JANUARY 16, 2018

Legaltech news©

ONLINE

An ALM Publication

Unit 8200 CEO Takes Accelerated Learning to the Cyber Masses

Cybint's Roy Zur aims to bridge the talent gap in cybersecurity by providing highly technical online self-guided certification

BY JARED COSEGLIA

As a major in Unit 8200, the elite cybersecurity Israeli intelligence corps, Roy Zur was tasked with finding ways to rapidly train inexperienced young soldiers on the basics of cybersecurity technology. "How do you take 18-year-old kids and train them to become relevant within a few weeks for their two to three years of service in the army?" asks Zur.

Unit 8200, often compared with the credibility and capability (though not the scale) of the NSA in the United States, has traditionally been composed of 18 to 21-year-olds and even boasts a scouting program to entice and identify the appropriate talent as early as age 16. Due to the brevity of their expected years of service, the unit aims to recruit individuals with the aptitude to rapidly learn new skills. Zur was tasked with training the next generation of cybersecurity special forces.

"The need to develop new methods to allow someone to immediately start working productively is the definition of accelerated learning, which we have now applied to Cybint's process and technology for commercial consumption," says Zur.

Cybint Solutions, a subsidiary of Barbri and parent company to the ACEDS certification in e-discovery, boasts three levels of training and certification. Level one focuses on cybersecurity awareness and integrates basic cyber disciplines in a non-technical faculty. Two certifications can be achieved in level one, the CIC (Cyber Intelligence Certification) and the CSPC (Cyber Security Protection Certification). Level two develops hands-on technical skills through custom labs, real-time threat alert simulations, virtual mentors, hands-on practice scenarios and more. Level two students can achieve a CSAC (Cyber Security Analyst Certification). Level three at Cybint is about specialization and deals in an advanced itinerary of training for working threat analysts looking for greater nuance within their existing portfolio of skills.

JARED COSEGLIA

Cybint's go-to-market strategy, like many security awareness and training companies, is focused on B2B and B2E rather than B2C client acquisition. For companies or educational institutions looking to give their employees or students tactical and technical SOC (security operation center) skills, level two is the ideal investment. "Level two training and the CSAC were designed to bridge the multimillion-person talent gap in cybersecurity," says Zur.

The level two lab is both a learning and a practice environment. Students can work at their own pace and have unfettered access to content and virtual servers hosting a wide array of proprietary and open source technology. Users will interface with Snort IDS for intrusion detection and prevention, Nmap for network management, Sysinternals utilities to help troubleshoot and diagnose Windows systems and applications, Cuckoo Sandbox for automated malware analysis, Metasploit for penetration testing and other software and operating systems like Wireshark, MySQL, Linux, and more. "We chose the easiest tools to teach and believe once they learn these, students can quickly pick up equivalent tools that address similar solutions," adds Zur. "If you can learn to read logs for anti-virus in one tool, you can learn them in any tool."

Students also receive simulated threat alerts in their dashboard where they can practice incident response best practices and techniques.

Cybint has employed a variety of experts to craft the lab alerts from PhD's in accelerated learning and gamification to CISOs from major corporations and consulting firms. The lab alerts indicate a cyberthreat on the user's screen that then triggers the user to complete a series of actions to problem-solve the threat. All alerts are based on real-life cybersecurity events. Each alert initiates a different case scenario and engages the student on different technology in the portfolio. These tasks may be as simple as dealing with infected files, learning how to quarantine or delete them, and not only gives intelligence on what to do and how to do it, but also explains the pros and cons of each solution option and why some are better than others.

There are 12 core scenarios built into the Cyber Security Analyst Certification curriculum. These include identifying suspicious FTP/HTTP traffic or unusual activity by a domain administrator from a VPN connection, troubleshooting an endpoint and server machine trying to log in with the same username and password at the same time, writing vulnerability assessments of an enterprise email server, building graphic dashboards to detect statistical anomalies and remediating an attack on a cloud service server. "Working as a cyber analyst is really hands-on technical work," articulates Zur, "and our scenarios are teaching users how to be proactive in reactive situations by delivering triggers that force a response."

While scenario 12 of 12 focuses on penetration testing, the core of Cybint's level two training is largely on incident response. When asked why the training emphasis has been placed on the reactive arts of cybersecurity, Zur states simply, "Because that's where the biggest demand in the job market exists." Not only is demand high and supply low for incident response talent, breach remediation is quickly becoming the most expensive and potentially brand damaging variable in a complicated cybersecurity and risk management equation.

Cybint is determined for its program to ultimately help people get jobs, so much so that the final exam for the CSAC is a mock interview based on real interviews with CISOs. Zur proclaims, "The CSAC training builds confidence around job interviewing, because users have to actually solve real problems on the spot in the final exam."

The CSAC level two training can be used not only to educate and prepare more novice talent for a career in cybersecurity, but also to validate and measure the skills of existing employees within an organization. Cybint boasts an ongoing assessment functionality that allows employers to identify the gaps in knowledge bases for threat analysts. This allows some users to test out of specific lab scenarios and accelerate their training to more sophisticated areas of expertise. Zur comments, "We have found that larger organizations hiring top talent sometimes have internal training programs, but many organizations don't know how to assess the talent they have on staff or are looking to hire."

Level two also has a virtual mentor built into its process that helps students with "what to do next" if they hit roadblocks in their training. The virtual mentor accompanies each user through the entire training to understand the implication of each alert, create awareness around the known and unknowns of each scenario and question user thinking and decision-making along the way. There is also a group chat discussion portal for SOC teams to collaborate and communicate if taking the training as a unit.

Cybint does not want to be a school but rather to augment the curriculum of universities with cybersecurity programs. "A computer science major may not get the skills or tool exposure that we provide, and the CSAC training helps fill the gaps in hands-on technology skills needed to be employed in the industry," professes Zur. Many of Cybint's flagship customers are in fact universities. "Higher education institutions are adopting our training and integrating Cybint into their computer science departments to make their degree programs more hands-on."

While many large financial institutions can and will pay top dollar for experienced professionals, many midsize companies will have to find other ways to elevate or train talent to meet increasing regulatory requirements related to security. Hiring managers will need to be more open-minded about hiring for people with promise and potential and not just proven experience. Security experts may become experts by stepping up and into the role, and some organizations will need programs like Cybint to pave the way for those professionals to add value quickly. Otherwise, employers will need to open their wallets to meet the salary demands of those who are already established as experts in the field—at least for now.

Cybint will be offering eight free CSAC passes through the **TRU Scholarship Program** in 2018. Applications will be open for the program in late January.

Jared Coseglia *is the founder and CEO of TRU Staffing Partners, an Inc 5000 Fastest Growing American Company 2016 and National Law Journal's #1 Legal Staffing Agency, and has over 13 years of experience placing thousands of professionals in e-discovery, litigation support, cybersecurity and broadly throughout legal and technology staffing.*

Reprinted with permission from the January 16, 2018 edition of Legaltech News. © 2018 ALM Media Properties, LLC. All rights reserved.
Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. #010-01-18-03