A Short-Cycle Framework Approach to Integrating Psychometric Feedback and Data Analytics to Rapid Cyber Defense

Erik L. Moore, Steven P. Fulton, Roberta A. Mancuso, Tristen K. Amador, Dan M. Likarish

A Short-cycle Framework Approach to Integrating Psychometric Feedback and Data Analytics to Rapid Cyber Defense

Erik L. Moore[0000-0003-1566-526X], Steven P. Fulton[0000-0001-6962-8558], Roberta A. Mancuso[0000-0002-1486-5748], Tristen K. Amador[0000-0003-0622-8877], and Daniel M. Likarish[0000-0001-5654-710X]

Regis University, Denver Colorado, USA
{emoore, sfulton, rmancuso, tamador, dlikaris}@regis.edu

Abstract. Following earlier research in demonstrating the significance of behavioral analysis in cyber defense, the authors developed a framework to incorporating multi-disciplinary datasets along a common timeline to increase incident response feedback for coaching. Currently this framework is being introduced in the state of Colorado, USA as a part of a joint government, industry and academic partnership. Upon project initiation, the feedback cycle had been a minimum of several months from observation to feedback. Presented here is a new framework that can shorten the cycle of psychometric feedback to multiple times in one training day. This Short-Cycle Framework, gathering psychometric and cyber data to provide direct feedback to cyber defense team leaders, was conceived when Regis University's psychometric evaluators observed a real multi-agency cyber defense response. The authors realized the psychometric data can be used in live cyber defense incidents alongside things like network firewall traffic analysis as the cyber defenders provide relief for organizations under active cyber attack. This work presents the context in which the framework was developed, the characteristics of the framework, and suggestions for further research. The framework implements a specific set of short-term state indicators based on well-known personality trait and state models. The coaching cycle was scripted to shorten the delay between observation and feedback so that it can be more useful in both training and live incident response.

Keywords: Psychometric Analysis • Cyber defense • Myers-Briggs • Parker Team Player Survey • National Guard • Feedback • Training • Multi-agency • Short-Cycle Framework • Cyber Incident Response

1 Introduction

Beginning in 2013, Regis University has hosted joint training exercises of multiple Colorado state and local government cybersecurity teams, Colorado based public utilities and cybersecurity focused industry leaders. The University has hosted biannual large (over 100 participants from adjoining states) and smaller joint training exercises that the authors recognized the personal individual member, team cohesion

and incident responses community growth and maturation leading up to recognition of a dynamic self-sustaining Collaborative Training and Response Community (CTRC). We also have witnessed the individual professional development of team members, for instance after hours cyber range practice, 7/24 threat awareness and analysis, regional and national group exercises. Since May of 2016, these exercises have also included psychometric analysts with expertise in personality trait preferences and role diversity to guide the cybersecurity teams toward better team interaction, leadership efficacy, and self-awareness for individual participants, which ultimately benefits the team. The observations and analysis outlined here have occurred at numerous events, providing feedback to leadership and to individual team members based on observed training and incident response behavior.

The leadership of the joint training had completed their initial roadmap of exercises, including technical, incident response practice, and relationships. They recognized the need to improve team performance using additional methods and began looking for a next set of methods to enhance response capabilities. A Regis-based member of the joint training leadership realized that behavioral psychology and health care faculty may be able to add significant value to enhancing cybersecurity team performance. The entire joint training leadership agreed and invited Regis faculty specializing in these fields to perform an initial unstructured observation and present initial ideas on what strategies they might use to enhance cybersecurity team performance.

The authors on the Regis social and health sciences faculty, Mancuso and Amador, were authorized by the joint training leadership to support the training as psychometric analysts. Their operations indicated two areas of opportunity for team enhancement, awareness of behavior types for the individuals and team interaction awareness to support leadership coaching. They recommended Myers Briggs Type Indicator (MBTI) psychometric tool for individuals. For leadership coaching support they recommended the Parker Team Player Survey (PTPS). These tools were selected because they have been extensively tested and utilized with a variety of populations, including those working in crisis management [1] and those working in technical positions [2]. One of the authors, R. Mancuso, had significant experience in using the MBTI to determine team-based efficacy, including certification in the method, so the deployment of psychometric analysts could happen fairly rapidly based on that existing capacity.

