splunk>

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.

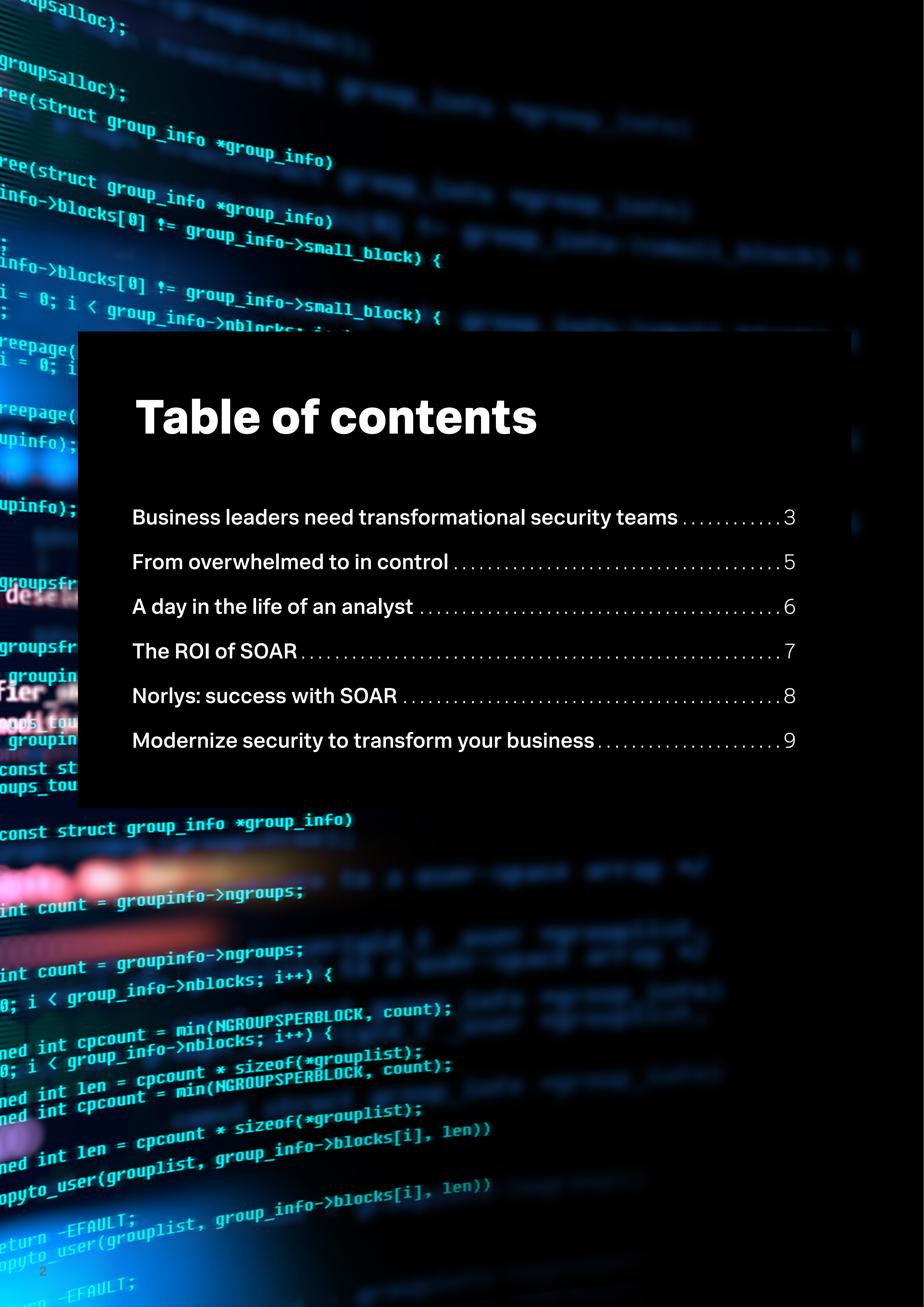


Table of contents

Business leaders need transformational security teams

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

Like CIOs and 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.

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.[1]

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. The ability to take smart risks
3. Leadership skills
4. The ability to identify and grow 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.

