The Transformational CISO's Guide to **Security Orchestration, Automation and Response**

How giving security teams time to be proactive and strategic helps businesses innovate and thrive

splunk>

Table of Contents

Business leaders need transformational security teams

The role of the chief information security officer (CISO) is changing.

Like chief information officers (CIOs) and chief technology officers (CTOs) before them, CISOs are evolving from contributors with a limited portfolio of responsibility, to highly integrated and strategic drivers of business transformation. The most successful organizations are recognizing that genuine digital and business transformation depends on security modernization.[1]

PwC found that 40 percent of executives are seeking CISOs capable of leading cross-functional, agile teams that are not only keeping pace with digital transformation, but, in many cases, pointing the way forward. A survey conducted for the Information Security Systems Association revealed that security professionals worldwide ranked communication and leadership skills as the most important traits of a successful CISO.[2]

The Four Qualities Executives Value the Most:

1. Strategic thinking
2. Taking smart risks
3. Leadership skills
4. Identifying and growing innovation

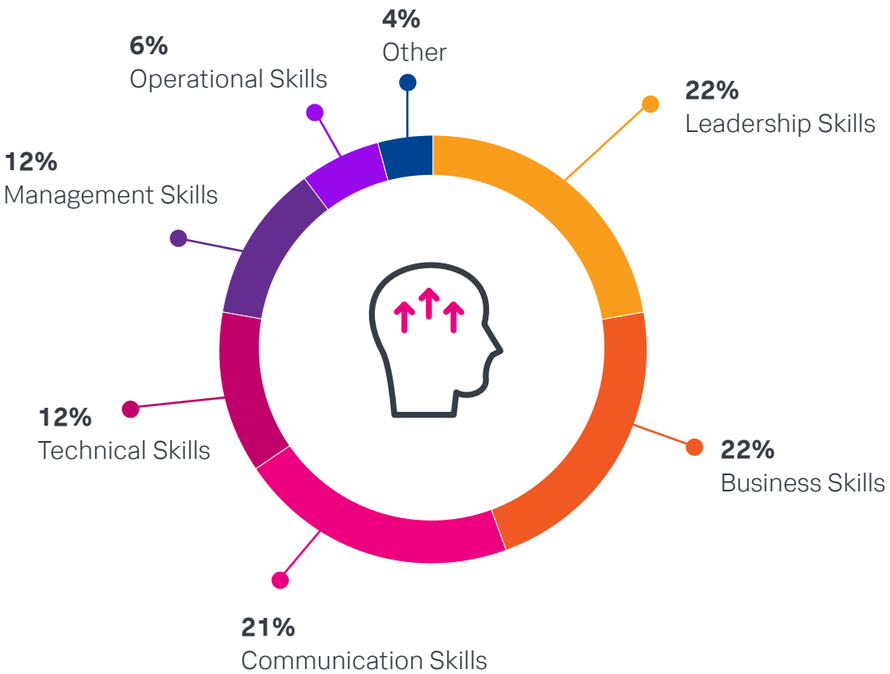
The ISSA survey also found that a majority of security analysts want to take on more strategic roles, and they recognize that they will need to develop leadership, communication, and business skills to become leaders of growth and transformation.

[1] https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-digital-trust-insights/cyber-strategy.html
[2] https://www.issa.org/wp-content/uploads/2020/07/ESG-ISSA-Research-Report-Cybersecurity-Professionals-Jul-2020.pdf

Security analysts know they need more than technical skills to become organizational leaders.

Enterprise Strategy Group asked security analysts which skills they needed to develop to become chief security officers (CSOs) or CISOs.

Source: Enterprise Strategy Group



But in too many cases, the strategic aspirations of security chiefs and analysts are thwarted by the day-to-day realities of **too many alerts and too few people to respond**.

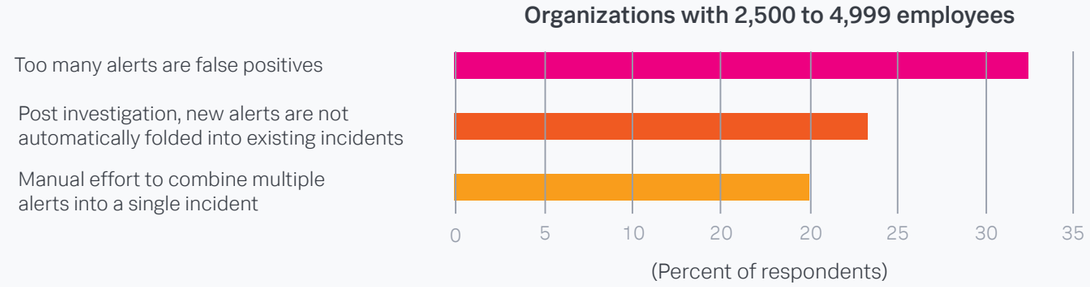
From overwhelmed to in control

Nearly a third of cybersecurity professionals told the ISSA that keeping up with an "overwhelming workload" was the most stressful part of their job. That overwhelming workload can be counted in the hundreds — even thousands — of alerts per day that demand prioritization, investigation and response.