During a cyber defense exercise in May 2017, Regis faculty performed psychometric analysis on surveys and observations to create the first coherent baseline data set that combined psychometric data with pre-existing performance measures for cyber defense operations. Thus, the digital behaviors recorded in network firewalls and first-person journaling of participants was interpreted in concert with general psychometric analysis of the training exercise. An actual cyber defense incident occurred in February 2018 where the psychometric evaluators were invited to observe in real time. The framework presented here is based on the baseline data from the May 2017 exercise and the February 2018 cyber defense incident.

2 The Cyber Defense Incident Response

Because of an existing relationship between Regis University and the Colorado National Guard, Defense Cyber Operations (CONG-DCO), select faculty were invited to observe the February 2018 cyber defense incident response activity. The CONG-DCO received a request from the Office of the Governor of the State of Colorado to provide urgent support to the Colorado Department of Transportation in the face of an active intelligent and persistent cyber threat. This was the first time that any National Guard unit within the US had been dispatched to support a state agency in cyber defense activities. This engagement provided the psychometric analysts opportunity to directly observe behavior while the team was under the stress of a real cyber defense incident and engaging in the larger interaction with the chain of command, collaborating teams, and the staff they were supporting. The value of this opportunity was immediately recognized by both the cyber defense experts and the psychometric analysts. Observations could provide leadership coaching multiple times during a live event in support of improving actual cyber defense capabilities. Since then, members of the cyber security training team and the psychometric analysts have collaborated on developing a new "Short-Cycle Framework." This framework is an integration of psychometric and other team performance indicators that provides along a single timeline to provide feedback to the cyber security team during training exercises and real incident response.

When the CONG-DCO was deployed as part of a state response, they embed as a member of a multi-agency response team. These multi-agency response teams are made of individuals who are members of separate institutions with significantly different institutional practices and social norms. These include government IT Departments, National Guard soldiers, and corporate technical staff. Recognizing the personality types and behaviors rapidly may facilitate adaptation to more rapid convergence on threat identification, vulnerability mitigation, and recovery solutioning.

Several questions drove the authors' development work. "Can a Short-Cycle Framework of multiple psychometric and cyber defense indicators help cyber defense team leadership better recognize individual personality and team dynamics for coaching opportunities that can enhance team performance?" Follow-up questions of interest are, "Can psychometric indicators help team leadership move from intuitive to analytical response, overcoming the vulnerabilities of intuitive thinking often exploited by social engineering and psychologically designed attack strategies?" "Can psychometric-based intervention strategies shorten the delay between a single team member's awareness of an exploit, and the team's mitigation of that exploit?" In order to provide a context in which these questions could be effectively answered, the authors added a layer of preparation for both cyber defense training exercises and cyber defense incidents.

3 Event Preparation for Exercises and Cyber Defense Incident Response

In order for the psychometric analysis to be effectively framed during either a cyber defense training exercise or response incident, significant preparation is necessary. Up-front baseline assessments of each team member needs to be established using the Myers-Briggs Type Indicator and the Parker Team Player Survey and then a focused set of during-event assessments will continue during both cyber defense exercise opportunities and incident response. This established a set of traits against which the psychometric analysts could assess certain variable psychometric states along a combined timeline of cyber defense activities and events within the timeline that the CONG-DCO experienced, either in an exercise or during an incident. The state data is used in both training and incident response to generate short-cycle coaching for team members.

The authors have initiated a traditional pace of psychometric data feedback to cyber defense team leaders where data is analyzed between events. Currently, the sample size is small and the delay in feedback is the months between exercises. Following a March 2019 cyber exercise, we expect the increase in data gathering rate should improve data reliability. In addition, the Short-Cycle Framework is being applied to a broader range of cyber defense exercises including student competitions. Earlier work in the behavioral analysis of teams in cyber defense suggests that team dynamics is significant in relation to outcomes [3]. This impact of team interaction within cyber defense is similar to that observed in exercises like competitive challenge [4].

