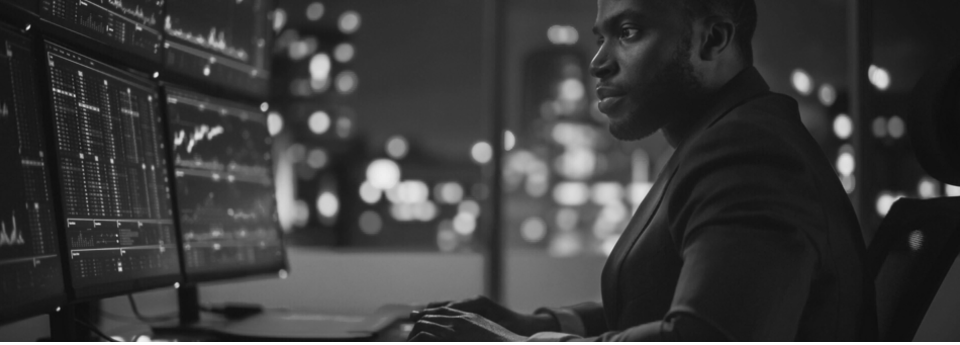
DEVO

Deal Your SOC a Winning Hand

A CISO's Guide to Strategizing and Investing in a Modern SOC

TABLE OF CONTENTS

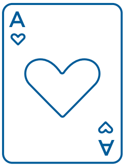


CISOs can’t afford to gamble on the effectiveness of their security operations center.

SOCs lie at the heart of a modern cybersecurity program, central to an organization’s ability to swiftly detect and respond to incidents that cause costly data breaches, ransomware disruptions, and ongoing cyber compromises.

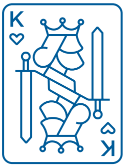
But dealing your SOC a winning hand takes a whole lot more than just keeping a straight poker face in front of your board. You need a solid combination of strategic planning, well-balanced tooling, and well-supported people to run your SOC day in and day out. There’s no easy shortcut to this game. But there is a winning formula that many security leaders use to improve the odds that their teams can successfully execute on a solid strategy.

Call it the royal flush of the SOC world. SOC teams win when CISOs ensure they have:



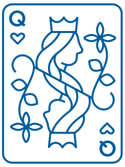
ACE

A strong security data platform that can ingest, process, and analyze data with the speed and scale that enable truly real-time analysis and alerts.



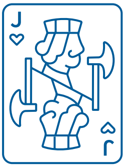
KING

Automated case management and incident response playbook capabilities that aggregate and group alerts, streamline activities into fewer cases, and automate common response actions.



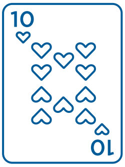
QUEEN

The ability to identify and communicate threat activities using a common language, namely through the MITRE ATT&CK® framework.



JACK

Automated correlation and searching of incident and threat intel data that speeds up investigations and cuts down on burnout-inducing manual work.



10

Access to the broader security community, with discussions and information sharing that helps analysts tap into valuable information and collaborate to solve problems faster.

Here's how to plan ahead and ensure you deal your SOC team a winning hand.

Start With a Winning Strategy

Before digging into what it takes to develop a good SOC strategy, let's talk about the current landscape. For most organizations today, the cyber risk management odds are very much in favor of the attacker. 61% of SOCs handle more than 1,000 alerts per day and nearly 40% of IT security professionals say their SIEM is ineffective because it could not scale to meet their business needs.

61%

of SOCs handle more than 1,000 alerts per day

CISOs need a thoughtful strategy in order to make progress on overcoming these challenges and start shifting the odds in their favor. Unfortunately, too many security leaders still play fast and loose when it comes to planning out their SOC's capabilities and the processes that analysts use to investigate and remediate incidents. According to Deloitte, only 62% CISOs develop an operational and strategic plan to defend against cyberthreats, and just 58% have a cybersecurity incident response plan that's updated and tested annually.

Every SOC strategy is different, as the risks that SOCs should be monitoring most heavily for will be dependent on the assets an organization supports, the risk priorities of the business, and the threats that are most likely to target their specific industry. On top of all of these factors are budgetary realities, as well as staffing and tooling resource constraints.

