PwC and Google

From SecOps to SecOptimal: Transform your program and your business

Traditional Security Operations (SecOps) programs require a more agile approach to harnessing data and keeping up with emerging security threats. These programs have been challenged to handle a wide array of data sources, creating an even murkier picture of the threats they should prioritize.

Your SecOps professionals should consider transforming their programs **from SecOps to SecOptimal.** Host everything – technologies, processes, dashboards, automation – onto a single, unified platform.

The upside: everything works together easily and effectively, delivering better security and automation to save time and money. Given it's platform-based, there'll be no need to transform again. You can just switch out features, instead — more savings for your enterprise.

This type of movement requires nimble coordination between C-suite stakeholders – not just the CISO. There's a real opportunity to improve program efficiency, free up resources and enhance security to deliver greater value to customers and investors, if the C-suite is aligned and engaged.

The challenge at hand

Your security information and event manager (SIEM) was most likely designed for the smaller and more contained digital universe of even a few years ago. It might take hours to sift through quantities of logs and other data in search of a given threat.And you may have invested good money for security applications to handle zero-trust architectures, detect anomalies, encrypt data in motion and at rest, and perform myriad other tasks that defense-in-depth requires.

But if these technologies don't communicate with one another, they can't work together. Your SIEM should operate with information from your security stack.

Likewise, if the SIEM doesn't operate in tandem with security orchestration, automation, and response (SOAR) due to lackluster integration, your teams should correlate the information and coordinate responses manually. This can be time consuming, tedious and ineffective, leading to a drain on time and potential budget constraints.

SecOptimal: Better security, savings and value

A SecOptimal program offers coordination, orchestration and collaboration for enterprise-wide security. Your program can become:

- **Expansive.** For the new SecOps, there's no such thing as too much information. Built in the cloud, for the cloud, its SIEM takes in as much data as your systems, networks, and devices send. There's no need to retrofit legacy technologies with expensive add-ons to avoid overload.
- **Proactive.** SecOptimal means you don't have to generate your own detection-and-response workflow.

  Trusted vendors work with you to set the parameters, configure the platform for your enterprise's needs, and validate your controls. Your platform's threat hunting service tells you when a new threat actor might cause problems, and provides the info you need to program SOAR for rapid remediation in the event of an attack.
- **Fast.** Legacy SIEMs can only store so much data. Typically, anything older than a few months goes into a repository for comparison and analysis when needed. But before it can be used, it should be downloaded from storage – a process that can take many hours.

  Pressed for time, analysts might opt out of accessing this older data, losing some of their ability to spot patterns and react effectively. SecOptimal means your SIEM queries petabytes of data in seconds, all of it immediately accessible in the cloud.
- **Optimized.** No more using your finest and brightest to perform mundane, hum-drum data analytics tasks, or overloading your analysts as information pours in from more and more sources – if you can even find enough analysts with the experience you need. You could break your budget trying, and still not succeed.

  Artificial intelligence (AI) can perform time-consuming analytics in a fraction of the time that your staff would take, and at a much lower cost.
- **Intelligent.** Cyberattack is no longer a threat: it's a promise. Spies, saboteurs and profiteers alike are trying to find a way into your enterprise systems. To stop them, your SecOps should natively integrate with high-quality threat intelligence.

  SecOptimal threat intel means access to swaths of internet traffic. It means your threat intel's security researchers work 24/7 to understand cybercriminals' tactics, tools, and techniques, and tell you when your organization faces threats and how to keep them at bay.
- **Collaborative.** SecOptimal means that all security and privacy data that comes into your enterprise or that's created there could be shared and used as needed, with no barriers except the ones you set up.

  Today, inaccessible data can be a huge impediment to holistic enterprise security and data privacy. Applications used throughout your organization likely contain their own valuable data about who's trying to get in, but your legacy SIEM can't take it in.

  Using a single platform lets all that data flow as one, with technical barriers removed. Security analysts can use it to stitch together a comprehensive picture of an evolving threat.
- **Cost effective.** Many traditional SIEMs don't have their own low-cost cloud, so your organization may pay increasingly more to use a vendor's services. You may also pay an added price for each new SIEM log source.

  At some point, you should make tradeoffs. In the SecOps of the future, you pay for features, not according to how much data you collect or process, or where it comes from.

Questions for the C-Suite to consider

Key questions each respective group across leadership will want to focus on as they get a better understanding of SecOps platform transformation.

CISO

1. **Do I have the right people to make this project succeed?** CISOs often lack the right people needed to do security the right way. Their staff get tied up with today's priority tasks while more strategic operations go unresolved, and budgets don't keep pace with the needs.

   Instead of economies of scale, it's time to shift your mindset to one of "economies of learning," to apply brain power instead of ever-increasing person power. Rather than searching endlessly for security issues that you already know exist – an approach that can leave your teams blindsided when new problems occur – why not use a connected SecOps platform with AI to predict events, share information with other teams, and resolve threats in advance?