The technology infrastructure necessary to facilitate a cyber defense training exercise with live active networks are broadly known [5]. Usually all parties involved in the exercise meet at a single facility using a specialized network that simulates the Internet, an adversary network, a network to be defended along with business systems that must sustain services under attack. This can be a competitive challenge between multiple teams or a single-team exercise. These simulate defensive operations like defending a hospital, public utility, or government agency that is under attack where the trainees are brought in to defend the institution and facilitate recovery to normal operations.

The preparation required for an actual cyber defense incident response does not include the same level of network infrastructure as a training exercise. Typically, the cyber defense response team brings in laptops, switches, flip charts, and other resources necessary to establish an incident response center and forensic base of operations embedded within the large, possibly compromised, operations network of the institution that is under attack.

4 A New Model Through Which to Understand Types of Data for both Exercises and Cyber Defense Incidents

The Myers-Briggs Type Indicator surveys were provided through a web interface by distributing a link to participants approximately six weeks prior to the May 8, 2017 training session. The analysts reviewed 7 completed MBTI surveys from team members before the May 8th training session. The Parker Team Player Survey was provided to participants on the day of the training session. The analysts reviewed 13 completed PTPS surveys. The team was provided by the Colorado National Guard and consisted of active cyber defenders selected by their leadership. The surveys of this team provided a baseline of self-awareness so that members would be more aware of their behavior. The Parker Team Player Survey has behavioral traits that set a baseline and adaptive behaviors that can be observed in real time. The psychometric analysts identified adaptive behavior options as deliverable feedback with coaching support scripts in near real time. This came to be known among the group as the Short-Cycle Framework for psychometric coaching feedback.

The types of data gathered by the authors to enable the Short-Cycle Framework fall into baseline data (MBTI and PTPS traits) , established before exercise scenarios and cyber defense incidents, and ongoing data (PTPS adaptive behaviors) that is gathered with different frequencies throughout the event. This all could then be plotted on the same timeline with traditional cybersecurity training metrics listed below and described in detail in later sections.

- Personality Trait Assessments
    - Myers-Briggs Type Indicator (MBTI)
    - Parker Team Player Survey (PTPS)
    - Adaptive Behavior Scale
    - 14-Item Resilience Scale
- Ongoing Data
    - Personality State Assessments
        - Team Cohesion Assessment Scale
        - Observed PTPS
    - Digital Observations through System and Event, Information Management (SIEM) Network and Log Traffic Data from devices like Firewalls, Server Logs, and Switch Flow Traffic
    - Digital Service Scoring Engine - tracking business digital system state over time of the defended services.
    - Red Team Journaling - presents the active attack and often intentionality
    - “CEO” Injects - provides the timelines of directives issued by a mock CEO

Psychometric state analysis like “Team Cohesion” during events makes ongoing relationship dynamics and causal events of behavior clearer. This is why data were aggregated into a single timeline. To meaningfully address this, the team is developing a set of scripted feedback messages for particular psychometric states that can be evaluated for efficacy as more event data are collected. More detailed explanations of

data types, such as the author's use of Parker Team Player Survey components applied as states to the Short-Cycle Framework are provided in later sections. In Figure 1, the second line of data from the top, they are represented along a single timeline by a circled "F" to facilitate cross-reference as analysis occurs.

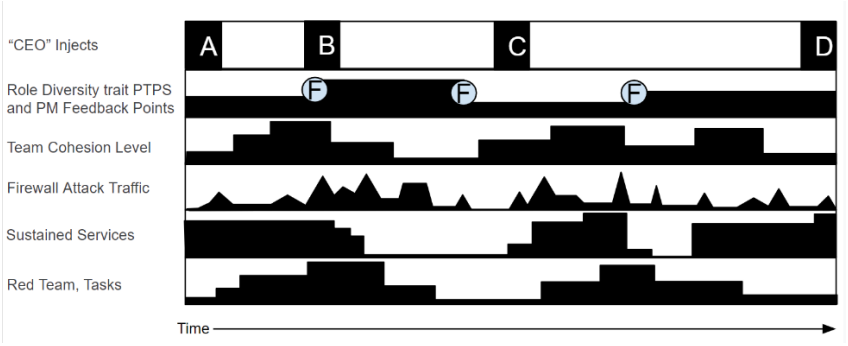

Fig. 1. Short-Cycle Framework, a simulated set of metrics across cyber defense and team psychometric indicators set in parallel on a timeline to rapidly analyze cyber event causes in relation to ongoing psychometric measurement of the team.