The top three causes of uninvestigated alerts

What is preventing your organization from investigating and responding to ALL suspicious alerts every day?

Source: IDC



The challenge of unending alerts is compounded by a shortage of cybersecurity talent. There simply aren't enough qualified cybersecurity professionals to adequately staff security operations centers (SOCs) around the world. This well documented talent gap, combined with the sheer volume of alerts per day, explains why 64% of security tickets generated per day are not being worked.[3] Analysts aren't able to address every alert, leaving their companies vulnerable to attack.

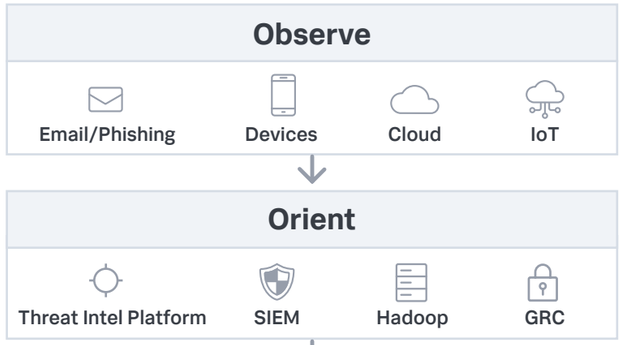
64%
of daily security alerts are unaddressed[4]

The answer to these challenges is security orchestration, automation, and response (SOAR). Splunk SOAR provides security orchestration, automation and response capabilities that allow security analysts to work smarter by automating repetitive tasks; respond to security incidents faster with automated alert triage, investigation and response; increase productivity, efficiency and accuracy; and strengthen defenses by connecting and coordinating complex workflows across their team and tools. Splunk SOAR also supports a broad range of SOC functions including event and case management, integrated threat intelligence, collaboration tools and reporting.

[3]https://www.splunk.com/en_us/form/an-enterprise-management-associates-research-report.html
[4]https://www.splunk.com/pdfs/analyst-reports/an-enterprise-management-associates-research-report.pdf

A day in the life of an analyst

Before and after SOAR



10,000 suspicious incidents per day

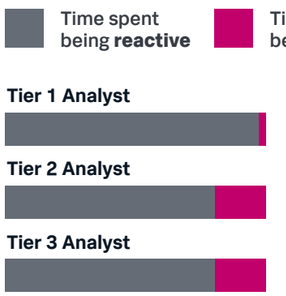
Without SOAR

Analysts have to **manually sift** through, analyze and manage all incoming logs and alerts

Analyst

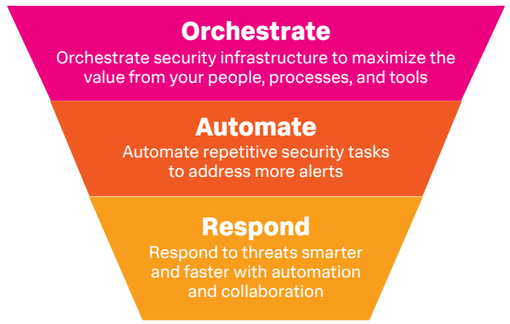
Decide and Act

Analysts of all tiers spend most of their time being **reactive,** with little time spent being strategic.



Time to respond:
30 minutes

With SOAR

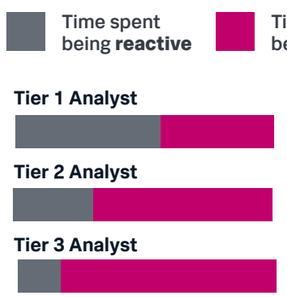


Act on every alert every day

Analyst

Decide and Act

With SOAR, the analyst workflow is simplified, so analysts can collaborate and respond to security incidents faster.



