What you need to know about...

WatchTower
Co-Managed SOC

24/7/365 Cybersecurity

SECURITY PURSUIT

At Security Pursuit, We Solemnly Swear

To sweat the small stuff, so you don’t sweat alone. To always be focused on your perspective, so we get things done just the way you want. We swear to always be absolutely and unconditionally crazy about the things you are crazy about. We swear to bring calm to every situation, even when you are having a really bad day. Finally, we swear to be available to you day and night.

Does this Sound Like You?

"*I am the cybersecurity leader at my company. I have a small team and excellent tools. But, we just can't keep up. We get constant alerts from tools that don't talk to each other, putting us in never-ending response mode. Our threat landscape is growing faster than we can handle, and we are being held to more compliance requirements."*

4 Key Benefits of a Security Operations Center (SOC)

1. Threat Detection and Response:

A SOC can detect security threats in real-time and respond quickly to mitigate any potential damage. This is critical to reducing the risk of a data breach or attack.

2. Proactive Security Measures:

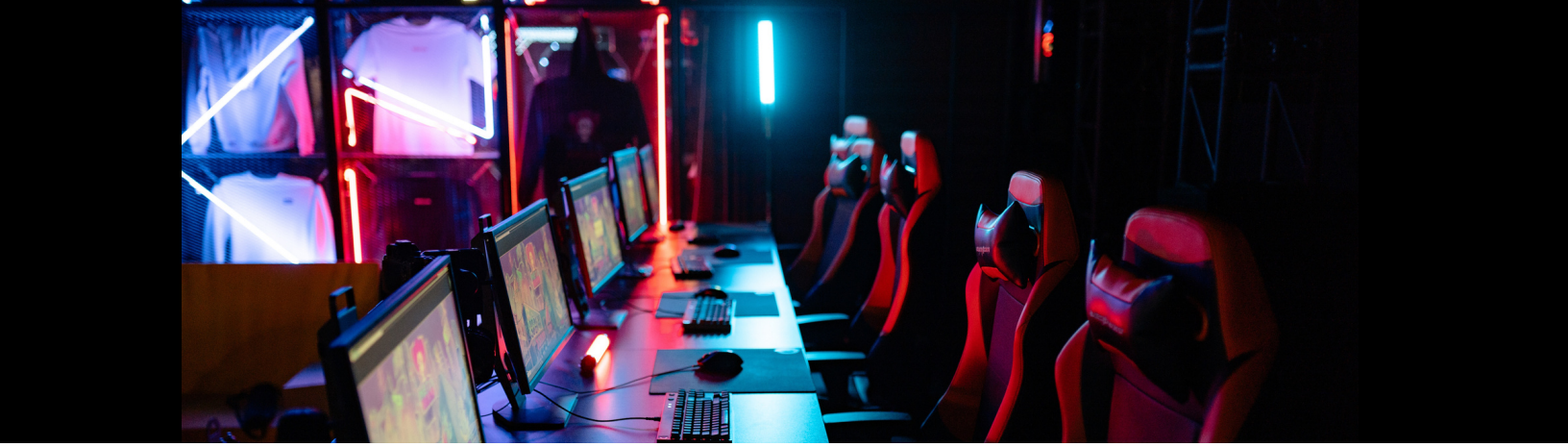
A SOC can help identify vulnerabilities before they are exploited by attackers, enabling the security team to implement proactive security measures to prevent future attacks.

3. Compliance:

A SOC can help ensure that the organization complies with relevant regulatory and legal requirements. This includes monitoring for unauthorized access to sensitive data, which can help meet compliance and best practice requirements.

4. Cost Savings:

By implementing a SOC, the organization can reduce the cost of cybersecurity incidents by minimizing the potential for data loss, system downtime, and reputation damage.



What is a SOC?

A Security Operations Center (SOC) provides a centralized location where trained security professionals monitor and respond to various security alerts. A SOC team uses a variety of security tools and data feeds to identify and monitor potential threats before they become attacks. They also investigate active security incidents and deploy effective response plans. Finally, a SOC determines what really happened after an event, allowing the organization to get better and more secure.

What is a SIEM?

A Security Information and Event Management (SIEM) collects data logs from a range of sources, identifies activity that deviates from the norm with real-time analysis, and either automatically takes appropriate action or alerts the SOC to respond.

It is the key tool for a SOC. A SOC team really can't simply look at tools and logs manually. There is too much information in too many formats. Tools alone operate in silos, leaving you to make sense of what each means in a larger context. For example, there may be an anomaly on a server, three spam alerts, and a switch that just went down. Without a SIEM, the SOC team must manually sort out what this means. But a SIEM can correlate those events to determine if they are indicators of a compromise and alert the SOC to quickly respond.