5 Cyber Defense Exercise Scenario

Cyber Defense Exercise scenarios are to provide realism and context for success in terms of business scenario, technical infrastructure, and the situation in which the intervention occurred. While scenarios can range from public utilities infrastructure like water dam controls, and electrical grids, it is best to create a scenario from recent cyber defense incidents in order to maintain relevance. An example presented here to provide context was used in the CONG-DCO training exercise in May 2018.

5.1 Scenario Description

A fictitious financial department is in the middle of migrating from local to regional corporate control. With uncontrolled growth and change in governance the department had significant loss of focus on its cybersecurity infrastructure. A major cyber exploitation has occurred with an advanced, persistent threat that is disrupting the department operations. The CONG-DCO are asked to provide defensive intervention against the cyber attack. Primary goals are to identify compromised systems and remove exploits and vulnerabilities. They are responsible for defending the computer system and supporting the internal audit team. Concurrently they must maintain internal and external business services. The department has significant cloud-based service offerings.

5.2 Exercise - CEO Injects

A key control factor was implementing a realistic cybersecurity exercise simulating the behavior of leaders. In the exercise these simulated as a set of directives injected into the scenario by a trainer playing the role of mock CEO of the fictitious organization to be defended in the simulation. In Figure 1, the mock CEO injects line at the top identifies specific injects by letter (A, B, C, etc.) that can be referenced when evaluating the impact of each inject across the combined timeline. The mock CEO injects range from requesting a status update or asking for a service to be restarted, to sometimes disruptive events like standing up alternate financial systems to sustain a business' ongoing needs mid-incident. Simulating the demand to service institutional needs instead of focusing solely on defending against the red team provides a more realistic simulation of actual cyber defense incident response situations. Another purpose the CEO fulfills is to accept requests from the cyber defense team training in the exercise. This simulates business process, governance, communications, and leadership interaction at the highest level.

6 Cyber Defense Exercise Data Gathered Prior to the CDOT Incident

6.1 Security Incident and Event Management Data

The advantage of a Security Incident and Event Management system (SIEM) for training teams and for the psychometric evaluations is that the logs may be analyzed in real time. A SIEM is a coordinated set of services that aggregate the ongoing digital logs of network and computer devices into a single database. An analytical engine provides alerts, automated responses, and visualizations that guide live security team members as they respond to threats.

In a cyber defense exercise, the Red Team, a team acting as an in-scenario adversary, journals their attack exploits and that journal is confirmed by traffic analysis of the SIEM data. The trainees see the alerts from the SIEM and respond. In a live incident, the attack data presented in the SIEM would be perpetrated by a malicious actor potentially from anywhere in the world. See Figure 2 for how the types of data vary between a training scenario and a real cyber defense incident.

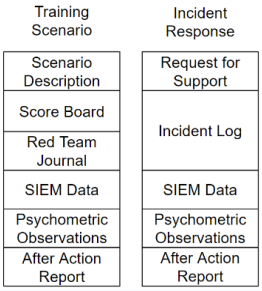

Fig. 2. The exercise scenario and incident response data differ in that more external data can be reviewed independently regarding the threat actor and external services.

Figure 3 indicates digital traffic events as they occur as reported by the SIEM based on known potential indicators of compromise (IoC) as published by the relevant SIEM manufacturers published standards and customized alerts. The vertical scale is each type of IoC events per minute.

