Blog Post

Do We Need Our Own SOC?

Published
Mar 24, 2021

Written by
John Headley

Filed under
Cybersecurity

Credit: This blog post is a reimagination of the chapter with a similar name in MITRE's Ten Strategies of a World-Class Cybersecurity Operations Center. Their document is an invaluable resource and highly recommended reading, but as it was published in 2014, both the cyber threats that organizations are up against, as well as the defense tools available, have evolved. This article reimagines their advice to be more applicable in today's cybersecurity landscape.

What is a SOC?

Before an organization can answer the question of "Do we need our own SOC?", it first needs to understand what a SOC is.

A SOC, or **Security Operations Center**, is a group of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents. Sometimes going by other names, such as Computer Security Incident Response Team (CSIRT), this group is the organization's focal point for security operations and computer network defense (CND).

SOCs vary in maturity levels and therefore the capabilities they can bring to an organization.

However, these are some of the core capabilities that are normally provided by any SOC:

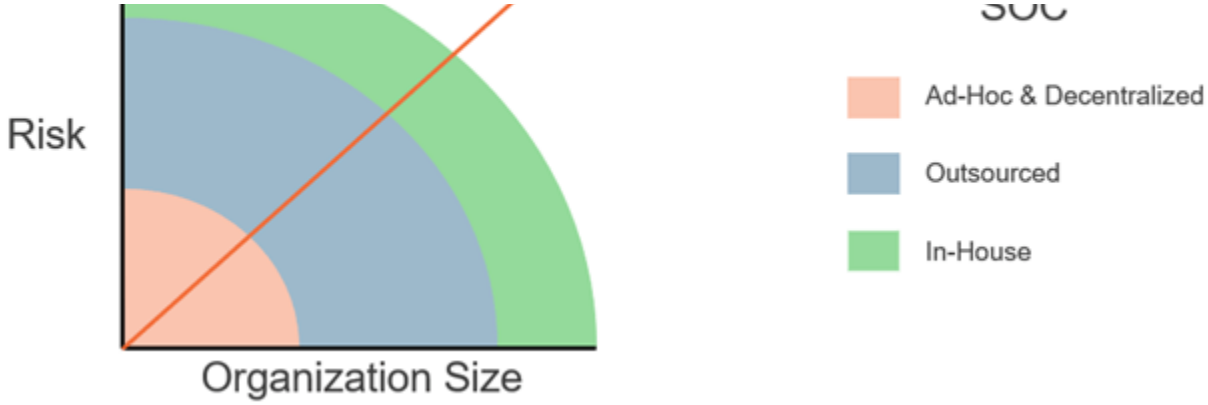
- Real-time monitoring, detection, and analysis of potential cyber incidents
- Incident response, including containment, eradication, and recovery
- Prevention of incidents through proactive activities, such as vulnerability scanning and remediation

With that said, many organizations may feel they are already doing these activities without a SOC.

It is common for businesses with an immature cybersecurity program to perform the above using an ad-hoc, decentralized SOC composed of members of its IT staff. If this is how your organization operates, it is imperative to ask the question: do we need our own SOC?

Do we need our own SOC?

Not every organization needs its own SOC. With MSSPs offering affordable 24×7 SOC-as-a-service options, outsourcing can be a great option instead of building an in-house SOC or forgoing a SOC altogether. The chart below shows the typical type of SOCs that we see among organizations based on their size and the amount of inherent risk factors to their business model.



To aid in determining where you stand on this chart, and to ultimately answer the question at hand, MITRE developed a worksheet that you can use to quantitatively guide the decision process. VPLS's modified version of their worksheet assigns your organization a score. The more points you accumulate, the more it's recommended to have either an outsourced or in-house SOC.

DO WE NEED A SOC? WORKSHEET

Fill out the worksheet below to see your score.

You immediately get 1 free point because you will have an incident at some point in time.

1

1. Has your organization detected an incident that had a measurable impact on the mission or came at a significant cost within the last six months?*

- [ ] Yes
- [ ] No

2. Is there a perception that your organization faces a targeted internal or external cyber threat? Targeted meaning a threat beyond the normal Internet-based opportunists, such as bots and script kiddies.*

- [ ] Yes
- [ ] No

3. Does your organization conduct high-risk or high-value business and is that business heavily dependent on IT, such as finance, healthcare, or energy production?*

- [ ] Yes
- [ ] No

4. Does your organization offer IT services to directly connected third parties in a business-to-business (B2B), business-to-government (B2G), or government-to-government (G2G) fashion?*

- [ ] Yes
- [ ] No

5. Does your organization serve sensitive or privacy-related data to untrusted third parties through some sort of public-facing portal such as a Web application?*

- [ ] Yes
- [ ] No

6. Does your organization retain sensitive data provided or owned by a third party, such that the organization faces significant liability if that data is stolen or lost?*

- [ ] Yes
- [ ] No

7. How many hosts (users/IPs) are in use in your organization?

- [ ] Less than 1,000
- [ ] Greater than 1,000

Evaluating your score

Below is a quick summary of how to evaluate your total score. Note that the score ranges and recommendations below are just guidelines, not hard and fast rules.

1 - 3 total points

VPLS Recommends

The organization can probably make do with an ad-hoc, decentralized approach to a SOC using members of the in-house IT staff, but an outsourced SOC is still recommended.

4 - 14 total points

VPLS Recommends

The organization probably doesn't warrant its own SOC, but a SOC is necessary,

so an outsourced SOC is recommended.

15+ total points

VPLS Recommends

An outsourced SOC may still work, but the organization should strongly consider its own SOC, especially if points are much higher than 15.

We notice organizations who fall between 1 and 3 points will typically try to perform SOC services using existing members of the IT staff due to budget constraints.

One word of caution here is that in this SOC model, there is significant risk that the incidents will go unnoticed by your team, especially when you consider incidents that happen after business hours. Even if they are noticed, there is still risk that those incidents won't be dealt with in the most efficient, effective, or comprehensive manner.

Action items

There is no one-size-fits-all answer to "Do we need our own SOC?". However, now that you have some tools to guide the decision process for your own unique organization, we ask that you:

- Assess your organization quantitatively using the worksheet
- Assess your organization qualitatively
- Compare the results – does your score match your perception?

VPLS provides a wide variety of cybersecurity services, including **24×7 SOC-as-a-service** and **professional services**. If you would like to discuss all things SOC with VPLS, including our recommendation based on your SOC worksheet score results, then please contact us. Our staff of certified security experts are always ready and available to help.

Read More from this Author

John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

More from this Author

PREVIOUS
VPLS Acquires New York Data Center and Strengt...

NEXT
VPLS Expands Bare Metal and Cloud Platform into...

If you enjoyed this article, you'll probably like:

5 Reasons SOC-as-a-Service Features Help You

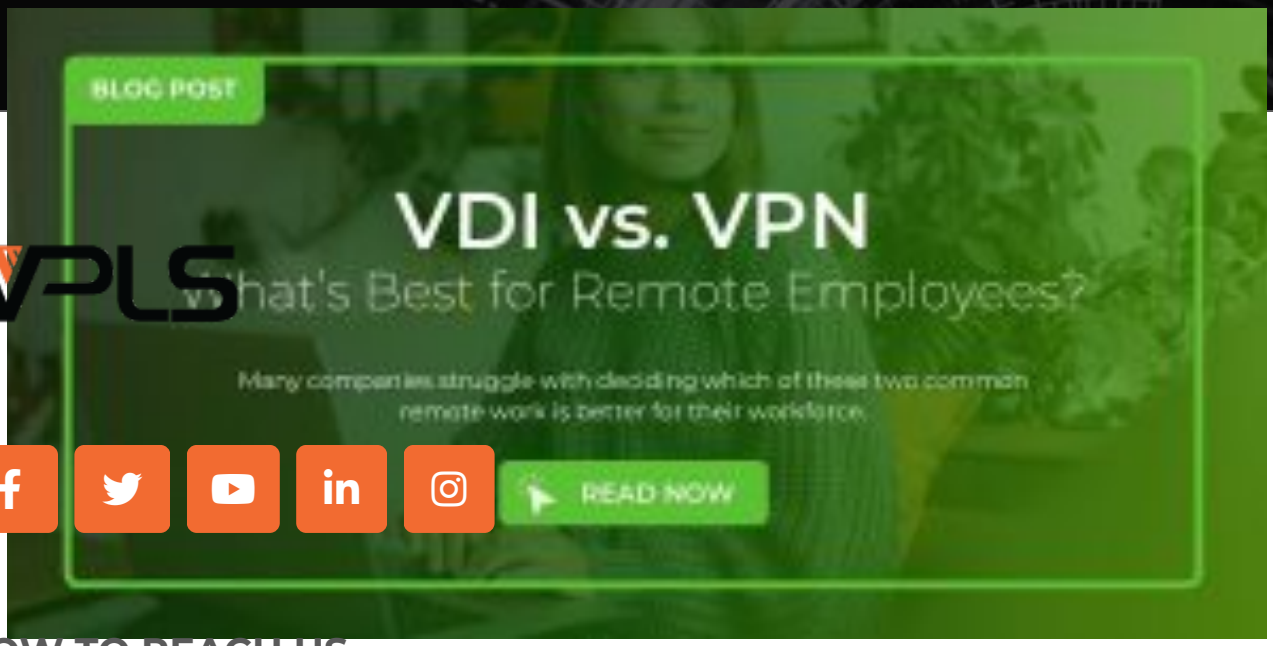
March 29, 2022

Read More »

What Is SOC-as-a-Service?

March 28, 2022

Read More »



VDI vs. VPN: What's Best for Remote Employees?

March 28, 2022

Read More »

HOW TO REACH US

Corporate Headquarters

600 West 7th Street, Suite 510
Los Angeles, CA 90017

24/7/365 Customer Service

+1 (888) 365-2656

support@vpls.com

Sales Inquiries
+1 (888) 365-2656
sales@vpls.com

WHAT WE DO

Cloud
Hosting
Colocation
Network Services
Managed Services
Professional Services
VAR

WHO WE SERVE

Financial Services
Healthcare and Life Sciences
Media & Entertainment
Telecom
Startup
Enterprise
Public Sector