Outlining Your Plan

As you plot out the future of your SOC, your strategy must include:

Your Operating Model
You need to decide between a centralized in-house SOC, multiple distributed in-house SOCs, a managed/outsourced SOC, or a hybrid SOC with some combination of in-house/outsourced capabilities.

Staffing and Skills Development
On top of establishing roles and responsibilities, you have to consider career paths, mentorship, and training.

Tooling Roadmap
Set a course for upgrades based on current visibility/controls gaps, availability of analysts and skills to run the tools, automation needs, and budget considerations—including plans for managing stack complexity/tool sprawl.

Proactive Planning for Future Growth
Your strategy must be proactive and consider your company's projected future growth and expansion. For example, if your organization is planning to expand into new markets, what do you need to plan for from an attack surface perspective today?

Incident Response Preparation
Establish processes and procedures that standardize how analysts and responders react in different detection and response scenarios.

Controls Validation and Testing
Institute regular tabletop, simulated attack, penetration tests, and red/purple team exercises to see how well SOC controls and incident response plans work in action.

Performance Monitoring
Establish measurable KPIs to track security outcomes over time. Common KPIs include number of alerts, number of reported incidents, and MTTD/MTTR.

CISOs should be collecting opinions, insight, and observable data to determine the right strategy. This means collaborating closely with business stakeholders, listening to analysts about their needs and their pain points, and being mindful of gaps in coverage that could skew risk assessments.

> CISOs should be collecting opinions, insight, and observable data to determine the right strategy.

Collaborating With Business Stakeholders

CISOs need to have conversations with their C-suite/board in order to align their strategy to business risk priorities and get buy-in. You should be asking questions that will get everybody to align on what the mission-critical processes are that need to be protected, the assets these processes are tied to, and what resources are required to ensure your SOC prioritizes the visibility and protection of those assets.

Getting Analyst Input

As the boots on the ground, security analysts can offer some of the most painful and insightful observations about the current limitations of your existing SOC—as long as you're willing to listen. Honest analyst input can provide insight into why a SOC may be missing critical incidents, why a team is experiencing churn or morale problems, and why MTTD/MTTR is stagnant or increasing. Some areas to explore with your analysts are where they're spending the most time on manual tasks, how many alerts they're missing each day, how many tools it takes for them to capture security data, and what the most frustrating parts of their job are today.

Assessing Coverage Gaps

In addition to collaborating with both business stakeholders and analysts, consider conducting a risk assessment and tools gap analysis that takes an honest look at the potential controls and visibility holes in your existing security stack. It may be beneficial to have an MSSP do a risk assessment for your organization. This will require not only a good awareness of the threat environment, but also thoughtful usage of new technology to scan for previously undetected tactics and techniques.

Recruit and Retain the Best Players

SOC automation can help speed up response, but the success of your SOC ultimately depends on smart people backed by great resources and training. Unfortunately, most organizations are unable to attract the right talent, and even when they build a dream team, they're unable to provide the support necessary to retain talent.

A recent study conducted by Wakefield Research on behalf of Devo found that 83% of security professionals admitted that they or someone in their department has made errors due to burnout that have led to a security breach.

What's more, 85% say they anticipate they will leave their role due to burnout, with 24% saying they're thinking of leaving cybersecurity entirely.

85%

anticipate they will leave their role due to burnout

24%

think of leaving cybersecurity entirely.

The study also found that almost half of the surveyed analysts felt that their leaders do not take proactive steps to help them avoid burnout and achieve maximum SOC performance. The top three measures they said they wished their leadership would implement to support them were:

1. Offering additional training, mentorship and development
2. Increased staffing
3. Investment in automation tooling

Successful CISOs must be prepared to go all in on recruiting and supporting their SOC analysts. This means not only having enough people, but also the right tools to allow them to flex their skills and maximize their efficiency. This will not only improve job satisfaction and retention, but it will also foster positive security outcomes for the business.

> Successful CISOs must be prepared to go all in on recruiting and supporting their SOC analysts.

Dominate the Game with the Right Tools

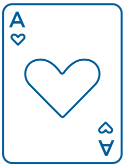
Unfortunately, many SOCs have unfavorable odds because they depend on legacy security information and event management (SIEM) platforms. These tools can't scale to handle the volume, variety, and velocity of security data that needs to be collected and analyzed across today's digital infrastructure to offer true SOC visibility. As a result, SOC teams are left to detect and investigate threats with incomplete information and limited visibility. This makes it difficult for security analysts and leaders to get the kind of visibility, consistency, and automation necessary to run a truly effective SOC.