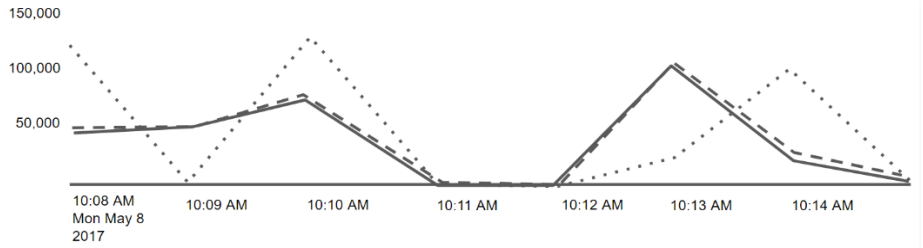

Fig. 3. Illustrates the rough format in which data is presented from the SIEM.

Focusing on the particular data isolated in Figure 3 graphed are three example indicators of compromise:

Dotted Line: ASA-6-302014 - A TCP connection between two hosts was deleted.

Dashed Line: ASA-6-106100 - The ASA might generate message 106100, indicating that the packet was permitted; however, the packet is later correctly dropped because of no matching connection.

Solid Line: ASA-6-302013 - A TCP connection slot between two hosts was created.

Each of these IoC events has immediate potential impact for the cyber defense teams, and through comparison with other data, each cyber security team's ability to respond can be analyzed. While the timespan represented in the samples is very short, full-day event data would be collected to lay in comparison to the other forms of data like team journaling, psychometric analysis observations, etc. This information is graphed in the 4th line of Figure 1 in order to determine both impact of digital traffic events on team behavior, and the effects of control efforts by the cybersecurity team on digital traffic.

Using the Splunk tool to analyze the SIEM IoC data, a Colorado School of Mines (CSM) analyst interpreted the data from the Regis University Security exercise held on May 8th, 2017. The CSM analyst identified common penetration techniques utilized by the Red Team and common techniques used by the Blue teams to protect their payloads. In addition to running queries to generate statistics and identify patterns, the CSM team upon review also constructed the line graph visualizations using the Splunk capabilities to develop a more abstracted timeline. This would become the basis of a multifactor timeline presented below.

The CSM team was able to identify the actual firewall used in the exercise which led to the discovery of the syslog codes and opened up a new realm of analysis. They identified the top log codes from the 8-10am log and created several visualizations to show high-level appearance of the top logs relative to the rest as well as over time. They further analyzed data related to each of the fixed red team IP addresses and

listed, described and commented on the top ASA codes. While not presented here, these data are important as an interpretation of red team activity.

6.2 Security Incident and Event Management Data

The Red Team is the attacking team in a cyber defense exercise to simulate what an attacker might be doing to trigger an actual incident response operation. Events on the Red Team Journal, Table 1, can indicate the intentionality of their activities in addition to specific attacks that can be recorded as a journal entry as they engage in training scenario attacks. This provides excellent capabilities to cross reference in the device logs, in the defensive team's behavior, and in relation to whether full recovered status of the network was achieved.

Table 1. Sample journaling performed during exercises by the "Red" cyber attack team playing the role of a malicious perpetrator.

Time started	Time ended	Action
10:05		Scanned Domain Controller using nmap
10:15		Remote desktop login of DC
10:20	10:30	Blocked internet access
10:24		DNS service, cha ged scope to give 4 Ips only
10:34		Removed 192.168.111.10 from DHCP scope User Network and added 192.168.111.12
10:35		Removed WiFI network from DHCP address 192.168.113.1
10:40		Changed password for Blue 8 and Blue 7 to xxxx and Blue 3 to xxxx
10:43		Lost connection to DC, tried to RDP but could not
10:59		Disabled MAIL from AD
11:10	1:11	Remote desktop to Cyclos DB server, and closed out active windows, got kicked out at 11:11

Number of red team tasks per minute are plotted in Figure 1, line 6, in order to indicate their impact on both service levels and team behavior.

