the Blue Forensics analysts for further analysis. Blue Forensics may provide additional malicious files for Red operators to search for on other hosts. Although data is passed back and forth between Red and Blue, Blue tools do not easily support the ingestion of Red-collected data and vice-versa; data exchange, examination, and analysis between the teams are usually manual processes.

Throughout the operation, both teams also attempt to identify vulnerabilities on the network and offer countermeasure recommendations to customers. Notes on the status of accessed hosts (e.g. suspicious, exploited, cleaned) are generally kept in a shared spreadsheet.

As the operation progresses, the integrated team may shift from a *detect-and-analyze* approach in which they are learning about the intruder's tools and tactics, to a *detect-and-clean* mode in which they attempt to remove malicious software from affected hosts and mitigate vulnerabilities. Blue Network analysts generate a list of infected hosts based on known bad network activity. After Red operators clean a host, the host is removed from the list.

During on-site IRs, team members are co-located in the same room, and verbal communication is fairly easy. Situation awareness information is typically shared via drawings on a white board, spreadsheets, and tool dashboards. However, they do not have an automated way to fuse Red and Blue data into one knowledgebase.

5. TOWARD IMPROVED INTEGRATION

The value of integrated Red/Blue operations is clear: each team brings its own strengths that result in more robust support to the customer. Blue provides a broader view of the network because they can do large-scale network enumeration. Red brings their adversarial mindset and stealthier methodology to look for malware and collect information. In the use case described, DOD cyberdefense teams worked well together, each leveraging their own strengths to accomplish the mission. However, their disparate toolsets and lack of data integration inhibit more efficient integration. As integrated operations become a more common service provided by these teams, it is imperative to reflect on current challenges. We explore opportunities for better tactical situation awareness by addressing the following four gaps.

Data Fusion. As both teams move towards integrated operations, shared situation awareness that incorporates the input of all teams becomes paramount. Currently, each team uses different tools, and there is no common way teams store, share, and analyze data. This hinders the ability for analysts and operators to quickly find relationships between data collected by different teams.

Integrated operations teams need tools that can ingest and analyze multi-team data to form a common picture of the network and to aid in identification of items of interest and subsequent exploration and deeper comprehension. For example, Blue has an expanded view of a network that Red does not, but this view would be useful to Red during incident responses. Red may have specific information about vulnerabilities or malware on certain systems, which would be valuable to include in Blue's overall situational view. 'Word-of-mouth' sharing and sketches on a whiteboard are helpful during these cooperative efforts, but do not allow analysts the opportunity to manipulate the data based on their own unique perspectives, such as exploring Blue analyst data from Red's adversarial perspective. Even within Blue, there is little data fusion between Blue technology teams. Each team focuses on hosts within their distinct technology purview, so they may not be able to easily see relationships across other team member's data.

To support activities that require data fusion, we recommend establishing a common platform in which to ingest and view situation awareness data. The platform should support common data analysis requirements, but also allow for customization to each specific mission.

Change Detection. The detection of changes within a network is a critical component of the perception stage of cyber situation awareness. The inability to quickly detect changes in host data over time was identified as a significant gap for both Red and Blue. This introduces the possibility that an important event could be missed during the course of an IR, especially if the event is never captured in network traffic. Blue Windows and Unix analysts and Red operators who examine hosts (Windows and Unix devices) said that since host-based data is a snapshot in time, they cannot quickly see changes such as the launch of new processes or services, which could be indicators of vulnerabilities or compromise.

Even though Red operators periodically conducts host situation awareness on systems they have accessed, they mainly use the results of their actions to monitor current activity.

Making a comparison to previous states would be manual since there is no automated mechanism to support change detection. Furthermore, analysts and operators have no immediate indication of the 'freshness' of the host data, i.e. how long it's been since the data was last collected and how it may or may not reflect the current state of a host. As part of the perception phase of situation awareness, freshness directly contributes to an analyst's ability to form a confidence level in the collected data, which in turn helps them make decisions on how to proceed. We therefore recommend allowing for a way to view the freshness of data, perhaps a confidence level or visual cues (e.g., color saturation) depending on what was collected and data age.

Network Mapping. Cyber situation awareness requires an understanding of the network and how its components interact. The ability to provide analysts and operators with an overall view of both host and network data is absent from their current integrated operations workflow. Because Red operators do not have the specialized training to interpret Blue-collected network data, they in particular are limited to a narrowed network view that lacks a good perspective of relationships between hosts and other devices within the larger network. As one Red operator noted during IRs, he looks at the network from a focused "sniper" level, but depends on a "spotter" to tell him where to go. From a Blue perspective, it is currently hard for analysts to annotate or highlight the status or significance of a system within any of their tools outside a spreadsheet.

