CASE STUDY

Cybersecurity Skills Shortage is Critical and Getting Worse

Boosting Singapore's Cyber Security Skills

A January 2018 survey report published by ESG[3] revealed that 51% of organizations have a problematic cybersecurity skills shortage. It is yet another indicator that organizations could be heading toward a cyber-security skills crisis; back in 2014, ESG reported that only 23% of enterprises said they had a shortage of specialist cybersecurity skills.

These latest findings correlate with an earlier research project conducted in late 2017 between ESG and the Information Systems Security Association, which revealed that 70% of cybersecurity professionals felt that their organization was impacted by the skills shortage. The effects of this included an increasing workload on cybersecurity staff, the hiring of junior personnel that required training rather than experienced pros, and a culture where the cybersecurity team was consumed with firefighting issues as and when they arose rather than working strategically.

In the specific case of Singapore, the Cyber Security Agency evaluates the country's demand for cyber security professionals to be expected to grow from 4,700 in 2015 to 7,200 in 2018 and 9,700 in 2021.[1]

What can be done to help address this problem? How can information technology (IT) organizations develop the elite cyber warriors they need to protect

Company

Singapore's financial, technology, government, and educational organizations

Key Issues

- Demand for cyber security professionals is expected to grow from 4,700 in 2015 to 7,200 in 2018 and 9,700 in 2021
- Cyber security skills gap leaves 1 in 4 organizations exposed for 6 months or longer
- 55% of hiring managers report that practical, hands-on experience is the most important cyber security qualification

KEYSIGHT TECHNOLOGIES

their assets and customers? To address this issue, we looked at our portfolio of technology and expertise to offer the industry a hands-on approach to stay current, upskilled, and updated on the latest tools and technologies.

From Conventional Warfare to Cyberwarfare

Just because warfare is moving to the cyber realm, it does not mean that lessons from real battlegrounds have lost their relevance and significance. The main rule from Sun Tzu's Art of War still applies: if you know the enemy and know yourself, you need not fear the results of a hundred battles.

To know the enemy's warcraft, aspiring cyber warriors can leverage the knowledge of security experts, such as the Ixia Application and Threat Intelligence (ATI) Research Center, that offer exposure to 6,000+ live attacks, 35,000+ malware, 330+ application signature families, distributed denial of service (DDoS) and botnet attack simulations.

To know themselves, cyber defense teams need to be tested in real-life conditions in a cyber range environment to practice on a realistic production-like environment integrating a multi-vendor agnostic environment.

The best cyber warriors train, train, train. They test their limits at the cyber range. They train for combat with multiple simultaneous scenarios and enemies. They train to the breaking point with scalable real-world traffic and attacks.

Ixia Cyber Combat Event: Offering Hands-On Experience to Cyber Warriors

This is why we recently ran the Ixia Cyber Combat competition in Singapore, where 20 teams of cyber security industry professionals and students competed to test their skills against one another.

The objective of the competition was to present cybersecurity in an exciting and engaging context to potential professionals of the future and enable security professionals to hone their skills in simulated cyber security attack scenarios.

Participants came from a range of industry backgrounds, including financial services, technology, government, and education. During the contest, the teams competed to take down enemy servers, expose vulnerabilities, and win flags while defending their home ground against enemy attacks. The participants were exposed to a range of new tools, skills, and situations.

Each two-person team was made of an attacker (red team member) and a defender (blue team member). Victory was defined as successfully mastering the combination

Solutions

- Ixia Cyber Combat Live Events
- Ixia BreakingPoint
- Ixia Threat Armor
- Fortinet NGFW
- Quali Orchestration
- Splunk

Results

- S$10,000 prize for the winning team
- 20 two-person teams of security-focused technical participants experienced 12 hours of intense expert-level cyber security hands-on challenges
- 60 c-level business observers assessed a cyber range approach to addressing the cyber skills gap

of infiltrating opponents' servers while diligently defending their own over a 12-hour timeframe. All teams resided in the same Cyber Range environment on the same network with over 250 flags to capture and defend. More than 40% flags were designed to test the latest security breaches.

Red team players had to use the best techniques of network infiltration, data mining, and exfiltration. Red team scenarios were:

- Discovering, enumerating, and infiltrating Windows and Linux servers defended by a Fortinet NGFW
- Exfiltrating and cracking salted, hashed passwords stored in databases
- Searching penetrated machines for valuable data hidden via steganography
- Combing through metadata for breadcrumbs of valuable information
- Writing custom scripts to unlock data

Blue team players had to race the clock in rapidly identifying ongoing attacks, hardening their servers, tuning their security infrastructure, and even rooting out attackers inside the networks they were protecting. Red team scenarios were:

- Monitoring SIEM and NGFW logs for ongoing attacks
- Modifying configurations to thwart attackers
- Examining network traffic, and correlating events to discover and stop coordinated attacks

> **"It was a stressful but fun experience. In the end, we came from behind and took the show."**
>
> - Ang Guo Gen, co-winner of the competition, Singapore Institute of Technology undergraduate, intern at Wizlynx (Switzerland-based cyber security service provider)

The Ixia Cyber Range platform presented in real-time a dashboard of key performance indicators for teams, individuals, and executives to learn from scenario success rates, red team performance, blue team performance, and individual cyber warrior performance.

The entire Ixia Cyber Combat event was executed on the Ixia Cyber Range in a box, called "The Beast", composed of Ixia BreakingPoint on Ixia PerfectStorm, Ixia Threat Armor, Fortinet Next-Generation Firewall (NGFW), Quali Orchestration, and Splunk Security Information Event Management (SIEM).

Conclusion

The Ixia Cyber Combat competition in Singapore provided a unique high-pressure experience to the cyber security professionals who participated. They brought back to their organization new insights and perspectives on cyber warfare. Their associated C-level business observers took away the importance of realistic cyber range exercises and how such events can be setup and run effectively and efficiently with Ixia security solutions.

High-performance skill-building programs need to offer new scenarios and attack elements all the time to build up the right level of adaptability the new elite cyber warriors will need in real situations. As the U.S. Marines say: "Improvise, Adapt, Overcome". The ATI Research Center regularly feeds new live attacks, malware, and application signatures to Ixia Cyber Range simulations so that cyber cadets face new situations every time.

Develop the best cyber warfare professionals by teaching them to know their enemy, their techniques, and their view of the IT world, and help your cybersecurity team know themselves by training all the time at the cyber range. Elite cyber warriors train on elite cyber range.

References

1. https://www.computerweekly.com/blog/Eyes-on-APAC/Plugging-Singapores-cyber-security-skills-gap
2. https://www.businesswire.com/news/home/20170213005553/en/ISACA-Survey-Cyber-Security-Skills-Gap-Leaves%20https:/healthitsecurity.com/news/how-healthcare-it-teams-bring-value-and-security-to-providers
3. https://research.esg-global.com/reportaction/blog0111201801/Toc?SearchTerms=survey%20of%20620

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus