SightGain

BEST PRACTICES FOR YOUR SOC FROM THE US MILITARY

sightgain.com

The United States Military has two main goals: to protect the nation and to win wars. Their success relies on a well-armed force, precise planning, watertight processes, and consistent training to develop, maintain, and deploy combat-effective units. The military terms this methodical approach "readiness."

Your organization is in the middle of a war too — a cyber war — and your security operations center (SOC) is your frontline force. To succeed in its mission of defending an organization, the SOC needs to be confident that its people, processes, and technology will perform under fire, just like a top military unit.

Readiness for missions is a proven strategy with the US Military, and it can effectively address the challenges of running a SOC, too.

Mission and Readiness in the SOC

The military has one of the toughest goals on earth: keeping the United States of America safe. Every mission ties into that goal, and every task ties into a mission. In order to assess their ability to accomplish missions, the US Military relies on the concept of readiness.

Readiness encompasses three essential elements:

Building initial readiness
Establishing a baseline of initial training, testing, and resources to build basic capabilities

Increasing readiness
Exercising and training to improve performance of individuals, teams, units, and various combinations of other military capabilities

Sustaining readiness
Continue providing updated training and resources to units, before and after deployments, in order to keep them ready to accomplish their assigned missions.

The key here is that readiness is an ongoing process. Military units constantly evaluate the threat landscape, collect performance metrics around how suitable their equipment, personnel, and training are to address the threat landscape, and adapt as the threat landscape changes.

This outlook and these challenges mirror what the SOC faces on a daily basis. Similar to a military unit, a SOC is a team responsible for missions that include:

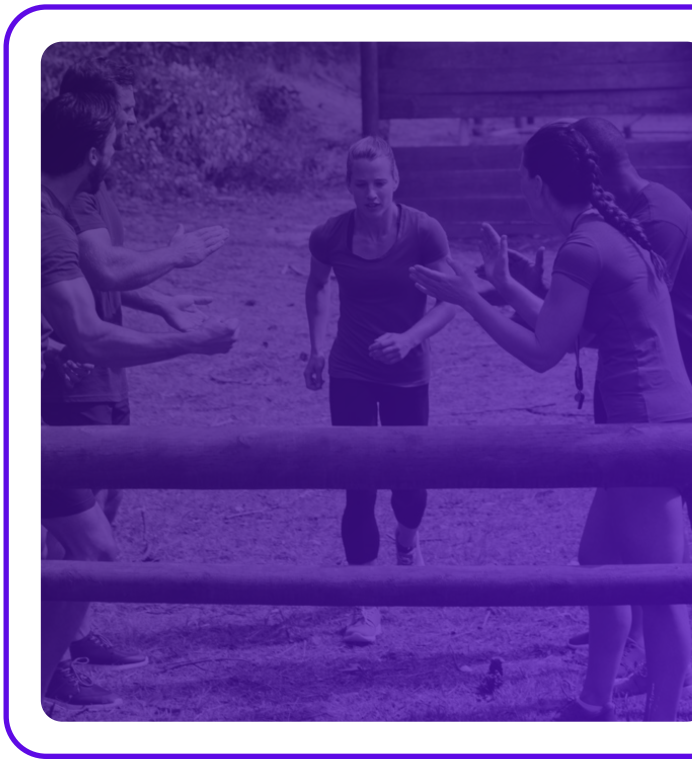
- **Protecting intellectual property and trade secrets**
- **Protecting personally identifiable information of clients and employees**
- **Maintaining business continuity and operational uptime**

Like the US Military's challenges, a SOC does not operate in a static environment. It cannot just set up one defense and then declare victory. The business's goals change over time. Assets and data crown jewels grow and change. The goals and motivations of threat groups change. Attacker techniques change. By adopting the concept of continuous readiness, the entire SOC can be constantly training and improving to be ready for these evolutions.

Build Readiness with Best Practice

Best practices are an important foundation for building readiness in the military. Through process documentation and training around those documented processes, the military can define missions, identify the best units to perform tasks to support those missions, and bring a standardized and understandable approach to missions that involve hundreds, if not thousands, of personnel.

This approach can help build readiness in the SOC as well. No matter the size of a SOC team, it is a complex entity tasked with a complex set of missions. Using well-documented and battle-tested best practices as the backbone of the SOC helps build readiness. Without a strong foundation and clear guidelines, personnel will be disjointed in their ability to identify, defend against, and resist threats.



The Importance of War Games

Readiness is so effective because it allows teams to train and know they are prepared for their mission in advance — for both known and potential threats. A chilling example comes from the story of an elite team of Navy SEALs who were called upon to complete a high stakes operation. To complete the special op, they were required to make use of stealth helicopters that had not been combat-tested before, posing a significant risk to the team.

Prior to the operation, the SEALs prepared for the worst by simulating downed-helicopter scenarios over and over again. After each simulation, they conducted a debrief, talking through what went well and what didn’t. When the helicopter went down during the actual mission, the SEALs were immediately able to go into action and complete their objective because of all the preparation beforehand. Readiness saved the day.

Like the Navy SEALs, SOC analysts need to be an elite, trained team who are prepared to be on the frontlines of the war in cyberspace. Where and how analysts experience training is critically important.

Continuous Training in the SOC

Traditional cyber range training may teach concepts, but it leaves the SOC guessing about how well personnel will perform under fire, with the equipment they will have at hand when attackers strike.

On the other hand, Automated Red Team capabilities (also known as Breach & Attack Solutions) test actual exploits against production infrastructure. This live-fire testing allows security leaders to see how well their technologies, people, and processes are set to block, detect, and respond to current threats, as well as collect actionable metrics around how people actually respond to threats.

Data collected from live-fire testing in a continuous readiness platform can then give the SOC the right metrics for the following:

- **Ability to properly prioritize threat intelligence**
- **Visibility into how well technologies, processes, and personnel are working to defend against current prioritized threats**
- **A clear picture of the SOC's current readiness**
- **Tailored analyst training based on what they could be doing better**
- **Insight to help decision makers confidently design a roadmap toward future readiness**

This is what the SOC needs to know in order to adopt a readiness-based approach to security, and be able to prepare its people, processes, and technologies to mount an effective defense in cyber war.

Be Ready for the Challenge

A SOC is a sophisticated unit that is tasked with the security of an entire business. It is the SOC's responsibility to be able to detect, respond to, and resist the threats the organization is facing. Shifting to an approach grounded in the military concept of readiness allows the SOC to focus better on the mission of defeating real threats and keeping the business secure. It is a battle-tested approach that is well suited to a complicated organization tasked with defending against sophisticated, ever-changing attackers.

Why SightGain Is the Right Choice for Bringing Military Readiness to the SOC

SightGain's founder, Christian Sorensen, has over 20 years of cybersecurity experience, including deep experience in military cyber operations. An Air Force veteran, Sorensen has worked with all branches of the military during time in joint service in intelligence, the Pentagon, and USCYBERCOM. During his time at USCYBERCOM, he helped develop the foundations of the Cyber Mission Forces that the joint services now use.

That knowledge of and experience with the military pervades the company. 30% of our employees are veterans, who bring real military experience and make sure that SightGain can deliver the outlook of bringing military readiness to the SOC every day.

SightGain has not only applied military readiness to the SOC, but has worked throughout the DoD to reveal operational insights, tune their security technologies, speed up threat identification, and improve detection rates.

Visit sightgain.com to learn about our approach to cybersecurity readiness.