EBOOK

# SOC Efficiency Benchmark

June 2024

VECTRA®

# SOC professionals spend up to 500 hours a year investigating false positives

**Vectra AI surveyed 119 SOC professionals to find out how they spend their workday, and the results suggest that SOC professionals spend an overwhelming amount of time and talent on tasks that can be outsourced and automated.**

With an expanding hybrid attack surface, emerging attacker methods, talent shortfalls and flattening budgets, we have a rising defender dilemma. Today's SOC teams spend hundreds of hours of work managing thousands of alerts, configuring policies, investigating false positives, and tuning rules. In this infographic, Vectra AI explores how SOC professionals spend their day and the activities that are pulling them away from addressing real incidents.

**See how SOC professionals today can optimize their security program and maximize their own time and talent.** →

# Table of Contents

**TAKEAWAY #1:**

**TAKEAWAY #2:**

**TAKEAWAY #3:**

## TAKEAWAY #1:

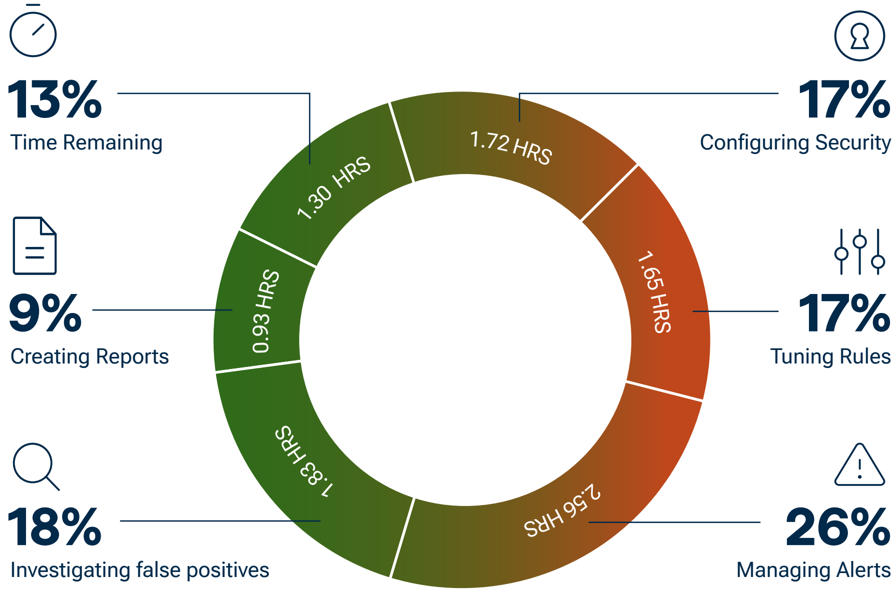
# A 10-hour workday is normal

Most corporate employees follow a standard 8-hour workday – **not SOC professionals**.

On average, professionals surveyed spend 8.7 hours a day on 1) configuring security posture, 2) tuning rules, 3) managing alerts, 4) investigating false positives, and 5) creating reports. This leaves a little over an hour for meetings, skills development, wellness, research, mentoring, and lunch and/or breaks.

The data suggests that security professionals are working 8 AM – 6 PM without taking any sort of break. However, when doing other responsibilities or taking much needed breaks, SOC professionals are realistically looking at a 7 AM – to 7 PM workday. That is a 60-hour work week, 20 hours more than the standard 40 hours.

In a
**10 hour**
**work day** with a
**5-person avg team**

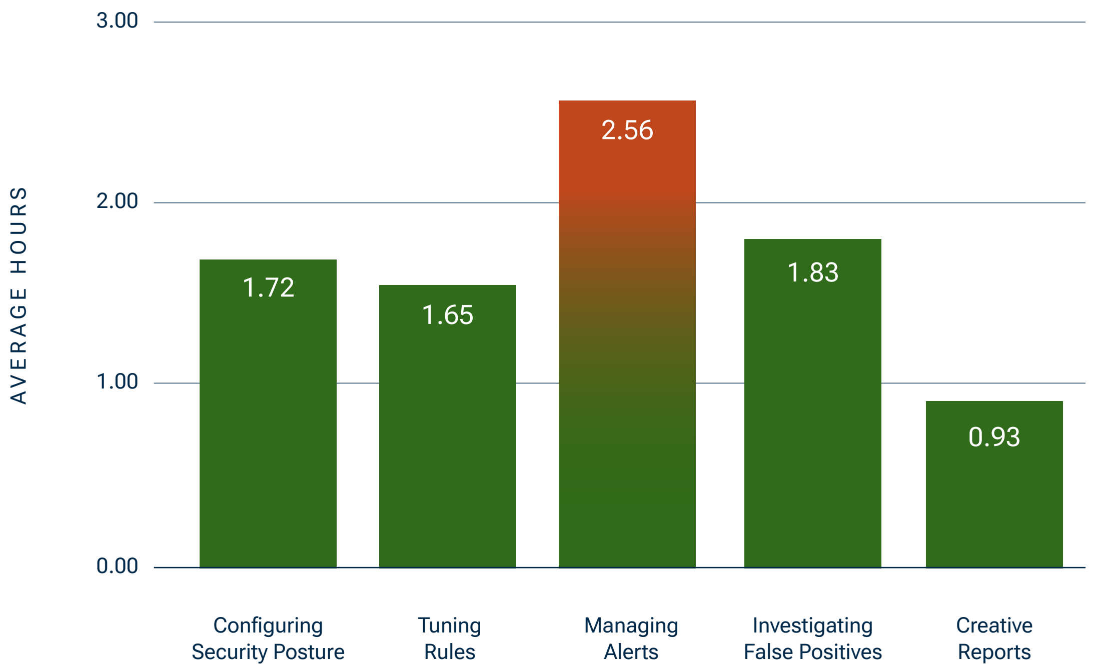


TAKEAWAY #2:

# SOC professionals spend the most time managing alerts — on average almost 3 hours a day

SOC professionals surveyed spend **over 25% of their 12-hour workday** reviewing alerts on various security tools.

