THE ROI OF SECURITY ORCHESTRATION AND AUTOMATION

KOMAND

Table of Contents

INTRODUCTION

The Security Landscape Today

Speed has never been more important for security operations teams today. As the technology we use at work expands from desktop computers and laptops to the internet of things, and as company-issued devices give way to a culture of BYOD, it's becoming increasingly difficult to discover and contain security threats. As the technologies change, the threats evolve, and so must security operations.

Today, security operations is often slowed down by manual processes that would be better left to machines. Additionally, while there are many great security tools on the market, they don't all integrate with other tools or systems out of the box, or share information in the form of relevant and contextual data and alerts.

Today's security talent gap also exacerbates these problems, as teams are stretched thin, struggling to optimize the resources they have, often without enough time or expertise on their side. Alert fatigue is all too common, and, in the chaos, incidents, compromises, and breaches are slipping by unnoticed.

Security Orchestration and Automation

It's not all doom and gloom, though. Security orchestration and automation are becoming an increasingly vital aspect of many organizations' security strategies, and they're helping to stack the deck in favor of defenders. In particular, we have seen many companies use orchestration and automation to successfully tackle these common security processes and investigation types:

- Email Phishing
- Privilege Escalations
- Malware Containment
- Compromised Credentials
- Security ChatOps
- Vulnerability Management

The Benefits

Security orchestration and automation offers security teams:

- **Faster incident response times**
- **Major time and cost savings**
- **Increased accuracy across security operations**

In fact, we have seen teams reduce their average time to response from **30 minutes to 5 minutes**, which equates to around **83% of time saved per alert**. Additionaly, teams dramatically improve their accuracy8, and ultimately they do more with the resources they have.

With machines gathering and compiling relevant context about a security event, teams can switch their focus to analysis and response instead of spending exorbitant amounts of time manually collecting data. Additionally, security orchestration and automation adds flexibility into the detection and response process, allowing teams to automate as little or as much as possible.

When to Introduce Security Orchestration and Automation

The ideal time for organizations to begin putting security orchestration and automation to work is **once they have invested in the people, processes, and technology that drive operations**.

Some examples include having: an IDS, a case management tool, a fire wall in place, threat intel and forensics tools, incident response processes, and a few full-time employees dedicated to security. Orchestration and automation optimizes all these investments by tying them together in a streamlined and cohesive way.

So if you're thinking about bringing security orchestration and automation to your organization, your first question (or your boss's) may be, *"What is the ROI?"* It's a smart question, and the purpose of this white paper is to provide you with a framework for calculating and demonstrating the ROI for your unique organization.

Demonstrating the Return on Investment

Security orchestration and automation can make teams faster and more efficient. But how can we measure exactly how much faster, and how much more efficient? How can security folks charged with investing in the right tools, processes, and people demonstrate the clear ROI of an organization's investment (or potential investment) in security orchestration and automation?

We know this is a difficult question to answer, and so we've put together a framework that will help your company evaluate the return on your investments in security orchestration and automation.

In this white paper, we will discuss your options:

- Manual security operations
- Building security orchestration and automation internally
- Out-of-the-box security orchestration and automation

We will show you how metrics surrounding the three primary drivers of security (people, processes, and tools) can be directly impacted by security orchestration and automation, which helps illustrate the value this can bring to your entire team. With this information, you can secure buy-in from leadership or simply prove the value of what you're already doing. Without further ado...

THE COST OF MANUAL SECURITY OPERATIONS

Overview

To visualize the ROI of security orchestration and automation, let’s look at how much the manual way of doing things actually costs. So, if your security operations are manual today, here’s what that may look like, and the costs involved. We break it into 3 sections:

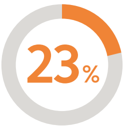
People

Process

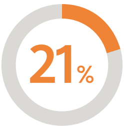
Technology

People

One of the most expensive and complex parts of your security investment is personnel. And that's, in part, due to the security talent shortage. In fact, 23% of security pros say the talent shortage is the biggest challenge facing the entire information technology industry. Unsurprisingly, there is a near-0% unemployment rate for folks with a security background. That's a good thing for security professionals, but not for employers. Hiring managers report that 21% of senior-level security jobs (those requiring 10+ years of experience) take over a year to fill.



OF SECURITY PROS SAY TALENT SHORTAGE IS LARGEST CHALLENGE



OF HIRING MANAGERS SAY SR. SECURITY JOBS TAKE 1 YEAR TO FILL

So, assuming you can find enough security experts to fill your open reqs, you'll have to pay them top dollar. Here's a look at some common security titles and their median salaries in a major city like Boston, according to Glassdoor, Silverbull, and several other sources:

ROLE	MEDIAN YEARLY SALARY
Security Analyst	**$93,000**
Senior Security Analyst	**$112,000**
Information Security Manager	**$105,768**
Security Engineer	**$98,000**
Security Director	**$115,000**
Chief Information Security Officer (CISO)	**$204,000**

So, let's talk about how salaries are being used. When we talk about human capital, what we're really talking about is time spent. How much time are your valuable security team members spending on routine tasks that could be automated?

For our purposes here, and to keep things simple (and conservative), we'll use an average salary of **$100,000** per security employee. Even without including other forms of compensation (like benefits or a 401(k) match), if your security hires work 40 hours a week for 48 weeks of the year (again, this is all conservative), that comes out to around **$52 an hour**.

At many organizations, security employees spend a bulk of their time on **dealing with security alerts**... many of which are false positives. The average large-scale U.S. enterprise receives **10,000 security alerts per day**, That includes everything, from false positives to actual indicators of compromise.

So it's no surprise that security teams far and wide suffer from alert fatigue today. Looking at the numbers here, **alert fatigue is probably costing you a ton of money**. It can also cost your reputation; take the well-publicized Target breach as a glaring example. Experts believe that it happened because real threats slipped through unnoticed due to alert fatigue.

Now, not all alerts get investigated, but for the ones that are manually investigated, on average, it takes more than **30 minutes.** Now multiply that by however many of alerts actually get handled every day. Naturally, as more alerts come in, more hires need to be made to deal with them, so personnel costs go up over time, too.
The bottom line is that you don't want your hard-won security talent to be spending their valuable time on repetitive manual tasks or false positives.

Security orchestration and automation can help you optimize the value of each member of your team by allowing them to focus on strategic, value-add efforts that can move your business forward faster and more effectively.

> *You don't want your hard-won security talent to be spending their valuable time on repetitive manual tasks or false positives.*

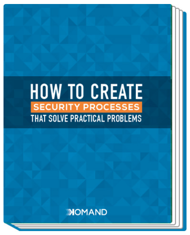
Process

It takes significant time to develop *good* security processes—ones that work consistently, save time, and improve your overall security posture. Many processes are handled manually today, which can take up huge amounts of time.

For example, to manually investigate a phishing attempt, you will need to manually:

- Grab the alert
- Extract URLs, IPs, domains, hashes, or attachments
- Scan the contents to see reputations or see if malicious content is found
- If an artifact is are indeed malicious, perform escalation by creating a ticket and notifying the team
- Find out whether the user clicked the links or downloaded the content, and if so, what happened next
- If any malicious code was downloaded, you will have to:
    - Figure out where the victim machine is located
    - Identify compromised files
    - Wipe and restore

It can take a long time to develop a clear security process like the above and then train the team on how to execute it. Additionally, once a process is developed, it needs to be tested and regularly maintained and updated. So you can see how manual processes can easily take up quite a bit of your security team's time. As we'll explain below, this amount of time and effort is often untenable given the security talent shortage.



Looking to develop efficient security processes, but don't know where to start? Get our guide, "**How to Create Security Processes That Solve Practical Problems**".

