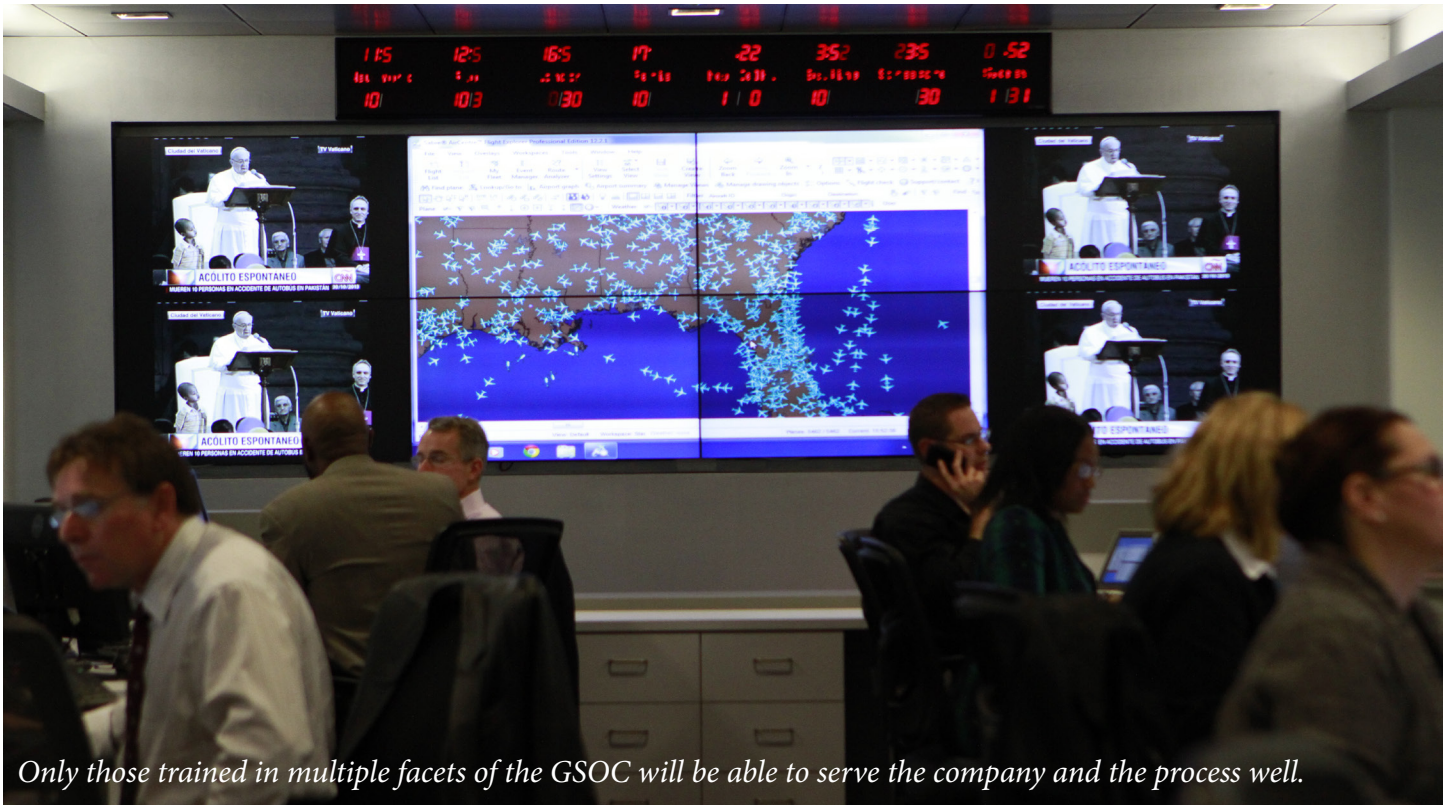
SIW SECURITY INFOWATCH.COM

# Focus on:
## *Security Training Trends*




*Only those trained in multiple facets of the GSOC will be able to serve the company and the process well.*

Courtesy of CMoor

## The GSOC and the Evolution of Security Training Trends

*Security executives share their insights to constructing an operations center that works*

**Author: Connie Moorhead**

Everywhere you look there is another article, blog, social media post or trade show session related to Global Security Operations Center (GSOC) technology and operations. Depending on who you ask you will get differing views of what the goal is for an organization's GSOC. But ultimately, when the hype is removed, the GSOC's objective comes down to identifying threats, mitigating risks and keeping the entire organization safe by informing and giving a more global view of corporate operations. It is not an easy task.