Here are some of the current limitations that legacy tooling places on SOCs today and how Devo can deal you the most playable hand to your SOC.

Why Your Current SIEM Is Sandbagging You

Current SIEM technology wasn't built to be a security data platform. Legacy platforms are slow to index and normalize data, can't make real-time queries, and struggle to make the complex correlations or connections necessary to enrich attack information with valuable context. As a result, analysts are always 15–20 minutes behind an attack.

Devo Deals You: AN ACE

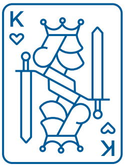


Devo HyperStream is a real-time data analytics engine that streamlines data ingestion, offers linear scalability, and enriches data at the point of a query to provide analysts with unlimited, multisource context. Most importantly, all those queries happen in real-time.

Do You Know When to Hold'em or Fold'em?

Security analysts are absolutely overwhelmed by alerts, and many of them are false positives or highly duplicative alerts about real threats. This leads to time wasted investigating incidents that aren't really threats and the inability to clear the alert queue each day.

Devo Deals You: A KING

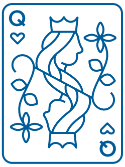


Devo ThreatLink arms analysts with decision automation and case management. It validates alerts and does the correlation automatically so they're aggregated and organized into cases. This provides a 90% reduction in alert noise, giving analysts an easy way to view data organized by incident cases rather than individually triggered alerts.

Know Your Limits

One of the biggest challenges SOC teams face is not knowing what they don't know. Too many security analysts worry about the visibility gaps lurking in their tool stack, and they expend energy and effort trying to cover those gaps through manual leg work. This is not sustainable.

Devo Deals You: A QUEEN

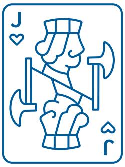


Devo's MITRE ATT&CK Adviser application not only shows security teams the tactics and techniques they currently have no detections against, but also what data sources they'll need to add in order to close those gaps.

Don't Go on Tilt

63% of security teams today use more than 25 different tools to get security visibility, and most organizations feed 30 or more data sources into their SOC. The problem is that all of this data is rarely fully integrated or aggregated into a single platform. This leaves analysts with a ton of manual, time-consuming investigative tasks to look for relevant information and piece everything together. Doing this work slows down detection and stops the SOC from acting quickly.

Devo Deals You: A JACK

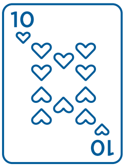


Devo DeepTrace uses AI to automate much of the investigative process for analysts, asking hundreds of thousands of questions in minutes to autonomously construct traces detailing an attacker's actions. It assembles the answers and timeline so analysts can get to the decisions and remediation work more quickly.

Learn to Read the Table

Cyberattackers outnumber defenders and only need to succeed once, whereas the SOC needs to be right all the time. SOCs often operate in an isolated bubble that makes it difficult to learn lessons from other organizations that are going through similar incidents. While open source threat intelligence feeds can help ameliorate that, information sharing and collaboration needs to go deeper in order to gain the wisdom of the community.

Devo Deals You: A 10



Devo offers a trio of options to tap into the content and wisdom of the cyber community. **Devo Collective Defense** securely analyzes alert data from across the Devo community and identifies insights, trends, and Indicators of Compromise (IOCs) that analysts can act upon immediately. The **Devo Connect** community allows experts around the globe to collaborate on solving security problems together. And **Devo Exchange** is a content marketplace providing on-demand access to an ever-growing library of curated security content created by Devo, our partners, customers, and the greater security community.

Win Tomorrow Today

Your strategy, your players, and your tools are all crucial to winning the cybersecurity game. Give your SOC a leg up by prioritizing thoughtful planning and investing in the royal flush of the SOC world. After all, if your SOC wins, your organization wins.

Are you ready to stack the deck for your team?

Devo unleashes the power of the SOC. The Devo Security Data Platform, powered by our HyperStream technology, is purpose-built to provide the speed and scale, real-time analytics, and actionable intelligence global enterprises need to defend expanding attack surfaces. An ally in keeping your organization secure, Devo combines the power of people and AI to augment security teams, leading to better insights and faster outcomes.

Visit devo.com to learn more.

DEVO