Subscribe for Company and Industry Updates

Constant Technologies, Inc.

# Why a SOC Is Necessary for Effective Cyber Defense

p: 401.294.7171
f : 401.294.7505
info@constanttech.com

125 Steamboat Avenue
North Kingstown, RI, 02852
www.constanttech.com

# Introduction: The Modern Landscape of Cyber Threats

It's no secret that there has been a significant shift to digital in the last several decades. Data is the new currency. Organizations have come to rely not just on data analytics but also on the accumulation of large amounts of data.

This shift to digitalization and new focus on data has simplified many aspects of business or critical operations, while complicating others. Though going digital has increased the overall agility of operations for businesses and other organizations, it has also put their data at risk in new and challenging ways. In particular, data housed in cloud storage, while in many ways a significant step forward, has made these environments more complex to defend.

As business grows more data-driven, so does the global economy – making data a lucrative target for cyber criminals. There are multiple types of cyber-attacks, from advanced persistent threats (APTs) and phishing to malware, cryptojacking, and ransomware. As the attacks become more sophisticated, so do the tools needed to effectively defend against them. Gone are the days where tools like anti-virus, firewalls, and access control would be enough. The new scope of the cyber landscape means that old solutions alone simply won't cut it.

The Trustwave Global Security Report for 2019 found that 57% of the total compromises that they investigated were in corporate and internal networks, up from 50% in 2017. This year's report also added cloud systems such as Software-as-a-service to their compromise investigations. While they currently only make up 7% of recorded compromises, it is expected that compromises of the cloud will continue to increase in coming years.

A recent report by Kaspersky Lab researchers found that the cost of enterprise data breaches has increased from $1.23M to $1.41M from 2017 to 2018. Year over year, data breaches continue to become increasingly expensive, making preventing and efficiently handling such breaches all the more vital.

# An Effective Solution: Cyber SOCs

Best practices for handling the challenging cybersecurity landscape dictate that the entire lifecycle of a cyber security incident, from the initial detection of a breach through the return to normal operations, should be handled in one place. That place is the cybersecurity operations center (CSOC).

While using a managed security services provider (MSSP) and outsourcing your SOC is a tempting option, the data says that implementing your own in-house SOC is the best way to handle today's advanced cyber security threats. The Kaspersky report found that organizations with an internal SOC experienced less than half the estimated financial impact from a cyberattack when compared to organizations without an in-house SOC. Interestingly, the report also found that outsourcing SOCs to MSSPs did not significantly reduce financial impact of data breaches. In fact, in some cases it may actually increase the impact.

## What a SOC Can Do for You

In the world of cybersecurity, threats need to be assessed in real-time. An effective SOC must be able to provide proactive, advanced threat detection as well as immediate incident response and swift containment and remediation. Having a SOC in your organization vastly improves your response time. It can help detect threats early, which can in turn prevent major damage.

As with many security applications, in cybersecurity time is the most critical element. The less time there is between a breach and its detection, the less of an impact the cyberattack will have on an organization. Early detection limits damage, and the best tool for early detection is the cyber SOC. Highly effective SOCs combine comprehensive threat intelligence with advanced automation tools and analytics.

When it comes to cyber-attacks, the question is "when" your organization will face a threat rather than "if." Having a SOC that conducts 24x7 threat hunting, real-time incident response and breach containment ensures that your organization can resume normal operations as quickly as possible following a cyber incident.

## Necessities for a Successful SOC

One of the core functions of a successful cyber SOC is its people. The talent you hire for your operations will be responsible for the day in, day out management of the threat landscape. Highly skilled analysts and engineers can combine the data from various sources and use this information to get to the bottom of a critical security incident when it occurs.

In addition to a top-notch team, you need an effective space to work in that will help, rather than hinder, their security monitoring. This means that not only is the security technology you use important, so is the design of the space itself.

Using the right video wall to display vital, real-time data is paramount to ensuring that the time between breach and detection is minimal. From display resolution to sizing and placement, the selection of your operations center video wall plays a key role in ensuring proper display of your data. It's also important to select video wall technology that can withstand the demands of a cybersecurity operations center; not all displays are made equal, and those in a CSOC must remain on 24/7 for constant monitoring. That means they need to be resilient, and the design of the audiovisual integration should include redundancies in case of any system failure.

The furniture in your CSOC can also be specifically designed to assist the function of your operations. A popular solution is arranging workstations in open pod configurations to streamline collaboration and communication. Another way to promote operators working together within a command center is the inclusion of set collaboration areas. These include huddle spaces or adjacent conference rooms where operators have a designated area to collaborate that is set aside but still within the cybersecurity space.

In a cyber operations center, having proper accommodation for all equipment is vital. Console furniture for command centers must have design that encompasses specific technological needs, whether it's the ability to

mount multiple monitors at each station or the space to house several CPUs within an enclosed module. Well-designed operations center consoles feature both utility and cleaner aesthetics due to equipment storage options.

## Constant Technologies: CSOC Design Experts

Functional design for cyber operations is a balancing act. It takes true expertise to ensure all components not only work together, but are also optimized for 24/7 use. Constant Technologies can provide all of that and more. We design control center furniture to meet your needs and exact specifications and provide expert audiovisual integration for large format video walls. Our decades of experience in the industry mean that no one does it better. Due to our comprehensive knowledge of the complex needs in mission critical spaces, we deliver solutions that make operations simple for the end-users. Contact us today at info@constanttech.com to begin a design consultation.

## About Constant

Constant Technologies, Inc. is a premier mission critical systems integrator providing customized audiovisual integration of large scale operations center video walls and control center console furniture worldwide. With over three decades of experience, Constant's team has the knowledge and clearance to work with sensitive environments in both the public and private sectors and has implemented turnkey solutions all over the world. Constant designs, installs and services projects of all scopes and sizes to create solutions with the highest levels of security, aesthetics and functionality in mind. Some of Constant's installations include: EOC builds, Network Operations Center design, Fusion Centers, Security Operations Centers, Control Room Design, Social Media Command Centers, and other command and control environments.

Keep up with the latest white papers and thought leadership from Constant Technologies:

Subscribe for Company and Industry Updates

Tell Me More

p: 401.294.7171
f: 401.294.7505
info@constanttech.com

125 Steamboat Avenue
North Kingstown, RI, 02852
**www.constanttech.com**