Secureworks®

WHITE PAPER

Enhancing Security Skills With Secureworks

Cybersecurity Professionals Can Never Stop Learning If They Want to Succeed in a Rapidly Changing Industry

The cybersecurity skills gap is here to stay. The global nature of business today, combined with increasingly sophisticated threat actors and complex security environments, has created high demand for skills that are often in short supply.

One of the main ways for cybersecurity professionals to keep up under these circumstances is to keep learning and developing. Cybersecurity is home to a lot of self-starters. Some people find their way to the industry through formal education such as bachelor's and master's degrees. Equally as many develop a passion for it and train for certifications by themselves. Regardless of an individual's route to the industry, a commitment to the profession means welcoming a lifetime of learning. Constant education and training are the most effective way for security practitioners to evolve with the security landscape. This paper will identify actionable steps and resources for continued professional growth that will enable you and your cybersecurity teams to stay at the top of your game.

Some organizations have moved away from annual merit programs in favor of bonuses and reward programs tied to achievements and milestones evaluated by peers.

Internal vs External Professional Growth in Cybersecurity

There are two main sources of professional growth for any cybersecurity practitioner. The first comes from inside the organization where they work. This includes learning from colleagues, as well as company sponsored certification training. The second source of growth is external. This includes relationships with a vendor's experts and access to tools that help professionals learn and grow.

The cybersecurity profession is relatively unique among jobs in the tech industry, in that a significant portion of security practitioners come from a self-taught background without extensive formal training. Of course, many people in the industry have trained at college, sometimes to a postgraduate level, but this path is not a requirement for most entry-level cybersecurity jobs. The most applicable certifications for cybersecurity jobs can often be taken in a self-guided manner, using a wide range of online resources. This fact, combined with the rapid pace of change in the industry, means on-the-job training is the norm. Whether someone has a postgraduate degree or is self-taught, they will struggle to advance in their career without taking advantage of both internal and external sources for professional growth.

The advice of experienced colleagues is an invaluable source for learning. Observing and inquiring as you work along with senior colleagues is an incredibly effective way to gain industry experience. In fact, peer support and training is a key part of a practitioner's career advancement. Some organizations have even moved away from annual merit programs in favor of bonuses and reward programs tied to achievements and milestones evaluated by peers.

This emphasis on peer support and collaboration has led to security becoming a tight-knit community where professionals look to learn from their peers across the industry. This external source of professional growth can be seen across a wide range of events, including RSA conference, Black Hat, DEFCON, Hackers on Planet Earth, as well as many local conferences and competitions. The best in the industry actively engage in these events to connect with the wider security community, network, and share knowledge.

There's an additional source of professional growth that many professionals and organizations overlook: vendors. The right vendor relationship can be invaluable for professional growth and knowledge-sharing. Vendors with deep security expertise and a long history in the industry represent an excellent source of knowledge for you and your team, and you have every right to expect them to share it with you. A vendor's tools should also equip you with the context you need to understand what's happening in your environment. Over time, this grows your knowledge of threats and how to address them. Any vendor tool should also put you and your team at the center of every decision.

Of course, this is all dependent on the vendor you choose. Not every vendor has a long history in the industry with high-caliber security talent on staff. Not every vendor designs tools in a way that helps the user learn as they use them.

Vendors with deep security expertise and a long history in the industry represent an excellent source of knowledge for you and your team, and you have every right to expect them to share it with you.

Secureworks as a Resource for Professional Growth

Secureworks is proud to help our customers learn from our expertise and through our tools. For over 20 years, our team of world-class experts has protected thousands of organizations globally. We believe in building deep working relationships founded on knowledge-sharing and 24/7/365 support that means customers can contact an expert whenever they need.

This ethos also shapes the solutions and products we offer. Using a tool or interacting with a solution shouldn't just be a process of following rote steps. Powerful tools provide users with context that arms them to understand every decision they need to make. Here are some Secureworks solutions that achieve that for our customers:

Red Cloak™ Threat Detection & Response (TDR) and Managed Detection & Response (MDR)

Secureworks Red Cloak TDR is a cloud-native software application that uses security analytics and AI technologies to analyze events in your environment and only escalate those that matter.

Red Cloak TDR presents you with all the context you need to understand the severity of events in your environment. Through contact with this contextual information, your team will learn about the hallmarks of the different threats that are targeting your organization. Suggested containment actions will also demonstrate the most effective ways to contain whatever threats are detected.

An instant chat box removes the ticketing model and offers collaboration with our experts, 24/7/365. Collaborative event investigation means your team and our experts can work together to understand events, sharing knowledge in the process. Our MDR service offers all the same benefits of Red Cloak TDR, with our experts handling the day-to-day use of the software. Your team gets access to the software and chat box so they can validate and learn from what our experts are doing.

Advanced Endpoint Threat Detection (AETD) Elite Service

AETD is fully managed and hosted endpoint protection, equipped to find advanced threats using behavioral detections. This service helps your team grow with regular proactive threat hunting and weekly meetings where our experts share their findings. During the meetings, security professionals can discuss and view threat hunt findings through a shared portal. You get an opportunity to understand what our experts found, what it means, and what you should do. You can also continue investigation using the basis our experts provide. This collaborative, proactive approach helps enhance security efficacy and gives security professionals regular access to Secureworks experts to help grow their knowledge base.

Knowledge-Sharing Meetings

Secureworks also offers on-site or virtual meetings focused on conversation about what's happening in the security industry at large. These informal meetings are a time for Secureworks experts and security executives within an organization to discuss shared experiences and exchange knowledge around best practices and happenings within the industry.

A Consultative Relationship

Secureworks offers a consultative partnership which addresses every incident and security challenge in the wider business context, as well as the risk to an organization's other lines of business or services.

Secureworks also partners with security practitioners to provide prescriptive advice, helping build a knowledge-sharing relationship with our customers. We scale knowledge-sharing across our entire customer base by applying lessons learned from mitigating threats for the benefit of all our customers. Our Counter Threat Unit™ researchers provide advice and threat intelligence based on the full, global context of activity across our customer environments. This enables us to go far beyond perfunctory threat intelligence, which often merely points out something is a threat because it's been observed in a certain industry, targeting a certain set of applications.

Never Stop Learning

The speed of change in cybersecurity is one of the reasons it's such an interesting industry to work in. This change also makes continual education a necessary condition for becoming a top security practitioner. As the threat landscape and preferred technology in the industry evolves, analysts look for ways to keep up. For many security practitioners, this comes naturally. Self-directed, or organization-sponsored study, are common ways for practitioners to challenge themselves and develop skills to meet the complexity of security today. Likewise, learning on the job alongside senior colleagues is common practice.

While each of these sources of knowledge is important, they have limitations. Certifications equip you with the mental tools to problem solve using logic informed by solid security foundations. What they don't do, is tell you exactly how threats are behaving in the wild today, or how organizations are successfully addressing them. The same is true of learning from colleagues: each colleague is limited in their experience, no matter how formidable that might be.

For a truly global and current view into what is happening in security, there is an effective solution: partnering with a vendor with a global customer base whose activity is monitored by a team of world-class threat researchers. This vendor must also readily and openly share their knowledge with you and be available whenever you have queries. One effective way of identifying whether a vendor is willing to help your team grow, is to ask them how you can use their products, solutions, and services to develop the skills and knowledge of your whole team. If a vendor has built their portfolio with this as a key consideration, they'll offer a detailed and convincing answer.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp