SKOUT
CYBERSECURITY

# Managed Security for MSPs

The Challenges MSPs Face
When Providing Managed Security Services

# Cybersecurity for MSPs

How Managed Service Providers can provide viable cybersecurity monitoring solutions.

The startup costs and level of expertise required to build, run, and offer a Security Operations Center (SOC) and Managed Security Services (MSS) is tremendous. A common misconception is that MSPs can easily progress their Network Operations Center (NOC) into a SOC by rebranding and offering a few additional services. This is not true for many reasons, including the difficulty of obtaining accreditations such as SOC II Type II and hiring qualified cybersecurity staff to run the SOC.

## The Difference Between a SOC and a NOC

The roles of the SOC and the NOC are fundamentally different. Both are responsible for identifying, investigating, prioritizing, escalating, and resolving issues, but the problems they are tasked with solving are not the same and require different skills and backgrounds.

The NOC handles incidents and alerts that affect performance and availability. Its job is to meet Service Level Agreements (SLAs) and manage incidents in a way that reduces downtime – a focus on availability and performance.

The SOC focuses on incidents and alerts that affect the security of information assets. Its job is to protect intellectual property and sensitive customer data – a focus on security.

While both the SOC and NOC are critically important to any organization, combining them into one entity and having each one handle the other's duties can spell disaster. Their approaches are very different and their management skill sets are highly specialized.

A NOC analyst must know network, application and systems engineering, while a SOC analyst must have security engineering skills.

> "At SKOUT, we recognize that there is a surging demand among MSPs for effective and affordable cybersecurity solutions. Our channel-focused delivery of service is designed to make cybersecurity accessible to the SMBs that need it the most."
>
> -Aidan Kehoe,
> CEO and Founder
> SKOUT CYBERSECURITY

Each group tackles adversaries of a different nature. The SOC focuses on "intelligent adversaries" while the NOC deals with naturally occurring system events.

## Challenges

### STAFFING

The lack of cyber experts is one of the most significant issues in building and maintaining a SOC. According to PWC, the cybersecurity workforce gap will widen to 1.5 million job openings by 2019. The challenge is and has been recruiting and retaining cyber professionals. The challenge is even harder when trying to recruit or retain highly skilled workers, such as Tier 2, 3, or 4 experts. MSPs who want to get into the security game will be competing for this talent along with other security companies and government organizations.

### ALERT EFFICIENCY

Inefficient alerts are one of the major areas where SOCs fail. A common example of this would be receiving too many of the wrong types of alerts, thus missing the relevant ones. This happens for many reasons. The most common ones are:

1. Not understanding what the alert means. An untrained analyst may think a group of alerts is meaningless while a seasoned analyst knows the group of alerts could collectively represent a major cyber-attack.

2. Not properly training and tuning the security devices to the behavior of the client's network. Organizational networks behave differently just like businesses run differently. No two organizational networks are alike. Organizations are configured differently, use different applications, perform different functions, and allow/ disallow users access to different areas and applications on the network.

3. Not employing tools to quickly identify, investigate, and communicate true positives. Many MSPs turned Managed Security Service Provider (MSSP) soon realize that there are many background orchestration, automation, and workflow processes that are required in order to send immediate alerts.

4. Not utilizing threat intelligence correctly or at all. Threat intelligence is the key to identifying malicious software, IP addresses, websites, signatures, intelligence, etc. but if not used correctly or misinterpreted, it is ineffective. Many MSPs do not have the talent to ensure threat intelligence is correctly correlating the data and sending alerts about True Positives.

### PROCESSES AND PROCEDURES

Developing, implementing, and maintaining processes and procedures are critical to running a successful SOC. The ability to create a replica of routine processes is a major efficiency issue for many SOC teams. The hundreds of processes can be daunting. Although MSPs are often heavily focused on processes and procedures, there can be many challenges. SOC processes and procedures focus on incident handling and alerts while most MSP processes and procedures focus on assets.

