SANS INSTITUTE SUBMISSION 3: How 8 Extraordinary Cybersecurity Leaders Developed Their Management Capabilities

> *Response to question 8: "What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the nation's cybersecurity workforce?"*

Summary: This RFI response shows how 8 people made the transition from technologists to technology leaders and provides a roadmap for rapidly developing a much larger group of technical managers capable of leading teams of cybersecurity experts, ensuring they are doing the right things and that their work is of high quality and is communicated effectively.

Contact Information: Alan Paller, Director of Research, The SANS Institute, apaller@sans.org

Background: The Challenge of Managing Technical Cybersecurity Teams

With tens of thousands of new cybersecurity professionals joining the work force, a new generation of managers is needed. They must be able to command the technical respect of the technologists, make wise decisions on optimal allocation of people and money, build bridges to other teams, and persuade other executives that cybersecurity initiatives and budgets are justified and cost-effective. Of these requirements, the most challenging to find among potential managers is the technical expertise to command the respect of people with advanced technical skills and to determine, with technical fidelity, what actually needs to be done to protect the specific systems for which they are responsible.

Because technical skills are rarely found in general managers, the direct path to leadership development in cybersecurity is the enhancement of management and communications skills for people with deep technical skills. An alternative path is simultaneous development of both deep technical skills and management skills. A program has been quietly developing highly skilled technical cybersecurity managers for five years. Here is that program through the eyes of extraordinary technical cybersecurity managers whom it has produced as well as a Citi leader who has sent many developing managers through the program.

Extraordinary Technical Cybersecurity Leaders

David Martin, Supervisory Special Agent, FBI Cyber Division, Technical Operations Unit

"From inexperienced new FBI agent to supervisor of an elite FBI technical unit"

David Martin has worked in local, state, and federal law enforcement for the past 15 years. He has a Bachelor of Science in Computer Science from the University of Denver. When he began the Cybersecurity Technical Management Development Program (CTMDP), he was an FBI Agent investigating computer intrusion cases in the Detroit Field Office. As he developed additional technical and management skills through the program, he was promoted to Supervisory Special Agent in the Cyber Division's elite Technical Operations Unit. There he is responsible for running CAT, the FBI's computer intrusion response "fly team," responding to the significant cyber threats facing our nation.

> *"The technical and leadership skills I learned [in the CTMDP] allowed me to progress from an inexperienced new agent to a forensics and incident response subject matter expert, and also to become a supervisor of the most elite technical unit in the FBI.*

[Giving back to the community] Effective written and oral communication skills are keys to management success. During CTMDP, David worked with his program advisors to publish and present research including *Tracing the Lineage of DarkSeoul*, a case study of the April 2013 "DarkSeoul" cyber-attack in South Korea, and *OS X as a Forensic Platform*, which examined the process of configuring a native OS X forensic environment that includes many open source forensic tools. This latter paper served as a guide for his own incident response team, and has proven to be useful to many other forensic professionals.

Michael C. Long II, Cyber Operations Specialist, US Army Cyber Command

"From a basic cyber security role to a "special mission unit" to a candidate for promotion"

David's last annual performance review specifically recognized his accomplishments in the Cybersecurity Technical Management Development Program, including writing white papers, presenting his research at a national cybersecurity conference, winning Capture The Flag competitions, and earning industry-recognized skill-specific security certifications. Michael is currently waiting for the results of a centralized promotion board decision expected this fall.

The "cyber selection process," through which he won his assignment to serve on a special unit mission, included over 50 hours of highly technical challenges, in-depth interviews, two papers, and more. Michael was 1 of 6 candidates selected from an initial pool of over 200 individuals. He attributes his success directly to the knowledge and skills gained through the CTMDP.

> *As a result of the selection, I have been able to serve on many high profile cyber operations, improving the security of systems across the Army. The skills I've learned in the CTMDP allowed me to take a leadership role in these operations, and I've been credited as being amongst the best Cyber Soldiers the Army has to offer. This work is challenging and rewarding, and I am grateful for the opportunity to serve, and for the CTMDP for helping me get here. The CTMDP allowed me to learn from the industry's best, and I am exceptionally grateful to have received the opportunity.*

Jim Beechey, Director, Information Security, Consumers Energy

From being the sole infosec person t leading a team of 35 security professionals.

"When I began the CTMDP, I was leading a three-person team and was the lone InfoSec-focused person." Just after he joined the program, he was hired by Consumers Energy as IT Security Manager. The CIO at Consumers credited his acceptance into the CTMDP as a key reason for offering him the leadership job. By the end of the program in 2013, he said, "my team is 35 strong and growing." Just after the program was completed, he was promoted to Director, Information Security and has served in that role since.

Rod Currie, Information Systems Security Manager, The Boeing Company

When Rod joined the CTMDP in 2015, he was working as an Information Systems Security Officer at the Boeing Company. During the program, Rod was promoted to Program Security Lead, and was recently promoted again to Information Systems Security Manager.

Rod began the CTMDP in early 2015. He had recently been given a new title and a host of new leadership responsibilities, all unexpected and somewhat unwanted at the time. He was able to immediately apply what he learned in his CTMDP courses to carry himself with confidence in his new role. Rod was recently promoted again, from Information Systems Security Officer (ISSO) to Information Systems Security Manager (ISSM), taking on responsibility and signature authority for all mission computer systems across several different flight-test locations.