This discussion is not aimed at the overall benefits and challenges of implementing a GSOC nor is it a debate about when and where a GSOC should be put in place. That's been done. My purpose is to stick to what you know, and that is training. Our goal in this piece is to look at the GSOC from the perspective of training requirements it brings with its launch, maintenance and the many-faceted challenges that a GSOC imposes on your strategic training initiatives.

## What is the Industry Doing Today?

When searching for training on the GSOC you are more likely to get links to the Girl Scouts of Orange County or Gopher State One Call courses. But finding a large listing for training (classroom or online) for GSOC operations or analysis is challenging. Finding a specific certification is even more challenging. One reason for this may be the vast variances we see when defining the key factors driving the implementation and support of the GSOC. At a minimum, a GSOC should increase operational efficiency and improve risk management.

Where there is a technology being aggressively sought and an abundance of hiring taking place for said technology, one thing comes to my mind and that is training. There were 116 open jobs listed on LinkedIn and more than 8,300 positions listed on Indeed following a cursory search of companies seeking to hire for skills directly related to the GSOC. ZipRecruiter lists more than 156,282 unique positions related to the GSOC including management, operators and analysts. With all this potential hiring and given the growing number of implementations, it stands to reason that training would take a priority seat around the conference room table. But this is not necessarily so.

## Striving to Make a Difference

In the GSOC environment, devices will experience problems all over the world, so a strong partnership with a systems integrator is essential. Language barriers, regulatory requirements, cultural differences, local customs, and inconsistent installation can make this very challenging. Having comprehensive maintenance guidelines documented and available online for regional managers is important to the ongoing viability of your operations.

A wide spectrum of multidimensional threats continue to grow and threaten information assets, with cyber-attack motivations seeing an equally wide spectrum. A reactionary approach to these threats poses too great a risk to critical infrastructures. Companies and people alike must take a proactive stance. Only those trained in multiple facets of the GSOC will be able to serve the company and the process well.

## What is GSOC Training?

When it comes to putting a full and robust GSOC training plan together there are several key things that must be considered.

- There must be security operations training to help you respond to security incidents and vulnerabilities. In doing this you improve your operational security capability and leverage the GSOC analyst and specialist training techniques used in vulnerability management and security information event management (SIEM) platforms.
- Those partnerships you have in place with vendors and integrators should be exploited. Product training is essential. And not just the product installed at your locations but the specifics on how those products are configured for your organization. A customized approach to the training initiative is a must.
- Proper training on the GSOC directly impacts costs and performance in implementation, operations and support. Both by developing a guide for technology selections and learning about proper resource allocation and prioritizing expected deliverables of systems and people, it is only through education that a trusted crisis management system can be put into place.

## A Conversation with Industry Leaders

I recently had the privilege of discussing the GSOC and its related training strategies with three industry influencers. They are Ty Richmond, President, Risk Advisory & Consulting Services and International at Allied Universal, Kayla Prettitore, Technical Program Manager for Global Security at Cloudflare, and finally, Matthew Bradley, Vice President of Global Security Solutions at OnSolve. Each of these industry experts gave me some great insight into GSOC training strategies and methods. Here is our conversation:

***Moorehead: Why do you think there has been a surge in demand for more information related to GSOC operations?***

**Ty Richmond:** Information on the GSOC is in greater demand because the GSOC has become an integral part of the sourcing, distribution and management of situational intelligence, critical event management activity and the overall functionality of the security operations both from the physical and day-to-day operations standpoint.

**Kayla Prettitore**: The GSOC goes well beyond alarm management. A lot of companies are very concerned with the duty of care whether that be IT or cyber, employee care, etc. The GSOC is about how they are providing these resources to their employees.

**Matthew Bradley**: The GSOC is "gaining popularity because there are so many things happening in the world requiring companies to take action. We cannot just watch the news anymore to find out about a situation in a certain location because companies are operating in those places or we have employees traveling there.