A SIEM also lets you look back, allowing you to know what really happened. Did hackers get my data? Are they still on my systems? How did they get in? A SIEM provides limitless log and data retention so you can piece together what happened and make changes that improve your security.

Approaches to Building a SOC

In-house

Perfect for large organizations that can justify the expense of staff and tools

An in-house SOC is one that is built and managed entirely by the organization's internal team. This approach involves investing in a SIEM and the supporting infrastructure, training your security team on running the SIEM, giving them time to tune the system, and monitor and respond to events.

Outsource

Perfect for small organizations that have no security staff

An outsourced SOC is one that is managed by a third-party service provider. This approach involves contracting with a managed security services provider (MSSP) that offers SOC services. The MSSP provides security analysts, infrastructure, and technology required for security monitoring and incident response.

Hybrid

Perfect for organizations that have invested in in-house SOC, but can't staff for off hours.

A hybrid SOC is a combination of in-house and outsourced SOC. This approach involves having an in-house team that manages security operations during normal business hours, while the outsourced SOC takes over during non-business hours, weekends, or holidays.

Co-Managed

Perfect for organizations that have security staff, but not enough time or money to build and run it. Also, great when flexibility is needed.

Co-managed SOC: A co-managed SOC involves collaborating with an MSSP to manage pre-defined aspects of the SOC. The in-house team and the MSSP work together as a team.

What is Security Pursuit's WatchTower?

Security Pursuit's WatchTower service is a Co-Managed SOC. We use our tools to build your SOC, tune it with you, then operate it together. Our expertise provides you 24/7/365 coverage, but lets you still take as active of a role as you want.

Key benefits include:

- **Built by Experts.** Our SOC is built and operated by the individuals who built and operated the Department of Homeland Security's SOC. Our team consists of 20-year veteran security professionals.

- **Any Logs, Any Tools.** We use Splunk as our SIEM, considered one of the best SIEM's available. We use it because we can integrate with any tools you have, allowing us to build your SOC leveraging what you already have.

- **Flexible Co-Management.** Do you want to learn more about SOC operations? Great! Want nothing to do with monitoring? Fine! Security Pursuit will let you take as active or inactive a role as you want. Change your mind anytime. Want to take over your SOC and bring it in-house? That's fine, too.

- **24/7/365.** Our team and tools let us keep an eye on your systems all the time. You sleep...we watch. We are also very careful about who we accept as WatchTower clients and how many clients we have. For us, balance is the key to keeping clients safe.

- **Close Partnership.** We build a close relationship with you and your team. We meet monthly to review activity, tune, and discuss pulling in more feeds. We provide you with executive reports and recommendations for improvement every month.

What is the Process?

1. Implementation

Implementation is handled by one of our professionals that will guide you through the collection of basic security data. We generally start with perimeter systems, but we will decide together what will be best.

2. Expansion

We will work off our initial Roll Out Plan to continue to route new systems to a universal forwarder. Security Pursuit will continue to tune and monitor them. As mentioned, the Roll Out Plan is meant to guide us, and it can be changed according to the Client's immediate needs.

3. Continuous Monitoring and Reporting

Security Pursuit will continue to monitor, review, and tune the system. We will provide you with a monthly report showing key metrics and findings. Each finding will be accompanied with further recommendations for improvement.

4. Threat Hunting

Security Pursuit will proactively search for and identify potential security threats or breaches in the system before they can cause harm. We use the Splunk environment to analyze large amounts of data from your sources to detect patterns, anomalies, and other indicators of compromise. We also use other tools and manual analysis as needed.

5. Incident Management

Our team will address incidents from our SOC to the extent possible. Security Pursuit will escalate indicators of threat and compromise to your team if we cannot explain them or address them. You will need to have a designated person(s) who can respond quickly. Active Incident Response Services are provided on an as-needed, if-needed basis at a discounted rate.

What does this Cost?

"It Depends"

But most clients spend between $30,000 and $80,000 per year

Next Steps

Security Pursuit has been a leading cybersecurity service provider for over 12 years.

Security Pursuit is unique in the cybersecurity world. We answer emails. We answer the phone! When you need us...we are there. We also don't bother our clients with endless sales calls.

If you want the best cybersecurity service partner, you need not look any further.

Contact us today to scope out your WatchTower

SECURITY PURSUIT

720-675-ROOT (7668)
www.securitypursuit.com