CLOUDFIT SOFTWARE

THE RISK OF POOR INVESTMENT:

The Necessity of an Effective Security Operations Center

WE WON’T DWELL TOO LONG ON THIS TOPIC.

We won’t dwell too long on this topic. If you’re reading this, you’re already well aware of the rising tide of cyber threats and the growing risks they pose to businesses. However, for the sake of clarity, let’s establish the undeniable reality with some of the latest cybersecurity statistics from 2024.

Cyber Threat Impact: By The Numbers.

$13.82 Trillion

The estimated global financial impact of cybercrime by 2028.[1]

600 Million

The number of daily attacks on Microsoft customers alone.[2]

+4,151% Increase

The surge in phishing attacks since the public debut of ChatGPT in 2022, as attackers leverage AI to craft more sophisticated lures.[3]

$4.88 Million

Global average cost of a data breach (per breach, per company) in 2024.[4]

[1] Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities [2] Microsoft Digital Defense Report 2024 [3] Phishing in 2024: 4,151% Increase Since Launch of ChatGPT; AI Mitigation Methods [4] Cost of a Data Breach Report 2024

The cost of failing to invest in an effective SOC is not just measured in dollars, organizations should also consider factors like lost customer/ client trust, regulatory fines, and operational downtime.

With threat actors growing more advanced and AI-driven attacks becoming the norm, business leaders can no longer afford a reactive security approach.

Many organizations still view SOCs as an optional investment rather than a critical necessity. The reality is that no industry is immune; threat actors do not discriminate based on company size, sector, or even security maturity. Cybersecurity is no longer a compliance checkbox; it is a business survival requirement.

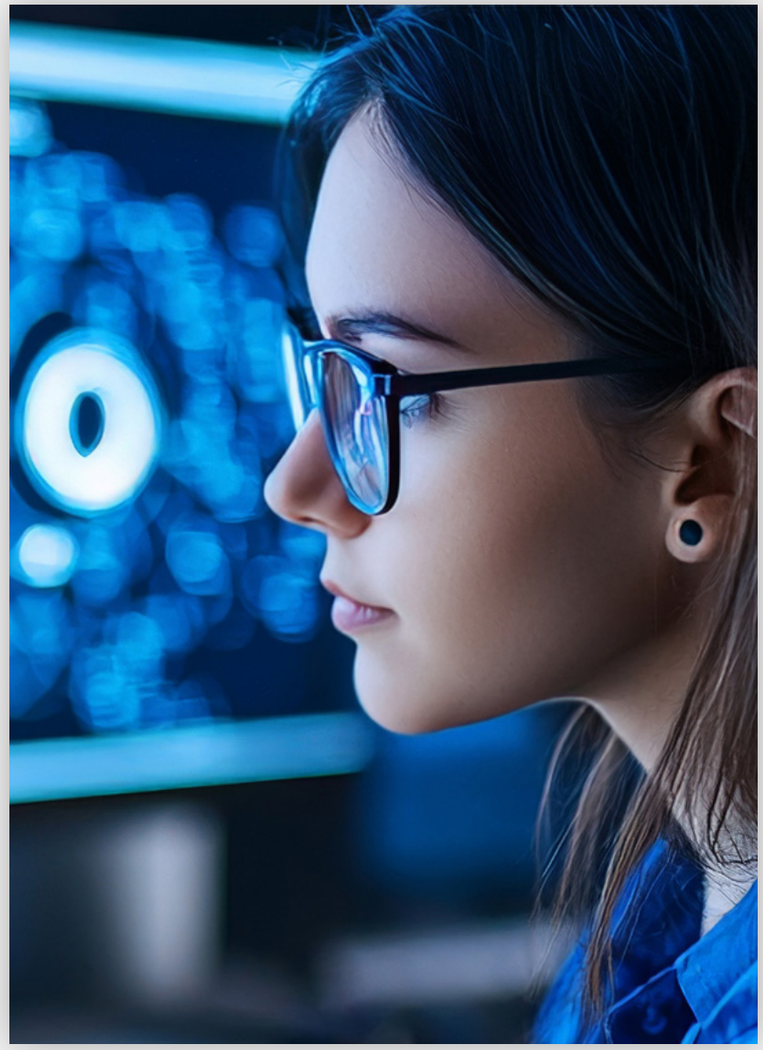
For organizations that lack the in-house resources to build a 24/7 security operations team, outsourcing to a managed security services provider (MSSP) has become the most efficient path to enterprise-grade security. Whether your SOC is in-house or outsourced, one thing remains certain: not having one is no longer an option.