DOWNLOAD THE GUIDE NOW

Technology

The tools you need to purchase in order to conduct effective incident response will depend upon your organization. Here are the major categories that you may need:

- Network or Host security monitoring
- Log collection and aggregation
- Application security
- SIEMs and event consoles
- Malware analysis
- Threat intel

IF you don't have all of these tools in place, you may be able to use some free or open-source security tools to get started. But regardless, making investments in these areas will ultimately make your incident response process easier.

To get specific around numbers for your unique organization, we have a table to help you calculate your tools costs. Remember: there is often a personnel cost associated to run and maintain these tools.

CATEGORY	INITIAL COST	RECURRING COST	MAINTENANCE*
Security Monitoring			
Log collection and aggregation			
App security			
SIEMSs and event consoles			
Malware Analysis			
Threat Intel			

*Hours spent x rate of pay

Finally, remember that, even with best-in-class tools in place, you won't be able to use them to their full potential without the ability to integrate them and automate processes between them. So if you skip integration altogether, that adds costs in the form of manual human effort. If you decide to build custom integrations, that can take up significant time before you're able to use things to their full potential.

THE COST OF DIY SECURITY ORCHESTRATION & AUTOMATION

DIY Security Orchestration & Automation

By now, you've probably come to the conclusion that manual security processes is not the most efficient or effective way to move security forward. You might be thinking, okay: We'll just build some automation into our workflows, right? Unfortunately, it's not always *that* simple.

Companies who try to build their own proprietary security automation systems from scratch do so for good reasons. They want to take advantage of all the benefits that automation can offer! We can't fault them for that. And if you have a large team of developers at your disposal, adding orchestration and automation is possible, especially if your internal culture is centered around DIY development. But there's also much to consider when DIY automation.

We've witnessed first-hand that "rolling your own" often comes with many unpleasant hidden costs.

- The time it takes to build automation is almost always far more than projected.
- Teams frequently hit snags along the way, scope creep grows, and ultimately expert consultants are brought in to move the process forward, which can wind up costing a lot of money and extend the project further.
- The time your internal security experts (or developers) spend building automation is time that they can't spend focused on other work such as revenue-generating projects, or other high priority work.
- The maintenance cost of automation systems when new process or tools are introduced, or when scale becomes a concern.

In most cases, it simply doesn't make sense from a cost and time perspective to build your own security orchestration and automation. All of this is on top of the cost of your tools and personnel, which we covered above.

THE COST OF OUT-OF-THE-BOX SECURITY ORCHESTRATION & AUTOMATION

Out-of-the-Box Security Orchestration & Automation

So what's the alternative? If you want to take advantage of all that automation can offer, without the steep costs of DIY, then investing in an out-of-the-box security orchestration and automation platform like Komand is your best bet.

These, of course, come with their own costs. But the good news is that they will help you get more out of your current security investments, including people, processes, and tools. Not only that, but they do so faster and more efficiently, so the ROI is quickly attainable. We'll break down the benefits between people, process, and technology again.

People

Human time, and the cost of their time, is the area where you'll see the biggest savings and ROI when implementing orchestration and automation. Because less time will be spent on manual processes, you can do more with the people you have.

You will also put your best talent to work on more strategic defense initiatives like vulnerability management or threat hunting, which will make them happier, and could retain them long-term. The less time your highly skilled security team spends on manual processes, the better your human resources ROI will be.

> *Human time, and the cost of their time, is the area where you'll see the biggest savings and ROI when implementing security orchestration and automation.*

Process

Security orchestration and automation platforms streamline the creation of automated processes, and oftentimes, many offer built-in or community-contributed workflows. When it is necessary to build custom automated processes, developing and executing them should be faster than ever, with less time-intensive work involved.

That's all time that can be funneled into threat hunting and analysis using the detailed context that orchestration and automation solutions offer. The result? Streamlined processes that enable a faster, more effective and accurate response to threats plaguing your organization.