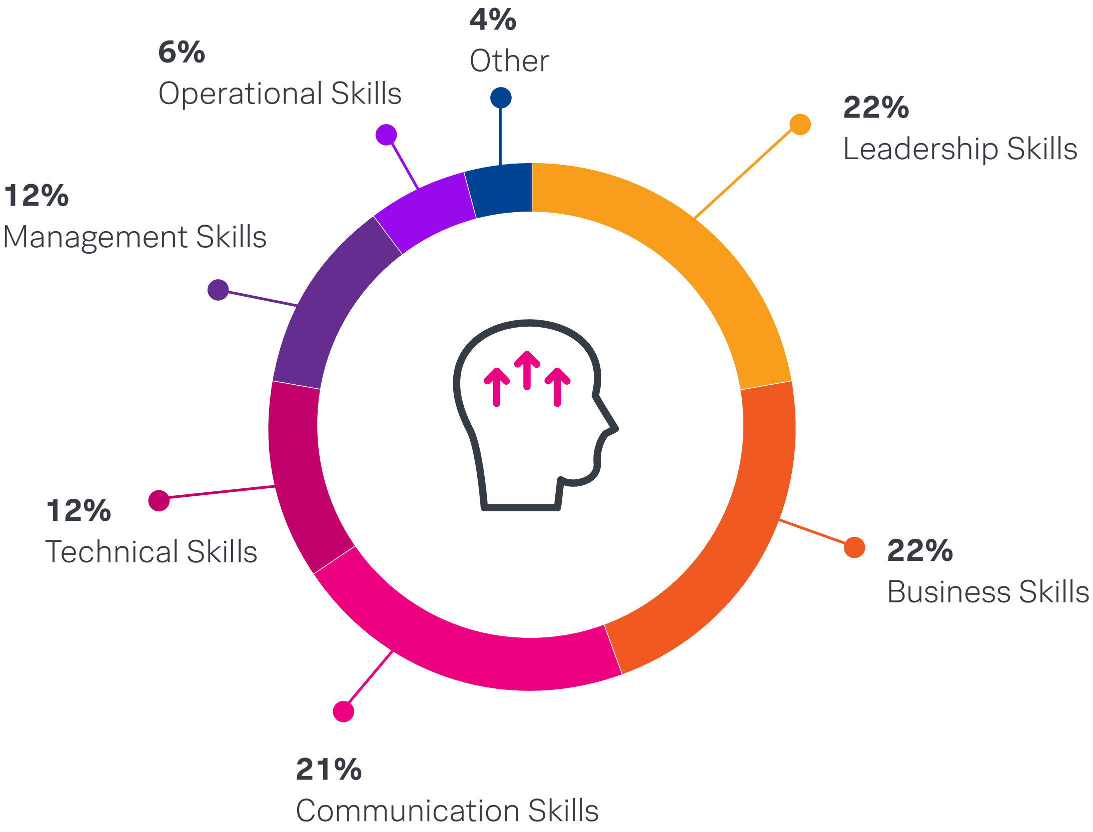
> **"Change is the one constant in cybersecurity. Orchestration and automation help us respond to the relentless evolution of threats. We can't wait for the next threat. We need to seek it out."**
>
> – Pamela Fusco, CISO, Splunk

[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 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**.

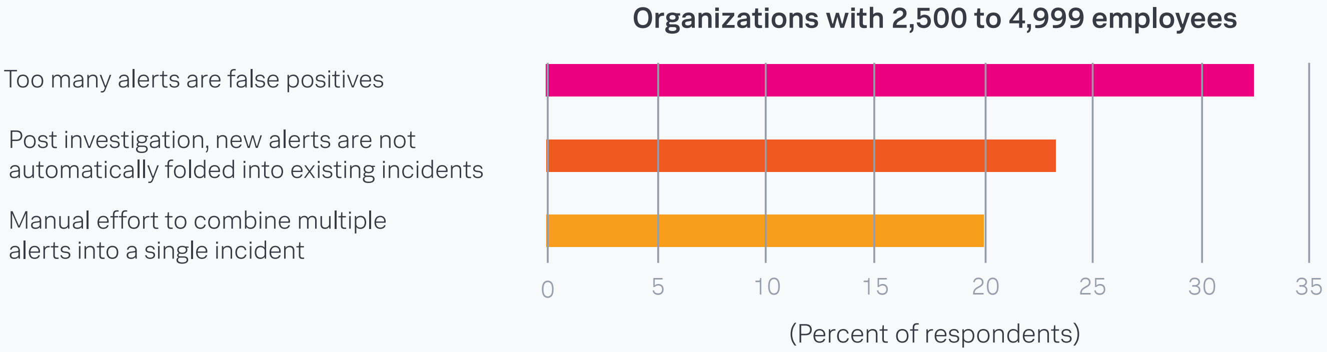
From overwhelmed to in control

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 SOCs around the world. This well-documented talent gap, combined with the sheer volume of alerts per day, explains why 64 percent of security tickets generated per day are not being worked.[3] Analysts aren’t able to address every alert every day, leaving their companies vulnerable to attack.

64%

of daily security alerts are unaddressed[4]

With security teams struggling to keep up with alerts, CISOs can’t provide strategic guidance and analysts don’t have the time to perform critical engineering and optimization tasks, tune automated alert responses, and proactively hunt for threats.