Even for companies that can, could or do afford their own SOC, there are pros and cons to doing it in-house vs finding the right, trusted service provider:

- **In-house pros include loyalty, sole focus on your company**

- **In-house cons include limited experience due to sole focus on your company, higher probability that new technology, cost savings, ability to scale, etc aren't applied as rapidly**

We will dive deeper into various challenges, opportunities and strategies below.



COMMONLY ENCOUNTERED STATES OF SECURITY

We've observed that organizations fall into distinct categories when it comes to their security posture, each with unique challenges and needs. Understanding where your organization stands can help define the next steps toward building an effective SOC.

Going from Zero to Full Throttle: The Reactive Approach

These organizations have historically underinvested in cybersecurity, often viewing it as a compliance necessity rather than a core business function. They have basic technical controls in place—such as multi-factor authentication (MFA), firewall rules, limited access controls, and email filtering policies, but lack an operational SIEM or SOAR platform.

As a result, they are functionally blind to security threats in the preventative stages, relying on reactive measures rather than proactive detection and response. Investment in security is often triggered by external pressures, such as:

- **A recent security breach that exposed vulnerabilities.**
- **Regulatory requirements mandating stronger detection and response capabilities.**
- **Customer or partner demands compliance assurance.**

For these organizations, the challenge is building foundational security operations that shift from reactive firefighting to a proactive defense strategy. Proactive defense allows you to identify vulnerabilities/risk factors before they get exploited whereas reactive means that the breach has already occurred, and the damage is done.

Dedicated Security Staff: Growth Creates Complexity

Organizations in this category have at least one or more dedicated security professionals responsible for maintaining and improving the company's cybersecurity posture. These are typically mature enterprises that have expanded in size and complexity, leading to:

- **Increased strain on security teams to manage and enforce policies across a growing IT environment.**
- **Challenges scaling security operations, particularly with incident detection and response.**
- **The need for automation and security operations maturity to reduce analyst fatigue and maintain effective security operations.**

For these companies, the next step is optimizing and scaling their SOC capabilities, ensuring they stay ahead of evolving threats without overburdening their security team. In a recent research article published on ACM Computing surveys, multiple sources were cited in the report indicating high levels of alert fatigue being felt by SOC teams. Upwards of 60% of SOC engineers interviewed reported experiencing alert fatigue and burnout.[1]

[1] Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities

Split-Responsibility Security Staff: Wearing Too Many Hats

This scenario is common in small to mid-sized organizations, where a handful of highly skilled engineers juggle multiple responsibilities across IT, security, and business operations.

These include:

- **Security operations and compliance.**
- **Help desk support.**
- **Network and infrastructure maintenance.**

While this approach provides flexibility, it creates significant risks:

- **Limited bandwidth for proactive security monitoring.**
- **Increased likelihood of overlooked incidents.**
- **Higher risk exposure due to stretched resources.**

For these organizations, outsourcing critical SOC functions is the best path forward, as even experienced resources can have issues with properly scaling SOC functionality while keeping the bandwidth needed for their other responsibilities. Outsourcing critical SOC functions may enable a team to extend security coverage without disrupting other business operations.

Where Does Your Organization Stand?

Regardless of which category an organization falls into, the common thread is a growing need for stronger security operations. A lack of visibility and dedicated resources increases risk, while scaling security without the right tools and expertise can lead to operational burnout.

Investing in a modern SOC whether in-house or through an MSSP ensures organizations stay ahead of threats, achieve compliance, and improve overall resilience.

CHALLENGES FOR SOC TEAMS

For many organizations, security wasn't a foundational priority at the outset—whether due to the evolving nature of the DevSecOps movement or a lack of regulatory pressure at the time. As a result, it's completely understandable to now find yourself in a position of needing to catch up.

More often than not, businesses are forced into security transformation in response to a compromise, regulatory pressure, or the need to meet cybersecurity requirements for new market opportunities.

Regardless of the driver, this shift is rarely simple.