Leadership within his organization has acknowledged Rod's development into a more competent, composed, and well-prepared incident handler as a result of the coursework in the CTMDP. Rod particularly valued learning how to build a risk prioritization matrix to present to management in the face of a staffing shortage and overall lack of support from leadership. The ability to effectively present risks to management and appeal to the individual stakeholders allowed him to drive the results he intended.

[Giving back as part of the CTMDP] Rod has done extensive research into automotive security. His published research includes *The Automotive Top 5: Applying the Critical Controls to the Modern Automobile* and *Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering*.

John Hally, Technical Director of Information Security, EBSCO

When John joined the CTMDP in 2007, he was working as a network and information security engineering team lead at EBSCO. Shortly after graduating from STI, John left EBSCO to pursue some independent opportunities, returning to EBSCO in 2015 in their senior security position.

John notes that the CTMDP enabled him to bridge the gap between the technical aspects of his work and the equally important project and business processes which are part of his portfolio in this more senior current role. His ability to merge the technical and the leadership components of information security “is a direct result of the broad range of skills and competencies that I have learned during my CTMDP studies.”

Aron Warren, Technical Lead, Sandia National Laboratories

Aron joined the CTMDP in 2011. At that time, he was a member of the technical staff at Sandia. Having set himself the goal of being promoted to technical lead, Aron “landed the job before completing the program, which is not uncommon for CTMDP participants. Every time I reflect on what has transpired during the work week it still excites me when I see how the CTMDP taught the skills to be a better technical lead.”

Reflecting on the topic of leadership in the field of information security from this new role and vantage point, Aron says that “Organizations value those who can lead because so many can’t. In this regard, the CTMDP design is spot on. Courses are geared towards building both leadership capabilities and in-depth technical skills. The program, with its management courses, public speaking requirements, and realistic and challenging group projects was really beneficial in developing my leadership skills.”

Giving back through the CTMDP: Aron’s papers and presentations covered:

1. *An In depth Look at Tuckman's Ladder and Subsequent Works as a Tool for Managing a Project Team;*
2. *Tor Browser Artifacts in Windows 10*
3. *Using Sulley to Protocol Fuzz for Linux Software Vulnerabilities*
4. *Setting up Splunk for Event Correlation in Your Home Lab*
5. *InfiniBand Fabric and Userland Attacks*
6. *Diskless Cluster Computing: Security Benefit of oneSIS and Git*

Rich Arellano, Program Manager, Citi Security & Investigative Services, Citigroup

“A key goal of the Citi executives who decided to send employees to the CTMDP was to help our security professionals write better reports on key security issues. Security improvements become reality only if they are communicated effectively by leaders in the organization. We can now prove that the people who are participating in the CTMDP are contributing to the leadership effort by writing more effective security reports than the other people we have working on information security. One of our Citi group managers has said that his CTMDP participants have ‘set the bar for how to present security information effectively, and that the other people in the group now try to raise their game to meet that standard.’ That is the leadership that we need, and we are getting it from our employees who are in the CTMDP.”

Michael Weeks, Security and Threat Intelligence Analyst in Critical Infrastructure in the electric sector and Cyber Operator for the USAF Reserve

Michael's studies at the CTMDP took his technical, leadership, and managerial skills to the next level. Because of the knowledge he gained while in the program, he was promoted to Security Operations Center (SOC) Manager. Michael was also promoted within the USAF Reserves to E-9 in a cybersecurity role.

Michael particularly valued learning Malware Analysis and Reverse-Engineering s part of the program, and his published research includes *Intrusion Analysis Using Windows PowerShell* and *Application White-listing with Bit9 Parity*.

Additional Statements Attesting to the Effectiveness of the CTMDP

"I have seen a direct correlation between my education and my professional career. From both public speaking to technical capabilities, I have increased my confidence and technical knowledge allowing me to be a more productive member within my team." (Nathaniel Quist, Incident Response Engineer, LogRhythm)

"I looked at a number of different programs, and the decision-making process looked like this -- I don't need more theory, I need more practical, hands-on experience, and that's exactly what the CTMDP offers." (Kevin Altman, Engineer-in-Charge/Program Manager, ICS Cyber Security, TransCanada)

"Ten years ago, almost to the day, I decided to change careers…I wanted to be in information security, it was an absolute... I have only been able to accomplish what's come to fruition in no small part thanks to the people who make up the CTMDP. From the curriculum, the students, the instructors, the faculty... this Institution has changed my life for the better, without question, in so many ways. This day, and every day hereafter, I am deeply proud to be a graduate of the CTMDP." (Russ McRee, Principal Group Program Manager, Microsoft)

A Final Word:

"CTMDP" is a generic name used only in this document. The actual program name is the Masters Degree in Information Security Engineering and Management awarded by the SANS Technology Institute (STI).

In July, 2017, STI awarded 28 masters degrees, a quadrupling of the number of degrees over the previous graduation. More than 150 technical cybersecurity professionals are now enrolled in the program, a doubling over just two years. That growth provides evidence that STI is ready to take on the much larger job of preparing technical managers for hundreds of organizations in government and the critical infrastructure.