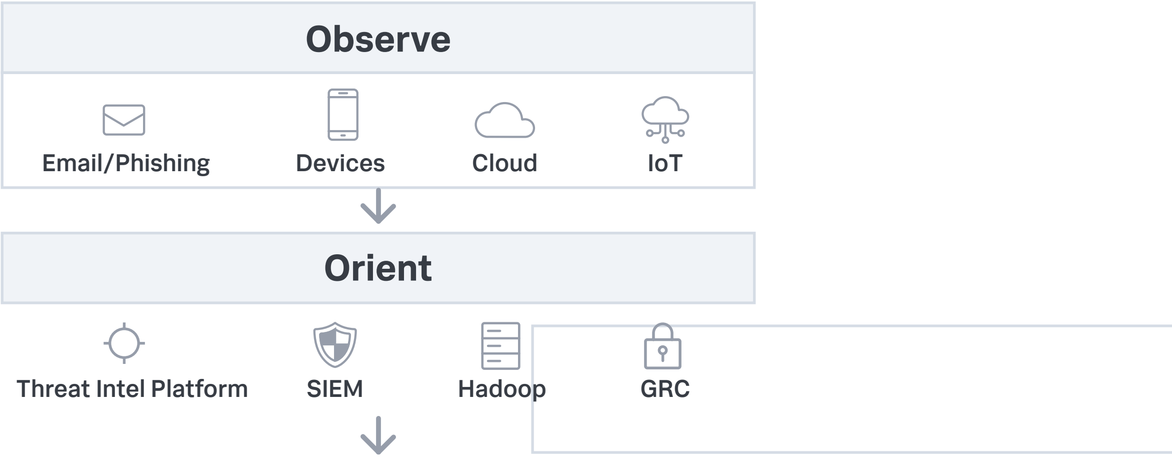
The answer to these challenges is security orchestration, automation, and response (SOAR). SOAR platforms, like Splunk SOAR shift the balance of power in security. By removing mundane and routine tasks from the analyst’s to-do list, and by orchestrating security tools to work together, security teams can spend more time improving the organization’s security posture and driving the business forward.

[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



Observe

Email/Phishing

Devices

Cloud

IoT

Orient

Threat Intel Platform

SIEM

Hadoop

GRC

10,000 suspicious incidents per day

Without SOAR

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

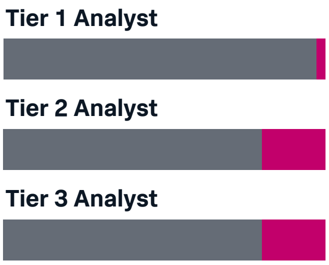
Analyst

Decide and Act

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

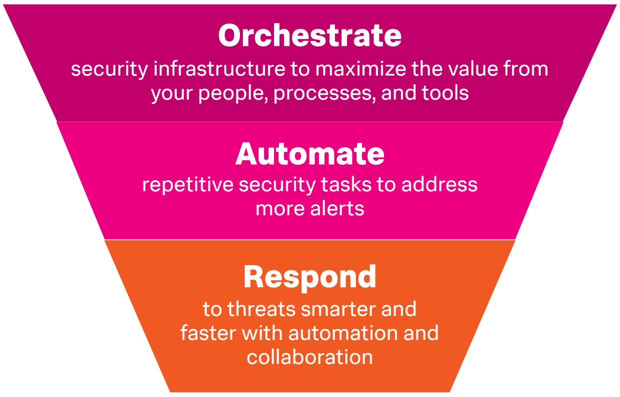
⬛ Time spent being **reactive**

🟥 Time spent being **strategic**



Time to respond:
30 minutes

With SOAR



Orchestrate security infrastructure to maximize the value from your people, processes, and tools

Automate repetitive security tasks to address more alerts

Respond to threats smarter and faster with automation and collaboration

Act on every alert every day

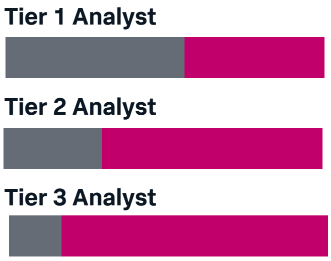
Analyst

Decide and Act

With SOAR, the analyst workflow is simplified: collaborate and respond to security incidents fast.