### TECHNOLOGY

MSPs manage traditional devices (e.g., routers, switches, and servers) while cybersecurity-specific technology requires more specialized training and expertise. If an MSP has not had extensive experience with security devices, [e.g. Network Intrusion Detection Systems (NIDS), Host Intrusion Detection System (HIDS), Security Information and Event Managers (SIEMs), etc.], they quickly discover they are out of their depth.

These advanced security technologies are more complex because hours of training and tuning are required to understand True Positives. Simply dropping security devices into a client network without an intimate understanding of how the devices work has proven disastrous for many MSPs.

After becoming an MSSP, many of them encounter the following scenarios:

1. Discover the level of support provided by vendors is not the same level of support provided by networking vendors
2. Belatedly realize the configuration and change management of security devices requires an even more precise skill set which is already in short supply in the marketplace
3. Need technology to make up for the shortcomings of operating with untrained personnel

In short, the cost to build a world-class SOC can exceed millions of dollars. Many MSPs fall victim to the misbelief that that the cost to build a SOC is small. They often begin to build out their own, only to later end up scrapping the idea. This causes a significant waste of money, time, and resources. Cybersecurity is the only technology that has an adversary, which requires a very specific skill set. It is important to address security problems and concerns properly.

## Providing MSS as an MSP

The best way for MSPs to provide Managed Security Services (MSS) is to partner with a security vendor like SKOUT. SKOUT is a cloud-native, streaming data analytics platform built to deliver effective and affordable cybersecurity products for SMBs, delivered through MSPs.

At SKOUT, we know that our best way to reach SMB customers is through MSPs. MSPs are trusted technology advisors and know their customers best. SKOUT provides MSPs with a world-class service, offering financial incentives, training, and support to enable them to provide MSS to their clients.

## About SKOUT CYBERSECURITY

The SKOUT platform uses multitenancy with a modern data analytics architecture and flexible pricing. This makes it easy for MSPs to integrate advanced security tools, threat intelligence feeds, and around-the-clock monitoring with their existing service offering. Artificial Intelligence augments human capabilities and enables SKOUT analysts and their MSP counterparts to do more than the ordinary security expert.

To address the staffing concerns that MSPs face in the context of cybersecurity, SKOUT has experts from 15 fortune 500 companies and five government organizations who have 30+ years of experience on the most complex and sophisticated cyber-attacks. SKOUT is constantly training staff on the latest threats and hiring new analysts to meet the staffing needs.

SKOUT has an SSAE-16 SOC 2 TYPE II certification. SOC 2 not only entails rigorous standards related to organizational controls surrounding client financial reporting, but also requires standard operating procedures for organizational oversight, vendor management, risk management, and regulatory oversight. A SOC 2-certified service organization is appropriate for businesses whose regulators, auditors, compliance officers, business partners, and executives require documented standards.

Additionally, SKOUT is a CJIS (Criminal Justice Information Systems) ready vendor. CJIS is an FBI- sponsored program and a CJIS accreditation allows SKOUT to provide services to federal, state, and local law enforcement agencies. Additional controls to achieve this accreditation include intense background screening and fingerprinting of all SKOUT analysts, physical security controls, as well as specific processes and procedures to protect the confidentiality of law enforcement information.
SKOUT is built with a "Write Once, Deploy Anywhere" architecture, which allows for sensors to be placed anywhere customers need them, from small offices to the cloud. SKOUT can integrate with existing tools and systems, including mainframes and custom applications. SKOUT can tailor a solution to meet the cybersecurity needs of any business and is focused on making cybersecurity accessible to all business, so companies understand what they are getting.

SKOUT offers MSP partners dedicated account management, event opportunities, sales enablement tools, and customized training. Additionally, SKOUT's partner pricing model allows MSPs to control how much money they make. There are no limits on the number of services you can sell and on how much money you can make.

# SKOUT

CYBERSECURITY

## ABOUT SKOUT

SKOUT is a cloud-native, streaming data analytics platform built to deliver effective and affordable cybersecurity products for SMBs, delivered by MSPs.

## GET IN TOUCH

If you would like to schedule a demo or learn more, visit getskout.com or email us at msp@getskout.com.

getskout.com