***Moorehead: Do you think that training is important to the overall success of the GSOC?***

*Ty Richmond, President, Risk Advisory & Consulting Services and International at Allied Universal.*

**Richmond:** It is more than important it is a necessity. This is because there are processes and protocols and overall response issues that are essential to the performance of the GSOC. There are interdependencies with other critical parts of the organization. Ty Richmond, President, Risk Advisory & Consulting Services and International at Allied Universal.Ty Richmond, President, Risk Advisory & Consulting Services and International at Allied Universal.

**Prettitore:** Training was absolutely necessary. There are a lot of unknown factors that come into play – what they [analysts] need to respond to and what situations will arise. The more you train for these the better-prepared operators and analysts will be.

***Moorehead: What kind of training is most valuable for the GSOC vendor?***

**Richmond:** Whether you are an operator or an analyst or a vendor who is selling and installing certain technology – at the end of the day you are an extension of the customer, you are integral to the GSOC operations in all aspects of the functionality.

**Prettitore:** You want to make sure the company is putting together rigorous training on incident command structure (ISC). This type of training originated out of government and law enforcement. It is imperative! It teaches about what are the roles and responsibilities of people responding to an incident.

**Bradley:** From a staffing perspective GSOC's serve many functions and not all do the same thing. Your training program should support the basic functions of the GSOC such as alarm monitoring, access control, etc. The most important skill is crisis management or incident response training. Looking at the functions of the GSOC most are responsive or reactive. The GSOC is notified of an incident and they must respond to that incident. The ability to respond is independent of the systems being used. In staffing a GSOC I want a thinker – someone who has sound judgment, therefore a value-add is analytical training. We are not talking about turning all operators into analysts but to have the operator learn how to process the information they must have an analytical mindset. Maybe reports are coming in of an incident such as an attack on the streets in Paris – they must analyze that event and determine what to do next. Without this ability to think and respond accordingly, you would have to have a documented procedure in place for every possible scenario which is impossible.

***Moorehead: What kind of training is most valuable for the company putting a GSOC in place?***

**Richmond:** You have a duty of care to make sure you have systems running, people trained and overall coordination with other parts of the organization that are part of the GSOC mission and workflow.

**Prettitore**: Whatever policies are rolled out to the employees such as active shooters or drills for a natural disaster, making sure everyone is trained on what the employees are supposed to do.

*Kayla Prettitore, Technical Program Manager for Global Security at Cloudflare.*

**Bradley:** When it comes to systems being used within the GSOC for things like access control of video management, you must train your operators to use the systems already in place. I am not changing my system, so you need to train on what I have.

***Moorehead: Are there any good industry certifications that support the GSOC concept?***

**Richmond**: Yes, there are some through the Department of Homeland Security designed around critical event management and all related to the operational focus and response.

**Prettitore**: Certifications on ICS or Incident Command Structure are important. These start out in more general terms and then get very specific. There are other certifications from ASIS like the CPP, but these other industry certifications do not pertain specifically to the GSOC., Kayla Prettitore, Technical Program Manager for Global Security at Cloudflare., Kayla Prettitore, Technical Program Manager for Global Security at Cloudflare.

*Matthew Bradley, Regional Security Director Americas at International SOS.*

**Bradley:** There is no industry training that is specific to GSOC operators. The ASIS CPP is a good one for physical security. To certify operators, I would use vendor training to certify them on the systems being used.

***Moorehead: When putting together a proposal for a GSOC, do you recommend a certain amount of time or money be spent on training?***

**Richmond:** It is a fusion center of situational intelligence information. Without a doubt, there are training set-asides.

**Prettitore:** Annual training is imperative as well as ad hoc, hands-on training. Many companies fail to encourage their teams to participate in tabletop drills or all hands-on deck drills. They may do eLearning or scenario-based training but don't do full-scale, hands-on companywide training. Budget ranges widely, but there is a lot you can do in house for a lower cost. Some of the ISC training is even free. Some of the partner systems for AC or video management do tend to get expensive. Doing as much of "train the trainer" as possible will help save on cost.