> *Streamlined processes that enable a faster, more effective, and accurate response to threats plaguing your organization.*

Technology

With an out-of-the-box solution, you'll still utilize the same products as you would normally use to conduct your security operations. However, you'll be able to extract more value out of them through integration and automated workflows.

Many security orchestration and automation platforms offer pre-built integrationfor your your tools, meaning it's plug-and-play to use them, no manual work or coding required. Put simply, security orchestration and automation enable you to get more out of the resources you've already invested in. The only new cost will be the platform, and with the amount in human time you save, and ultimately cost savings, will justify the purchase.

> *You'll be able to extract more value out of [your security products] through integration and automated workflows.*

THE ROI OF SECURITY ORCHESTRATION & AUTOMATION APPLIED

Applying ROI Theory

Now that we've discussed the advantages and ROI theory of orchestration and automation, let's put these concepts to work.

First, recall that we're using the average salary of **$100,000** for a security employee. That breaks down to an **hourly wage around $52**. Break it down even further to minutes, and it's **$0.87 per minute**.

Second, an alert, on average, takes **at least 30 minutes** to triage, investigate, notify, and respond. All of that work is manual, so multiply 30 by $0.87. **This means each alert costs you $26.10.**

Third, think about how many alerts you and your team manually handle in a day. For a small enterprise, let's use **100 alerts per day** as an example. That means you spend **$2601 per day on alerts**. Times that by 365, assuming you have a 7 day a week SOC, and you're talking **$952,650 a year** spent on alerts alone.

Now, we know capital needs to be invested to protect the organization. But with new technologies like security orchestration and automation available, your capital can be invested in other, more valuable and meaningful ways -- not just for the benefit of the organization, but for security team members, too.

Based on a security analyst salary of $100,000 a year, an average TTR of 30 minutes and 100 alerts per day, you would be spending ...

87¢	$26.10	$2,610	$953k
PER MINUTE	PER ALERT	PER DAY	PER YEAR

Now, let's compare these numbers with security orchestration and automation, and the benefit that it can bring once workflows are in place.

	MANUAL		AUTOMATION	
Alert Triage	10 mins	$8.70	Automated	$0
Analysis	5 mins	$4.35	5 mins	$4.35
Escalation/Notification	5 mins	$4.35	Automated	$0
Response/Remediation	10 mins	$8.70	Automated	$0
TOTAL	30mins	$26.10	5 mins	$4.35

With security orchestration and automation, you'd see...

83%
REDUCTION IN COST

$4.35
PER ALERT

$435
PER DAY

$159k
PER YEAR

Comparing the manual process with the automated process shows an **83.3% reduction in time and cost**. That costs savings is equal to roughly **8 new people you could hire** or **countless new security products you could purchase**.

Now, in this particular scenario, a security team member performed the analysis. However, analysis could easily be automated for certain processes, leading to a further reduction in time and cost.

The beauty of security orchestration and automation is that it can be customized based on your unique organization and needs. And with a platform like Komand, what you choose to automate or involve a human in can be extremely flexible.

CONCLUSION

Getting the Most Value from Your Security Operations

You’ve seen how much time and money security orchestration and automation can save you. And while you could add both of these concepts with custom development, using an orchestration and automation platform will bring value and and demonstrate ROI at a considerably faster and more effective rate. This is where Komand comes in.

Komand is the orchestration and automation layer for security operations. We can help you orchestrate and automate your security tools and tasks faster than ever before. With Komand, you can easily connect your tools and automate all your security processes, without writing a single line of code. Save time and money, all while increasing productivity, efficiency, and accuracy!

To get started, visit komand.com to request a demo or get in touch with a member of our team at sales@komand.com.

About Komand

Komand is a security orchestration and automation platform that gives security teams the power to quickly automate and streamline security operations, with no need for code. Teams can integrate their tools, build automated workflows, and utilize human decisions to accelerate incident response and move security initiatives forward, faster.

Learn more at **www.komand.com**

KOMAND