This includes clicking into alerts, reassigning to other team members, or closing alerts deemed irrelevant.



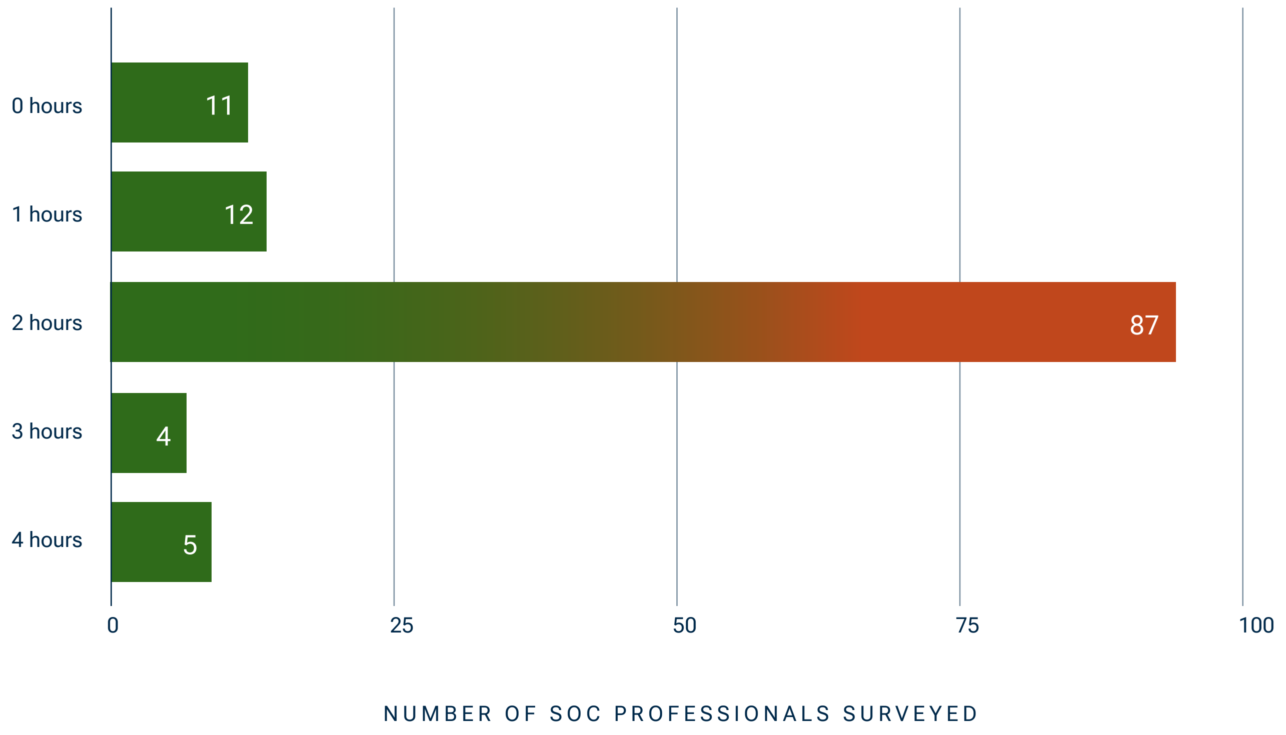
### TAKEAWAY #3

# SOC professionals spend almost 2 hours a day investigating false positives

Of the 119 SOC practitioners surveyed, 96 noted that they spend **2 hours or more investigating false positive alerts** triggered by their security tools.

That equates to nearly 500 hours (about 3 weeks) a year spent looking at threats that are not real.[1]

## Hours spent investigating false positives



[1] Based on a 249-day work year.

## Conclusion

As organizations grow bigger and their environments expand to a mixture of on-premises and cloud, the day-to-day of a SOC professional becomes more complex.

In this survey, we can see that SOC teams are spending many hours out of their day managing alerts with a large potential of those alerts being false positives. We see them tuning rules and configuring security policies daily to adapt to ever-changing attackers and data compliance policies. SOC professionals are spending the majority of their day on these tasks — so this begs the question: how can SOC professionals somehow optimize their own time and talents?

**Vectra analysts can take the burden from SOC professionals either partially or completely, based on the organization's preference.**

Vectra takes managed detection and response to the next level with remote response and remediation, so that you can truly get that 8-hour workday, take breaks, eat lunch, and save your nights and weekends.

**Learn More about Vectra**

Vectra AI gathered anonymized results from the Vectra MXDR calculator tool.

## About Vectra AI

Vectra AI is the leader in hybrid attack detection, investigation and response. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Vectra AI's patented Attack Signal Intelligence empowers security teams to rapidly detect, prioritize, investigate and stop the most advanced hybrid cyber-attacks. With 35 patents in AI-driven detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.