6.3 Services Availability - Scenario Scoring Engine Data

The scoring engine provides a real-time indicator to cyber defense exercise organizers and is analogous to availability dashboards present in network operations centers. If a service like a web server is up, it will indicate an up arrow in real time. If that service has been disrupted, its arrow will display as down. This is represented in Figure 1, line 5, to enable assessment of impact of red team activities, and the cybersecurity team's ability to respond fully to a service interruption. The timeline is designed so that it can become possible to analyze the duration of response times from IoC to service recovery in relation to team resilience.

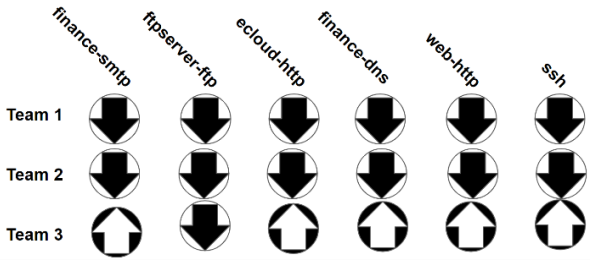

Fig. 4. Service Availability Scoring Engine indicates whether a business service is up or down by simulating the user and checking for success.

Figure 4 represents a sample scoring engine to illustrate how multiple teams can be tracked over time for various network system services. The scoring engine is a key tool in determining the effectiveness of cyber defense teams as they train against a particular scenario, in a competitive challenge, or in a technical walk-through. In this particular case, a single team consisting of 13 members was tracked over time and had access to this scoring engine to determine their performance as they worked to restore services.

7 Identifying and Infusing Personality Trait Preferences and Role Diversity in Cyber Security Teams

Our model utilizes both trait and state measures as central psychosocial factors in cyber security teams. The trait measures that comprise our initial psychometric evaluation will enable us to calculate a predicted effectiveness score for each team. Based on that score, we can develop scripts with prescribed feedback to enhance team performance.

Work in cybersecurity incident response human factors covers several related areas that each add value and provide context for the work presented and complementary value to the work presented here. For instance, Oltramari [6] focuses on the risk associated with trusting individuals. This human factors work highlights the importance of expectations of behavior as they affect the team performance through cohesion of purpose. As Pfleeger and Caputo notes [7], since 2010 there has been a significant effort to align the efforts of behavioral science and cybersecurity to encourage empirical studies to enhance the socio-technical systems that enable cybersecurity. The work presented in this paper follows along that thread, working to develop a systematic process that can generate measurable results in training and incident response events.

For the initial psychometric evaluation (before the cyber defense exercise or incident occurs) the psychometric evaluators identify personality trait preferences by administering the Myers-Briggs Type Indicator [8] and role diversity utilizing the Parker Team Player Survey [9]. Two additional trait assessments that we believe will be useful in predicting cyber security team performance are Adaptive Behavior [10] and the 14-item Resilience Scale [11]. Measures of resilience will be used to develop

scripts to support leadership in coaching and can also be used as the basis for future skill development. All of these measures have been shown to be largely stable over time as suggested in referenced material. The 14-item Resilience Scale is plotted in the graph in Figure 1 on the third line so that it may be cross-referenced to indicate if other events have affected team resilience.

We predict that teams with high trait preference diversity and high role diversity who self-report as being very adaptive and resilient may be more effective at cyber incident response. Using scores from the initial psychometric evaluation as a baseline, we can categorize teams into one of four quartiles by their predicted effectiveness score. Coaching injects in the form of direct, real-time feedback to team leaders can be tailored and scripted for each team in response to their predicted effectiveness score.

Personality state assessments will be used to provide real-time observer assessments of team performance. We propose to assess team cohesion and observed role diversity at three points during the cyber defense exercise in order to gauge the effect of the coaching injects. Team cohesion is measured using a modified Crew Cohesion Assessment Scale [12]. This is coupled with a modified PTPS that can assess observed role diversity. Both are completed by faculty observers following each coaching inject.

Below is a sample paragraph of the psychometric evaluators' assessment of cyber security team members' scores on the Parker Team Player Survey, our measure of role diversity. After uncovering Contributors, Collaborators and Communicators, an example finding was:

- Evaluation 1: There were no Challengers in the team.
- Evaluation 2: These results indicate that the group is predominantly task and goal oriented, but does not excel at process or at questioning that process.

