Train, Retain and Gain

How to put a stop-gap in your cybersecurity staffing skills gap.

THE EVER-CHANGING CYBERSECURITY LANDSCAPE AND GROWING DEMAND FOR CONNECTED BUSINESS MEAN THAT THE PRESSURE TO FIND AND RETAIN HIGHLY SKILLED CYBERSECURITY PROFESSIONALS IS NOT GOING AWAY. HOWEVER, IT IS MANAGEABLE WITH GOOD RECRUITING PRACTICES AND BETTER EMPLOYEE RETENTION POLICIES BUILT ON A "TRAIN AND RETAIN" APPROACH.

THE CYBERSECURITY SKILLS GAP

An estimated **1.8 MILLION** cybersecurity jobs will go unfilled by 2022[1]

The number of jobs in the security space will increase by **18%** between 2014 to 2024[2]

Research conducted by **451 Research in 2018**[3] reveals that of those companies that face a skills shortage:

62% believe they can address the skills gap by training existing staff to learn new skills

22% plan to outsource their security needs

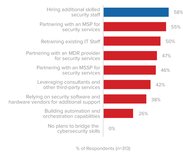
ADEQUATE STAFFING LEVELS DO NOT EQUAL ADEQUATE SKILL SETS

87% of organizations feel their cybersecurity staffing levels are adequate[3]

78% also feel they have a skills/expertise gap[3]

A REALITY CHECK

How are you bridging the skills gap?[3]



[1] https://blog.isc2.org/isc2_blog/2018/09/cybersecurity-hiring.html
[2] https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[3] 451 Research, study commissioned by eSentire, June 2018
[4] 451 Research, study commissioned by eSentire, Cybersecurity Investment Dynamics 2018
[5] 451 Research, study commissioned by eSentire, June 2018

A SELF-FULFILLING PROPHECY

Organizations believe there are not enough qualified professionals to fill the open positions yet:

58% are trying to hire additional staff in order to meet their cybersecurity needs

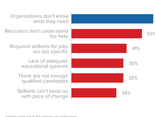
2/3rds believe retraining existing staff is the way to go

Yet only **half** of organizations say they are doing that.

Organizations are essentially creating a self-fulfilling prophecy based on the widely reported skills gap. They believe they cannot get the skilled talent they need, but they continue trying to fill open positions while neglecting to retrain existing talent, thus perpetuating the skills gap.

WHAT DO THE CYBERSECURITY PROFESSIONALS THINK IS THE REASON FOR THE SKILLS GAP?[4]

791 answers from 297 respondents



*Volume adds up of 451 cybersecurity professionals

CYBERSECURITY PROFESSIONALS AGREE WITH ORGANIZATIONS ON WHAT IT TAKES TO ATTRACT AND RETAIN TALENT[4]:

63% want ongoing education and certification programs

57% point to higher salaries and better benefits

TRAIN AND RETAIN

Cybersecurity professionals plan to stay in their roles for the long haul.

47% plan to stay put for at least five years

52% are trying to obtain additional certifications

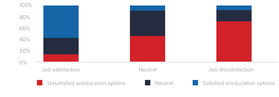
And, they are in agreement with employers on how to address the skills gap.

63% of professionals feel that ongoing education is the key to attracting and retaining talent.

62% of organizations agree that training existing staff to learn new skills is the answer.

Continuing education options directly correlate to job satisfaction amongst professionals:

Train and Retain: Satisfaction and Education Correlation



RETAIN AND GAIN

Providing a path forward for employees will keep them in place, and the new skills they obtain will help alleviate the burden of the skills gap.

66% believe their skill set constitutes a position higher than the one they currently fill.

49% do not feel appropriately compensated for their current skill set.

ADEQUATE COMPENSATION + ONGOING EDUCATION OPTIONS = STOP-GAP IN THE SKILLS GAP

IT TAKES 6 MONTHS TO FILL A CYBERSECURITY POSITION.

Job satisfaction for existing employees is paramount to avoiding costly turnover and retaining good talent.

DON'T HAVE TIME TO WAIT WHILE YOU PUT PROGRAMS IN PLACE?

eSentire can help you maintain a strong security posture while you plan for the future. Our services are designed to remove the staffing burden by pairing the strength of machine learning with integrated human threat hunters to give you full threat visibility and immediate action 24x7x365.

Machine

+ Patented machine learning processes
+ Patented inspection and disruption of encrypted threat traffic
+ Multi-tenant cloud native data pipeline
+ Continuous data correlation including PCAP, endpoint and log threat intelligence
+ Deep machine inspection across cloud and on-premises
+ Data aggregation to single threat dashboard
+ Continuous auto enrichment
+ Automated threat blocking
+ Integrated whitelisting and malicious IP blacklisting
+ Continuous countermeasure development
+ Customized Threat Intelligence integration

6+ INVESTIGATIONS EVERY MINUTE

646 CONFIRMED SECURITY INCIDENTS A DAY

Human

+ 24x7 Human analysis and investigation
+ 100+ SOC personnel
+ Continuous education curriculum
+ Industry leading certifications
+ 3 Analyst levels
+ Fully integrated threat hunting team
+ Fully integrated Threat Intelligence team
+ Fully integrated response team
+ Human-led tactical threat containment

ACCELERATING RESPONSE TIMES AND MINIMIZING THREAT ACTOR DWELL TIME AND THE RISK OF BUSINESS DISRUPTION

35 AVERAGE SECONDS TO BEGINNING TRIAGE

20 MINUTES AVERAGE TIME TO ISOLATION AND CONTAINMENT

Modernized business demands modernized security.
eSentire Managed Detection and Response

TAKE ACTION

eSentire, Inc., the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Since 2001, the company's mission has been to hunt, contain and investigate advanced threats that bypass traditional security controls and put critical business assets at risk. Protecting more than 1,000 customers in 70+ countries from its state-of-the-art security operations centers in North America, eSentire absorbs insider and perimeter threats around the clock, so its customers can focus on growing their business. For more information, visit **www.esentire.com** and follow **@eSentire**.