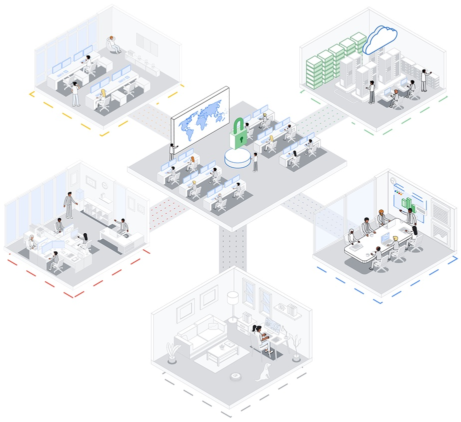
Google Cloud

The Security Operations Ecosystem



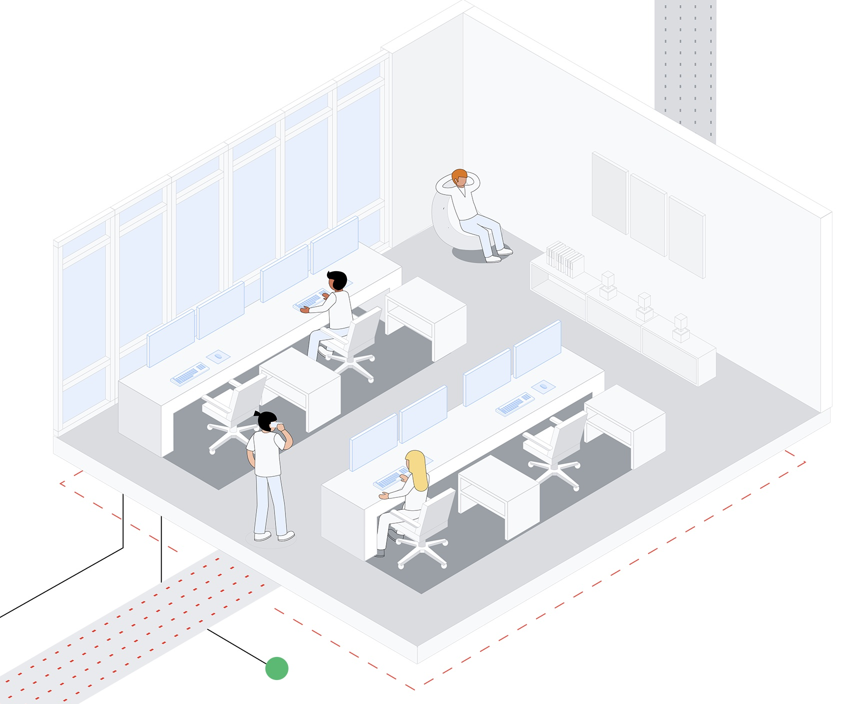
5 distinct business groups with whom today’s SOC is interacting

With security firmly entrenched as a boardroom imperative and the adversary landscape expanding in the era of remote work, digital transformation, and supply chain disruptions, the SOC is changing. It can no longer exclusively exist as the siloed, mission control-style room most known for its aesthetic of fancy monitors, flashy displays and dim lighting. Here is how the SOC is shedding its solitary reputation, blurring boundaries and building bridges with five different teams to build vibrant, mutually beneficial partnerships and improve outcomes for all.

01

Software Development and Engineering

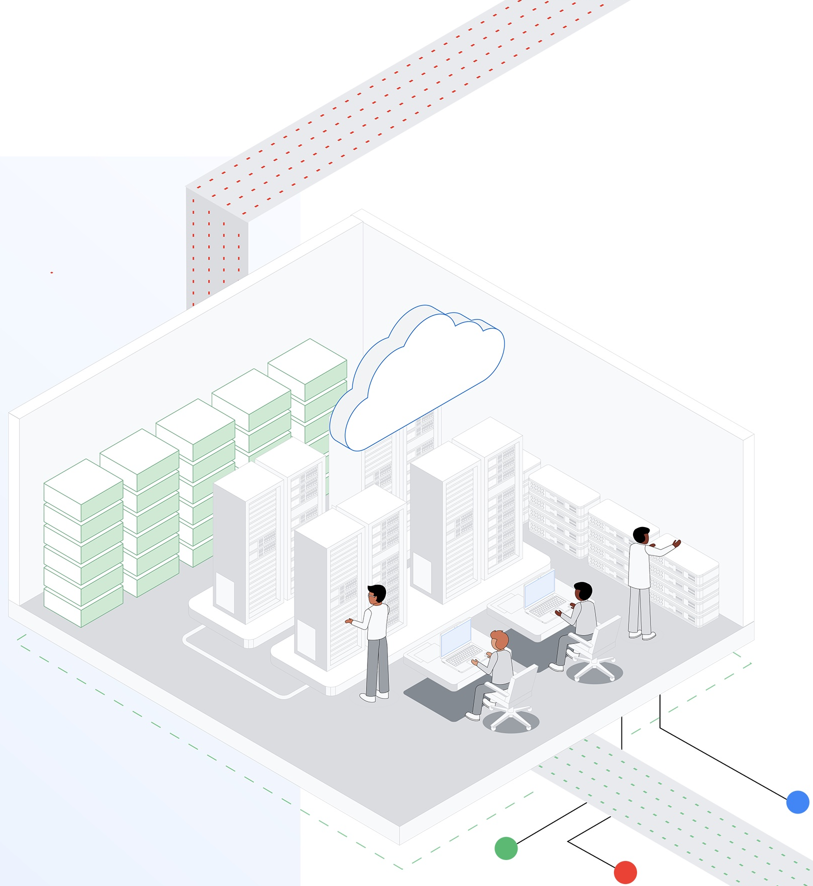
Cloud migration is enabling businesses to scale and thrive. But it's also yielding overwhelming numbers of alerts that are contributing to the chronic malady of alert fatigue. One way the SOC is responding to this challenge, beyond automated technologies like SIEM and SOAR which allow it to capture alerts, apply context, and deploy repeatable playbooks, is taking a page out of the DevOps and software engineering field manual to help improve resiliency and strong detection engineering. Forward-thinking SOCs, for example, may assign certain analysts to a site reliability engineering (SRE)-style team that divides its time between security operations and actually developing new capabilities through process automation development.