These examples represent general statements within the context of instruments and frameworks like the Myers Briggs Type Indicator [8] and the Parker Team Player Survey [9]. These examples suggest scripts for coaching and are a demonstration of process functionality. Once process is confirmed as functionally able to generate actionable findings in this study, observations and indicators will later be tracked over multiple exercises and adjusted and new constructs may be identified. Over time we expect to identify and differentiate different individual and team characteristics that suggest higher levels of capability in cyber defense training and incident response.

8 Live Response Incident Log and After-Action Report

The Incident Response Log is a compilation of observations entered by incident responders while working through the incident. Specifically, it is a real-time journal of observations and record of actions taken. Often in a digital form it will include malicious file names, system configuration settings, and commands used. In relation to cyber defense exercises it is analogous to a team journal. Also, the journal documents

when a service goes down and when it is restored from the perspective of the cyber defense team. The scoring engine provides an alternate means of confirmation.

After action reports occur in both cyber defense exercises and incident response. They are based on journaling and include later analysis intended to determine how things could have been done better, how successful it was, what follow-up items might be valuable, etc. The after-action report is initiated immediately after the incident with a live debrief of all participating members. This is formalized into a document with follow up items. The report is used to inform next steps on defense, revision of cyber defense exercises scenarios, and research on open-ended questions to enhance the capabilities of the trainers and the incident response teams.

9 Strategy for Relating Data

Cyber Defense Team Leads and the exercise designers use the new data from the Short-Cycle Framework to address two development challenges: 1) exercise designers need to increase the relevance of exercise to live incident response by comparing data across incident response and exercise and improve future cyber defense exercises and, 2) during a cyber defense incident or exercise, the team leads need to leverage the full set of new data to better coach their teams to enhance performance.

The authors have spent several years analyzing data pulled from exercises. The technical sets of analysis such as firewall and red team journaling were used to compare exercises to incident response and enhancing performance from session to session. The authors recognized though that key indicators of performance were not being gathered in the earlier data sets. Team interaction such as conflict, collaboration, and motivation played a strong part in success, and yet was not being recorded. The following is a list of key functions and strategies that the psychometric analysts use to enrich the interpretation with both new data acquisition and analysis across exercise and incident response.

Psychometric Analysts

- Provide observations, evaluations, and coaching
- Leadership skills and team member participation feedback for individual team members
- One-on-one discussion about personality traits and leadership guidance
- Increase awareness of participant's interaction styles so they can function more effectively in both cyber exercises and incident response.
    - Increase the rapidity of Multi-Agency Incident Response Teams by enhancing team members' cohesion
    - Develop awareness of leadership using feedback that supports coaching
    - Enhance ability to work in groups
    - Increase self-awareness and awareness of others
    - Adapt to team members and situation and demonstrate resiliency leading to quicker response and better collaboration

10 Conclusion and Recommendations

The Short-Cycle Framework, integration of psychometric observations, SIEM network data, and journaling may be applied so that incident response exercises and live incident response are enhanced through the use of psychometric analysis and feedback to team leads.

The authors intend to continue this research by developing a set of prescribed feedback or "scripts" based on the four psychometric evaluations through the quartile states. Then the team intends to evaluate the effectiveness of these types of feedback over time using the proposed method described here. Preparing scripts may allow leaders very early identification of the disruptive effects on team cohesion potentially caused by some social engineering or other types of psychological attack strategies. Because scripts may be delivered digitally and the psychometric analyst observations may not be interactive, video may allow psychometric teams to provide their services to cyber operations teams through networks.

Some of the authors' previous experience suggests that direct feedback from the psychometric analysts to individual team participants may undermine leadership so we recommend using leadership channels to provide coaching. This approach supports the appropriate authority in behavioral adjustments within the broader context of their individual institutional relationships.