Time to respond:
30 seconds

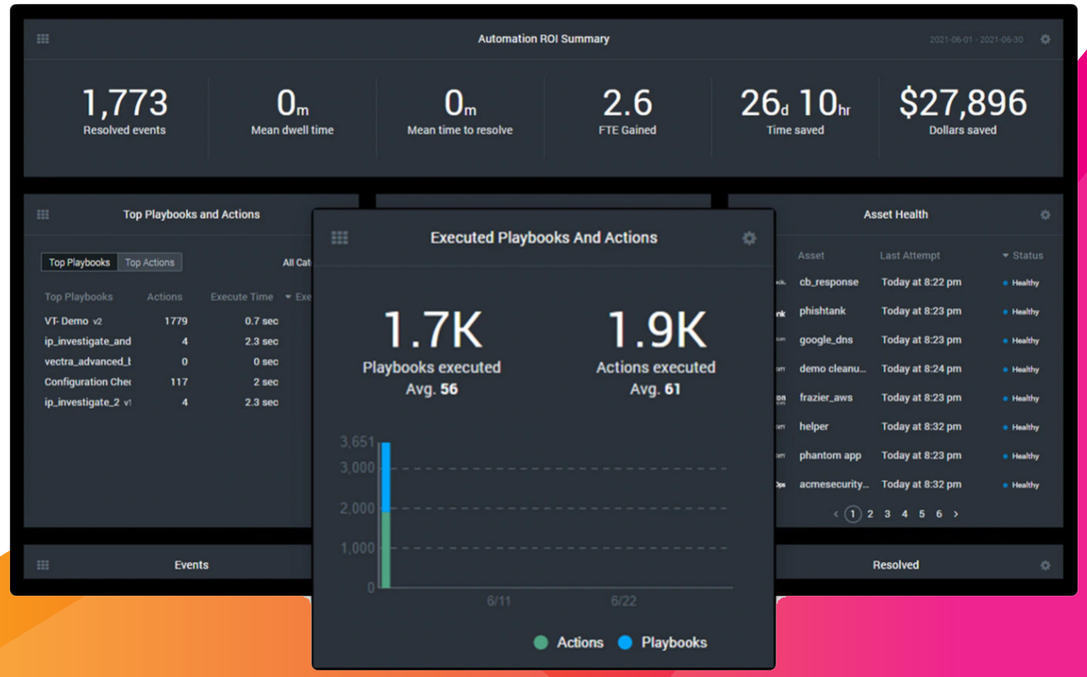
The ROI of SOAR

In a recent Ponemon report, the average annual cost of phishing was estimated to be almost $15 million. The cost of ransomware can also be expensive and cause lasting reputational damage.

Luckily, a SOAR tool can save you time and money[5] in a myriad of ways. For example, with a SOAR solution, a team of three analysts in a SOC can have the impact of a team of 10 to 15 analysts that would otherwise perform all tasks manually.

> **"There's going to be a point when you'll be overwhelmed with the amount of work that exists and won't be able to hire more people. It's humanly impossible to process the amount of data that needs to be processed, and the only path forward is automation."**
>
> – Jason Mihalow, Senior Cloud Cyber Security Architect, McGraw Hill
>
> View Case Study

The Splunk SOAR main dashboard provides security teams with an overview of SOC activity, notable events and playbooks, and a summary of return on investment from automated actions. The Automation ROI Summary shows the real-time impact of automation as the SOC uses it, such as time saved, dollars saved, FTE (full time employees) gained and mean dwell time.



[5]https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

CASE STUDY

Norlys: Success With SOAR

With 1.5 million customers, Norlys is Denmark's largest utility and telecom company. After building their own log analytics and incident response systems, the Norlys security team was hobbled by repetitive tasks, too many tools, slow web UIs and cumbersome processes. With Splunk, Norlys automated repetitive tasks and centralized investigations.

View Case Study

The results:

- 35 hours of work saved per week
- 30 seconds to complete processes that once took 30 minutes
- 98% less time to open tickets

Top 5 boring tasks that Norlys automates:

1 Forwarding notables from Splunk ES to SOAR
From **3 minutes** to **2 seconds**

2 Automating investigation upon AV alerts
From **40 minutes** to **10 minutes**

3 Automating investigation upon IOC hits from threat feed
From **15 minutes** to **10 seconds**

4 Automating the process of obtaining browser history
From **30 minutes** to **20 seconds**

5 Automating ticket opening to external systems
From **10 minutes** to **10 seconds**

"Automation is changing how teams traditionally use a SIEM. We heavily rely on Splunk SOAR, and Enterprise Security. They complement each other in a very good way and allow us to improve security capabilities for the entire company."

– Tibor Földesi, Security Automation Analyst, Norlys

Modernize security to transform your business

For CISOs to be the strategic partner businesses need — and for security analysts to find opportunities for professional development — orchestration and automation are essential. Splunk SOAR allows security teams to realize the full potential of investments in security tools and security talent.

Try Splunk SOAR Today

splunk>

22-20301-Splunk-Transformational CISOs Guide to SOAR-102