**Bradley:** Training will be ongoing so you must account for that. I recommend a minimum of 30 days set aside for on the job training. In the first month, we would run the GSOC and not announce it.

***Moorehead: Are there specific topics that are important to include in your training when considering a GSOC?***

**Richmond:** Several areas should probably be standard. One is management and use of the technology that resides inside the GSOC. Two is the response handling protocol for management of information.

**Prettitore:** Sometimes we get bogged down on physical security but the cyberworld bleeds over. Making sure cross-functional training is in place is a must.

**Bradley:** All the systems internal to the client through the vendor or client themselves must have appropriate training associated with them. Hot training topics include incident response, crisis management, and risk management. Risk is preventative and crisis is responsive. Matthew Bradley, Regional Security Director Americas at International SOS. Matthew Bradley, Regional Security Director Americas at International SOS.

To wrap up my conversations I asked each person if there were any other takeaways for our readers. Each one, without pause, noted that training of GSOC operators and analysts has to be a constant and recurring process Training, to be effective, must be a source of constant process improvement. There should be a regular tweaking of the standards by which you manage activity. Another mission-critical thing is making sure that you have support from the top down. If the executives are not adhering to the guidelines for security, then it is hard to enforce with the rest of the global population. When it comes to security, leading by example is the best way to go.

---

*Connie Moorehead is the President of CMOOR and Security-CEU.com, and a highly accomplished executive, with 30 years of experience across physical security, fire and life safety, and manufacturing industries.*

# (ISC)² Partners with CyberUSA to advance cyber education and certification

*Joint cybersecurity workforce development projects to include election security training for state and local governments*

**Source: (ISC)²**

Clearwater, FL, February 4, 2019 – (ISC)² – the world's largest nonprofit membership association of certified cybersecurity professionals – has announced a partnership with CyberUSA, a nonprofit collaborative community of states focused on a common mission of enabling innovation, education, workforce development, enhanced cyber readiness and resilience, and connecting the cyber ecosystem of the U.S. and its allies. (ISC)² will join CyberUSA in its efforts to coordinate public and private efforts across different states and communities to ensure American leadership in cybersecurity by shaping the education, innovation and policy landscapes at both the state and federal levels.

(ISC)² recently took part in the CyberUSA 2019 conference in College Park, MD, where John McCumber, director of cybersecurity advocacy, North America, for (ISC)² delivered a presentation outlining the findings of the (ISC)² 2018 Cybersecurity Workforce Study, which found that the industry is lacking 2.93 million qualified professionals globally. North America alone accounts for nearly one half million of this shortage.

As part of its partnership with CyberUSA, (ISC)² will help to jointly promote the importance of having trained and certified cybersecurity professionals on

staff within state and local government agencies and in the private sector and will advocate for the information security profession and the professional standing of its members. (ISC)² will also support a clearer career development process that can lead cybersecurity professionals through a career path.

"One of the biggest challenges the Department of Homeland Security has faced in the past is tackling the logistics of arming state and local governments with a consistent and repeatable platform for the delivery of cybersecurity training and information sharing," said McCumber. "This is where CyberUSA is making such a profound impact, and we are honored to partner with this community and further the goals of the DHS in certifying qualified cybersecurity professionals and providing training on a wide variety of critical topics, including securing our election processes."

"Training and certification in the cybersecurity industry is a tall task as technologies, adversaries and threats continually evolve, but what we're trying to do is to systematically enable state and local governments and private sector companies to prepare and defend themselves against attacks by building their workforces with the right set of relevant cyber skills," said Phillip Bond, executive director of CyberUSA.

"The strong reputation, experience and capabilities of (ISC)² made this a great fit to help us advance our initiatives and we look forward to a strong partnership," said David Powell, vice chairman and co-founder of CyberUSA, and CEO of FBC, Inc.

CyberUSA's Phillip Bond will provide a keynote address at the (ISC)² Secure Summit DC 2019 on April 24 at the Washington Hilton Hotel.

---

***About (ISC)²***

*Celebrating its 30th anniversary this year, (ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our membership, more than 140,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™. For more information on (ISC)², visit www.isc2.org, follow us on Twitter or connect with us on Facebook and LinkedIn.*