A prerequisite to this work needs to be acknowledged for those looking to produce similar processes. Transitive trust between the analytical/academic community and the cyber defense community must be pre-established. A consideration for future research is how to more rapidly build these types of trust relationships that can stand rapidly and at multiple scales.. Should we be successful in this line of research and development of framework structure, we are looking to achieve replicability of approach by baselining the team state and standardizing how scripts are used to provide feedback to team leaders. Over time, the team hopes to use frameworks like this to discover patterns of behavior that represent effective behavior types in relation to the various aspects of different scenarios. Developing a portfolio of scenarios, the team intends to test the predictive capacity of this type of framework in relation to effectiveness of cybersecurity incident response.

11 Acknowledgements

The authors have presented the context in which the Short-Cycle Framework was developed in conjunction and collaboration with our Regis University interdisciplinary investigators (Computing and Information Sciences, Liberal Studies and Healthcare), state and local Colorado government entities and private industry partners.

The team thanks Riley Miller, a PhD student at Colorado School of Mines department of Computer Science for his independent analysis of the red team attack traffic that was detected in the main firewall during the cyber exercise referred to in this analysis. The cyber defense exercises at Regis University are sponsored by a series of

grants from the Department of Defense of the United States of America. Thank you to Rick Cisneros, the project scientist of Regis University, College of Computing and Information Sciences, for his work gathering the network data as Red Team lead and providing exercise infrastructure. Thank you to Robert Moon for gathering the network data and being a red team member along with Nasser Esmail.

12 References

1. Sample, J. A., and Hoffman, J. L.: The MBTI as a Management and Organizational Development Tool, Journal of Psychological Type (11), pp. 47-50 (1986)
2. Beyler, J., and Schmeck, R. R.: Assessment of Individual Differences in Preferences for Holistic-Analytic Strategies: Evaluation of Some Commonly Available Instruments, Educational and Psychological Measurement (52:3), pp. 709-719 (1992)
3. Hoffman, L. J., Rosenberg, T., Dodge, R., & Ragsdale, D.: Exploring a National Cybersecurity Exercise for Universities. IEEE Security & Privacy, 3(5), 27-33 (2005)
4. Buchler, N., La Fleur, C. G., Hoffman, B., Rajivan, P., Marusich, L., & Lightner, L.: Cyber Teaming and Role Specialization in a Cyber Security Defense Competition. Frontiers in Psychology, 9 (2018)
5. Dodge, R. C., Ragsdale, D. J., & Reynolds, C.: Organization and training of a cyber security team. In SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme-System Security and Assurance (Cat. No. 03CH37483) (Vol. 5, pp. 4311-4316). IEEE (2003)
6. A. Oltramari, D. Henshel, M. Caines, B. Hoffman: Towards a Human Factors Ontology for Cyber Security, Proceedings of the Tenth Conference on Sematic Technology for Intelligence, Defense, and Security, Fairfax, VA, USA, pp. 26-33, IEEE Computer Society (2015)
7. Pfleeger, S. L., & Caputo, D. D.: Leveraging behavioral science to mitigate cyber security risk. Computers & security, 31(4), 597-611 (2012)
8. Myers, I. B., McCaulley, M. H., Quenk, N. L., & Hammer, A. L.: MBTI Manual: A Guide to the Development and Use of the Myers-Briggs Type Indicator, 3rd. Palo Alto, CA: Consulting Psychologists Press (2003)
9. Parker, G. M.: Team Player and Team Work: The New Competitive Business Strategy. San-Farncisko: Jossey-Bass Inc, Publishers (1990)
10. Charbonnier-Voirin, Audrey & Roussel, Patrice: Adaptive Performance: A New Scale to Measure Individual Performance in Organizations. Canadian Journal of Administrative Sciences / Revue Canadienne des Sciences de l Administration. 29. 280-293. (2012) 10.1002/cjas.232
11. Wagnild, G.M. and Young, H.M.: Development and Psychometric Evaluation of the Resilience Scale. Journal of Nursing Measurement, 1, 165-178 (1993)
12. Mission-Centered Solutions (n.d.). Crew Cohesion Assessment; Leadership Toolbox Reference.
https://www.fireleadership.gov/toolbox/documents/Crew_Cohesion_Assessment.pdf