Security doesn't exist in isolation—it touches every function, tool, and technology within an organization. Depending on where your business falls within the Commonly Encountered States of Security, the challenges associated with building or maturing your SOC can range from manageable to overwhelming.

For companies going from reactive to **proactive security,** the challenge is building visibility and operationalizing security from the ground up—often in response to a crisis.

Those with **dedicated security staff** struggle with scaling SOC operations efficiently as the volume of security events outpaces existing capabilities.

And for organizations with **split-responsibility security staff,** security is an ongoing battle for attention, that must compete with day-to-day IT operations and business-critical functions.

Regardless of what state their security programs fall under; SOC teams often encounter the following challenges:

Challenge 1: Juggling Unplanned and Planned Work

Unplanned work is a major productivity disrupter. It interrupts workflows, derails strategic initiatives, and exhausts valuable resources. Security operations, by their very nature, are filled with unplanned work.

SOC teams must respond to incidents in real time. Detection, investigation, and containment efforts often override planned projects and long-term security improvements.

This creates a perpetual struggle:

- **How do you balance immediate security concerns with the need to develop long-term security resilience?**
- **How do you maintain efficiency when unplanned work constantly disrupts structured workflows?**
- **How do you prevent burnout in a team overwhelmed with alerts and incidents?**

Challenge 2: Finding Stability Amid the Chaos

Security operations will always be a balance of planned and unplanned work, but organizations that mature their SOC structure gain the ability to respond efficiently rather than react chaotically.

For companies that are currently in a **reactive state of security,** this means establishing a security foundation with proper logging, alerting, and response capabilities. For those with **dedicated security staff,** it's about investing in automation and scaling security efforts to match the growing attack surface. And for businesses with **split-responsibility security staff,** outsourcing key SOC functions can provide the stability needed to keep security incidents from derailing operations

Ultimately, no organization can eliminate the unpredictable nature of cybersecurity, but by refining their SOC strategy, they can transform security from a constant burden into a controlled and efficient operation.

Challenge 3: Militant Prioritization and Incident Overload

For organizations that operate a SOC—whether internal or outsourced—incident overload is one of the most pervasive challenges. The sheer volume of alerts, false positives, and noise from security tools can create an environment where teams feel like they are constantly bailing water out of a sinking boat.

Without a structured approach to prioritization and automation, SOC teams risk:

- **Alert fatigue, where analysts become desensitized to high-volume, low-value alerts.**
- **Delayed responses, leading to prolonged dwell time and increased risk exposure.**
- **Missed critical threats, as severe incidents get buried in the noise.**

Effective SOC operations require a strategy of militant prioritization—focusing effort where it matters most.

This means:

- **Automating repetitive security tasks to free up analyst time.**
- **Implementing clear escalation and triage processes to prevent distractions from low-impact alerts.**
- **Leveraging SIEM and SOAR platforms effectively to streamline response workflows.**

SYSTEMS FOR SUCCESS:

KEYS TO A SUCCESSFUL SOC

The keys to success in security operations are simple but not easy. Like building muscle, breaking bad habits, or mastering a new skill, the results you achieve are dependent on the quality of the systems you put in place.

A mature and high-functioning SOC doesn't happen overnight—it is built through the accumulation of small, repeatable, and scalable systems.

However, these systems are not static. The environment in which your SOC operates is constantly evolving with new customers, emerging technologies, evolving exploits, shifting attack methodologies, personnel transitions, and infrastructure changes. As the landscape evolves, it will inevitably stress or even break whatever system you have in place today. Success is not just about implementing effective systems, organizations must also continuously scrutinize, evolve, and adapt existing systems to maintain resilience.

The key to sustainable SOC success is to keep systems simple and modular, allowing for easy modification and iteration. Just as a software engineer follows continuous integration and continuous delivery (CI/CD) principles to push small, testable code changes, a SOC should design its operational systems in small, adaptable increments that can be tested, validated, and improved with minimal friction.

The Three Pillars of SOC Systems

To build a scalable and resilient SOC, we categorize our systems into three groups:

Behavioral Systems:

The habits and mindsets that define how your team thinks, acts, and communicates. These are the "tribal" aspects of a team.

Administrative Systems:

The policies and documentation that standardize security operations.

Technical Systems:

The tools, processes, and automation that optimize security workflows.