60% of IT pros receive over 500 cloud security alerts per day, which is causing 55% of their organizations to miss critical alerts.

02

IT and Network Operations



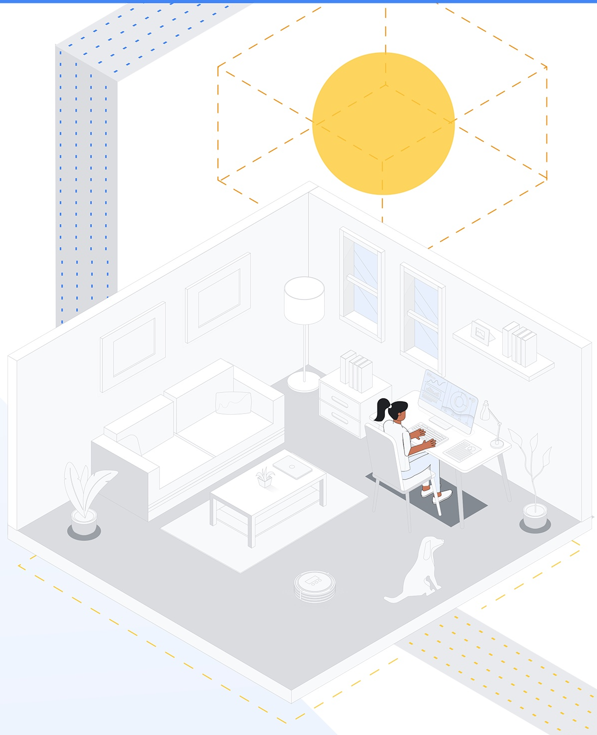
Long considered the primary drivers and enablers of digital innovation in the workplace, the IT and network operations teams have a new ally: the SOC. Because as the saying goes: You can't secure what you can't see (or know exists). When groups stand up new systems, they likely don't consider security and that controls like configurations and permissions are important, especially if mission-critical data is involved. SOC teams assist with helping to extend good hygiene–and gain an added benefit: By being involved in the process, they can build more effective detection rules and capabilities for these new technologies being stood up.

03

The C-Suite

Security teams and executives often only cross paths during times of emergency or high-profile attacks drawing headlines. Tools exist to streamline crisis communication during a major incident, but it's also important to establish proactive relationships that help impart consistent awareness about the SOC's duties and accomplishments, and champion for C-level buy-in. The best way SOC teams are achieving this is by dispensing relatable metrics and avoiding technospeak.

85% of enterprises budgeted more for security operations during the pandemic, 72% have increased their staffing and 79% have increased their adoption of advanced security technologies.



04

Everyday Employees

Virtually every SOC has received, for lack of a better word, unusual requests from other teams or departments related to data and system access. The immediate instinct likely is to say "no," especially if an alert is initiated. Unfortunately this usually gives rise to shadow IT. A more progressive approach is to position the SOC not as a roadblock but as an enabler by offering constructive (and friendly) security feedback and being seen a trusted adviser and problem solver that adds value to the organization by partnering with other teams to help them achieve what they need while also acting as the safety net to mitigate overall enterprise risk.

05

Managed Security Providers

Here's an uncomfortable truth: Virtually all SOCs will never be able to hire enough talent. This likely means that almost every SOC, if they aren't already, will follow a hybrid model that works together with service providers—be it an MDR (managed detection and response), co-managed SIEM, managed EDR, or a full-on MSSP. Not only does offloading things like 24x7 monitoring allow a resource-starved SOC to cover existing blind spots and compensate for incomplete skills, it also gets freed up to assign its in-house analysts to more inspiring–and distinctly human–tasks like threat hunting. It's important for SOCs to have the internal competency to engage with providers as well, both participate in mutual decision making and determine if the provider is able to meet their overall needs and demands.

52% of businesses have increased their use of an MSSP since the pandemic began.

As you can see, modern security operations is now a cross-collaborative, culture-minded and often distributed entity that has been reborn, continuously growing and permeating its influence beyond a single central location and across the greater organization. The future thus looks bright for the SOC, beyond the rows of glowing monitors and busy alert screens.

Chronicle

For help modernizing your security operations at the speed and scale of Google, visit chronicle.security today.

Sources: Orca Security, "2022 Cloud Security Alert Fatigue Report," May 2022; CyberRes/Micro Focus, "2021 State of Security Operations Report," August 2021; Siemplify, "The State of Remote Security Operations Report," February 2021