Based on the interviews, operators/analysts seem to have a limited understanding of network maps and their usage, and maps were not often utilized. Blue analysts are accustomed to seeing inaccurate, outdated endpoint maps or more basic maps that only show high-level architecture. They think of mapping primarily as the network scanning performed by the Blue Network team. Red operators regularly work with network maps in terms of static diagrams, which are time-intensive to build and not seen as particularly useful beyond inclusion in a report. Unfortunately, the Blue Network analysts do not regularly produce map visualization that can be shared or that could ingest other teams' data.

Despite limited prior use of network maps, most Red and Blue members appreciate that there could be value in these visual representations of the network both during traditional (single team) and integrated operations. Red operators see the benefit in creating a network map to keep track of both systems they have access to and those they know about. Blue interviews indicated that network maps could be valuable, especially if network and host data were fused together into a visual representation that could be manipulated to show relationships and allow for analyst exploration.

To support network mapping, we recommend fusing data from both Red operators and Blue analysts within the map to provide a rich visual representation, and allow for manipulation of data and analyst exploration.We also recommend support for preliminary views created with limited data to aid analysts in triage so they can make expedient decisions about next steps during the actual operation.

Access Tracking. The final stage of cyber situation awareness, projection, involves being aware of the evolution of a situation and anticipating future actions. We recommend, as a network map overlay, visualizations of operation and intruder timelines. Within the context of an integrated incident response, projection is largely accomplished via access tracking. To successfully accomplish access tracking, there is a need for a shared capability that allows analysts and operators to log current system status (e.g. infected, inspected, cleaned), track operator actions, and reconstruct the intruder's progression through the network. In addition, because there are no robust network maps, there is no way to overlay the intruder's path or cyber team progression on top of the network view.

6. CONCLUSION

In this paper, we explore challenge areas for Red and Blue network defense teams during integrated operations. Interviews revealed examples of successful interactions between the two, but also opportunities for more effective integrated tactical situation awareness. Such opportunities include improved data fusion, enhanced changed detection, incorporation of network maps, and better access tracking. As the value of operations that bring to bear capabilities from multiple teams becomes more apparent, attention to these challenges becomes essential to ensure team members have the information they require to make coordinated decisions about their next steps during an operation.

7. REFERENCES

[1] P Barford, M Dacier, TG Dietterich, et al. 2010. Cyber SA: situational awareness for cyber defense. *Cyber Situational Awareness*, Springer, MA, 3-13.

[2] A D'Amico, K Whitley. 2007. The real work of computer network defense analysts. VizSec 2007, 19-37.

[3] A D'Amico, K Whitely, D Tesone, B O'Brien, E Roth. 2005. Achieving cyber defense situational awareness: a cognitive task analysis of information assurance analysts. HFES 2005, 229-233.

[4] MR Endsley. 1988. Design and evluation for situation awareness enhancement. HFES 1988, 97-101.

[5] RF Erbacher, DA Frincke, PC Wong, S Moody, G Fink. 2010. A multi-phase network situational awareness cognitive task analysis. *Info. Vis.*, 9(3), 204-219.

[6] U Franke, J Brynielsson. 2014. Cyber situational awareness-a systematic review of the literature. *Computers & Security*, 46, 18-31.

[7] JR Goodall, WG Lutters, A Komlodi. 2009. Supporting Intrusion Detection Work Practice. *Journal of Information System Security*, 5(2), 42-73.

[8] NIST Computer Security Resource Center Glossary. 2018. https://csrc.nist.gov/Glossary/

[9] CL Paul. 2014. Human-Centered Study of a Network Operations Center: Experience Report and Lessons Learned. WSIW 2014, 39-42.

[10] CL Paul, K Whitley. 2013. A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. HCII HAS 2013, 145-154.

[11] RM Ruefle, M Murray. 2014. CSIRT Requirements for Situational Awareness. Carnegie-Mellon Univ. Software Eng. Inst., Pittsburgh PA, Jan. 2014.

[12] SC Sundaramurthy et al. 2014. A tale of three security operation centers. WSIW 2014, 43-50.

[13] S Trent, M Hoffman, J Haney. 2016. Measures of Operational Fit for Cyber Mission Forces. NDIA Human Systems Conference 2016.

[14] R Werlinger, K Muldner, K Hawkey, K Beznosov. 2010. Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, 18(1), March 2010, 26-42.

[15] S. J. Hutchison. 2013. *Cybersecurity: Defending the new battlefield*. Defense Acquisition Univ. Ft. Belvoir, VA.