1. **Are we using the appropriate level of automation?** Automating high-volume, low-risk tasks can free your security staff to focus on big problems. This is the collaboration of the future: AI analyzing mass quantities of data in the blink of a virtual eye, providing your team with recommendations on how to write detection logic to alert against emerging threats, and responding to identified threats in an efficient manner.
2. **Can I justify the expense?** CISOs face increasing pressure to hold the line on costs and do more with less. But not exploring how to automate more of your processes will only increase the risks – and costs – to your organization as bad actors use AI to find ways into your systems. Using AI and other automation solutions can help you do more – analyze data, detect threats, respond to security events - with your existing funds.

CRO

1. **How can this help us see enterprise risks all together and work together as an organization to manage them?** A SecOps platform that incorporates threat hunting could help identify new risks to your organization by coordinating and communicating with your technologies and using AI to seek out threats. It might also help you make more effective enterprise risk management decisions.
2. **How can this inform and improve my risk reporting?** Having access to more data can give you the documentation you need to make the case for risk response actions to the C-suite and board. AI features might help you quantify those risks so you can better prioritize them and enlist the support of the CEO, CFO and board in your initiatives to manage them.
3. **Does our company's existing level of risk support another technology transformation?** Adding AI to your business processes will certainly require sweeping change throughout the enterprise. And as new technologies, processes, and business models take hold, new transformations will certainly follow. Not keeping pace with threat actors that will unabashedly use AI presents its own set of risks. You should have flexibility to manage the overall risks amid rapid change.

CIO/CTO

1. **How can a SecOps transformation help our security teams innovate ways to better protect the organization from cyberattacks?** By leveraging platforms that can help to reduce the mundane tasks your talented security staff is focused on, allowing for more creativity to think ahead of where/how the next threat may emerge.
2. **How can this help us work faster and bring new products to the marketplace more rapidly and competitively?** Using an advanced platform that can scale and has an ease of ingesting information from a variety of sources can allow your organization to feel more confident that security can keep up with the pace of your changing environment.
3. **Is this platform the one that works better for your company and technologies?** Leveraging a centralized platform that integrates well with your business analytics strategy may enable the broader business to gain insights that they may not have had access to in the past.

CEO

1. **How can I put in place security technologies that aren't only a fix for now but scalable for the future?** The task of pivoting to new security technologies and advances is a constant priority, especially to keep up with technology innovation. Incorporating new technologies and capabilities becomes much easier when it's a matter of merely switching out a feature or installing a software update.
2. **Are we all working on this transformation together?** Leadership should work together to prevent and respond to attacks as a collective front. Having a single platform is an effective way to achieve the "big-picture view" you need – as well as for others to be able to use data for their discrete needs. Everyone can work together more easily and effectively toward the same goal: reducing risk.
3. **How can I enlist the board's support for this change?** SecOps transformation on the heels of, or concurrent with, overall digital transformation may risk "transformation fatigue" on your board's part. The CISO may be the one making the pitch to them but you may need to show your support. Aspects you might address include the cost-efficiency of moving to a platform, the ability to make better use of enterprise data by sharing access throughout the company, and the need for the C-suite and board to pull together for success.

Board

1. **How can this improve security? Can it improve network visibility?** New regulations regarding disclosure of certain cybersecurity events puts more onus on board members to be cyber-savvy. Understanding how a SecOps transformation can affect the organization's security overall can help the board better govern the change.
2. **How can the ability to share enterprise data affect data security? How can we satisfy regulators that it won't violate data privacy laws?** Data privacy and security have become overriding themes as regulators worldwide step up their demands on organizations to gain consent from data owners to use their information, and to know exactly where that data goes from the moment it's collected. A unified platform can make tracking that data much easier.
3. **How can this help the company achieve its objectives?** With costs leading the conversation in this environment, using AI to automate low-level tasks that are time sinks and leveraging generated suggestions from AI-enhanced security platforms may offer tangible ROI on some of the transformation costs.

Getting to SecOptimal with Google and PwC

You can't protect what you can't see. However, if your SecOps program is like many others, you're only seeing about 30 to 40 percent of your networks and activities.

Cost is often a big reason for this lack of visibility. Your SIEM may be able to handle a lot more information than it's taking in today, but buying the programs and licenses to make that happen may be prohibitively expensive. The typical SecOps program uses between 50 and 100 technologies.

The Google Cybersecurity Alliance — PwC and Google — work in tandem to help propel our clients' SecOps programs into the future. We've helped clients double their visibility using **Google Chronicle – a unified platform to achieve and maintain SecOptimal cyber programs.**

Using Gemini AI-enabled automation and analytics, Google Cloud storage capacity, Mandiant Threat Intelligence, and PwC's knowledge and experience in the cyber realm, our clients are achieving growth at an affordable, predictable cost.