⬛ Time spent being **reactive**

🟥 Time spent being **strategic**



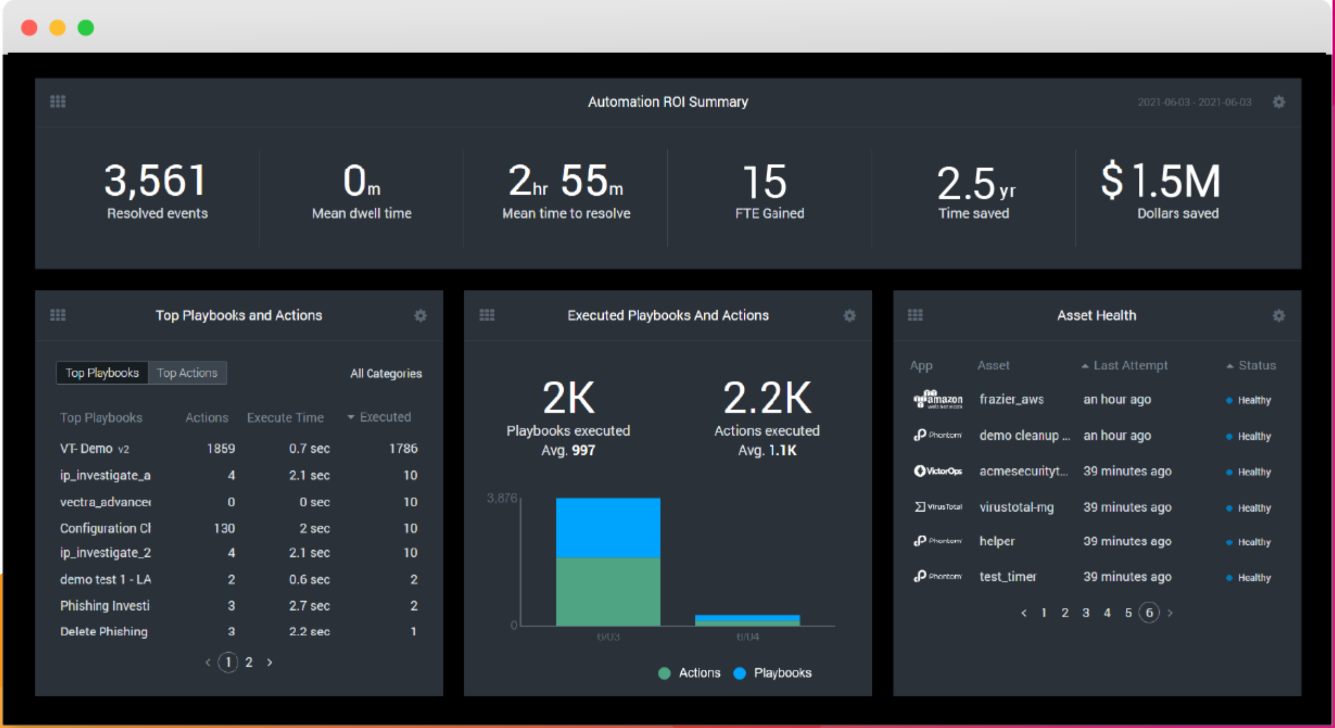
Time to respond:
30 seconds

The ROI of SOAR

By one estimate, the annual cost of stopping phishing attacks is nearly $700,000. The cost of ransomware can also be expensive and cause lasting reputational damage. SOAR saves time and money.[5] The amount of time saved is measured in the manual workload equivalent of a full-time employee. For example, with a SOAR platform, a team of three analysts in a SOC can have the impact of a team of 10 to 15 analysts that 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. Automation is the only solution.”**
>
> – 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.



Automation ROI Summary

2021-06-03 - 2021-06-03

3,561 Resolved events

0m Mean dwell time

2hr 55m Mean time to resolve

15 FTE Gained

2.5yr Time saved

$1.5M Dollars saved

Top Playbooks and Actions

Top Playbooks | Top Actions

All Categories

Top Playbooks	Actions	Execute Time	▾ Executed
VT- Demo v2	1859	0.7 sec	1786
ip_investigate_a	4	2.1 sec	10
vectra_advance	0	0 sec	10
Configuration Cl	130	2 sec	10
ip_investigate_2	4	2.1 sec	10
demo test 1 - LA	2	0.6 sec	2
Phishing Investi	3	2.7 sec	2
Delete Phishing	3	2.2 sec	1

‹ 1 2 ›

Executed Playbooks And Actions

2K Playbooks executed Avg. 997

2.2K Actions executed Avg. 1.1K

Asset Health

App	Asset	▴ Last Attempt	▴ Status
amazon web services	frazier_aws	an hour ago	● Healthy
Phantom	demo cleanup ...	an hour ago	● Healthy
VictorOps	acmesecurityt...	39 minutes ago	● Healthy
VirusTotal	virustotal-mg	39 minutes ago	● Healthy
Phantom	helper	39 minutes ago	● Healthy
Phantom	test_timer	39 minutes ago	● Healthy

‹ 1 2 3 4 5 6 ›

[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 webUIs, 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

The top five 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**

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>