Google Chronicle's technologies and services include:

- **Chronicle SIEM and SOAR:** This next-generation **SIEM** takes in and processes unlimited data automatically from a plethora of sources, communicates with our **SOAR** for rapid remediation, allows external access to its data in accordance with your needs, and more.
- **AI:** Google has a long and storied history with AI, having started, in 2017, the open-source project that kicked off the AI revolution. Years and billions of dollars have gone into research to develop and perfect the **Gemini AI** models. PwC and Chronicle can put them to work for you.

- **Threat hunting:** The world's largest search engine already has access to a huge percent of the traffic happening online day and night. Adding in the Chrome browser, Gmail, and other popular Google services gives our threat detection services a sweeping, holistic scope that no other security provider can touch.

  Security-first features give Google unique access to threat intelligence. Chrome's Safe Browsing, which detects malicious downloads using Chrome, shows where those downloads originate. Monitoring Gmail for phishing attempts and attacks provide even more valuable information about who's attacking, where, and how.

  The Chronicle platform also integrates with **VirusTotal**, the world's premier database for indicators of attack and compromise. VirusTotal collects data from every security vendor on the market, so Google knows which files, domains, and techniques cyber attackers are using from moment to moment.

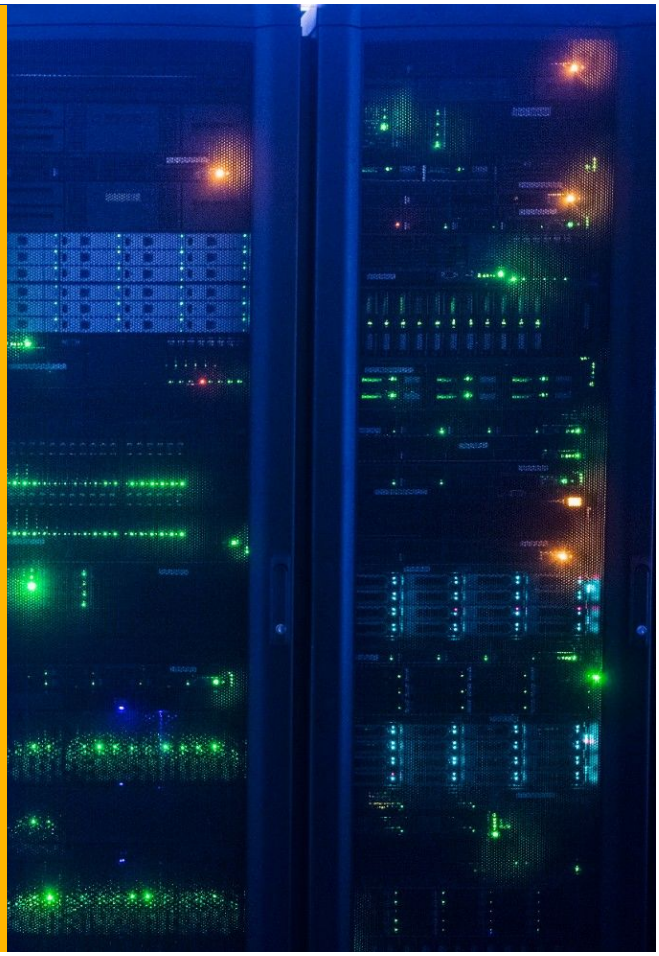
  Meanwhile, **Mandiant Threat Intelligence** uses hundreds of security researchers to analyze 24/7 what threat actors are doing, why, and how; where they're located; what tactics and solutions they use, and more. Mandiant's teams watch over Chronicle customers like guardian angels to tell you when threats loom and how to respond, so attackers never even get close to breaking in.

- **Storage:** The Chronicle platform includes access to **Google Cloud** so you can store as much data as you want for as long as a year, and its packages come at an affordable price with no surprises. SOAR, SIEM, security applications, threat hunting, AI – it's all there, on one platform with many features at a single affordable price. You won't have to trade security for cost-savings: with Chronicle you get both, every time and all the time.

And PwC configuration and support can help confirm that your new SecOps platform works exactly as you need, to:

- Rapidly process and analyze your company's data to inform decisions, not just that flowing into the SIEM;
- Alert you to potential threats as they appear and even beforehand for rapid response and proactive defense;
- Store raw data for later analysis as well as to provide evidence of compliance;
- Allow others in the organization to use the data with their solution of choice;
- Scale effortlessly and without limits as technologies and their data proliferate;
- Manage critical security applications on a single platform so that all work together;
- Free your teams from mundane "toil" so they can focus on essential security tasks;
- Work within your budget, with no surprises;
- And much more.

Contact us to learn more about how PwC and Google can help take you to SecOptimal with Chronicle, one of the most advanced security platforms on the market.



Authors:

Matt Wilden
Principal,
Google Cybersecurity Alliance Leader, PwC US
matt.wilden@pwc.com

Jeff Vierzba
Managing Director,
Cybersecurity, Privacy & Forensics, PwC US
jeff.jvierzba@pwc.com