Behavioral Systems – The Foundation of a High-Performing SOC

These are the core mental frameworks that shape how your SOC team—and your organization—thinks about security. While technology is essential, security is ultimately a people-driven discipline.

ENGINEERING THE SECURITY STATE OF MIND

Your SOC team isn't just responsible for protecting your organization—it should influence the security culture across every department. Security must be everyone's responsibility, from interns to executives. A well-trained and security-conscious workforce reduces attack surfaces and mitigates human errors before they become security incidents. Social engineering remains one of the most effective tactics used by threat actors to breach organizations—often exploiting human behavior rather than technical vulnerabilities. In fact, a report published by the Cybersecurity and Infrastructure Security Agency (CISA) found that "more than 90% of successful cyber-attacks start with a phishing email".[1]

Training, conditioning, and rewarding your staff to recognize and report phishing attempts is not just beneficial—it's essential to building a resilient organizational security posture.

[1] Shields Up: Guidance for Families

The Three Pillars of SOC Systems

To build a scalable and resilient SOC, we categorize our systems into three groups:

Behavioral Systems:

The habits and mindsets that define how your team thinks, acts, and communicates. These are the "tribal" aspects of a team.

Administrative Systems:

The policies and documentation that standardize security operations.

Technical Systems:

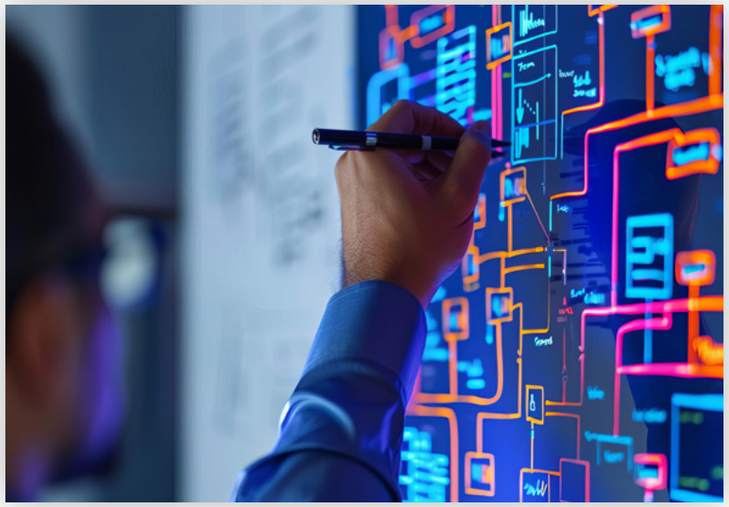
The tools, processes, and automation that optimize security workflows.

LEAVE YOUR ASSUMPTIONS AT THE DOOR

Making assumptions is a first-class ticket to compromise. Your SOC cannot afford to assume that:

- **A system is configured securely by default.**
- **A user's behavior is benign without validation.**
- **An alert is a false positive without investigation.**

This is why rigorous validation, structured triage processes, and an evidence-based approach are critical to preventing security blind spots.



DERIVING PLANNED WORK FROM UNPLANNED WORK

Security incidents are inherently unplanned—they disrupt workflows, override priorities, and demand immediate attention. However, the most successful SOC teams transform unplanned incidents into structured, actionable improvements.

- **Every incident review should identify gaps in detection, documentation, or automation.**
- **As incidents occur over time, security teams can use those experiences to repeatedly test and refine their guides. As security playbooks mature, response efficiency and accuracy improve.**
- **If a Security Incident Handling Guide (SIHG) or Technical Support Guide (TSG) does not exist for an event, create one.**

The Three Pillars of SOC Systems

To build a scalable and resilient SOC, we categorize our systems into three groups:

Behavioral Systems:

The habits and mindsets that define how your team thinks, acts, and communicates. These are the “tribal” aspects of a team.

Administrative Systems:

The policies and documentation that standardize security operations.

Technical Systems:

The tools, processes, and automation that optimize security workflows.

FRIENDLY FAILURES: ASSUME BREACH

False escalations and procedural failures are inevitable—but missing a true positive is unacceptable.

Unlike criminal justice, where the standard is “innocent until proven guilty,” your SOC should operate under the assumption of breach. Every security incident should be treated as guilty until proven innocent to minimize the risk of a real attack slipping through the cracks.

In the early stages of implementation, this mindset shift may result in false escalations, but these should be viewed as learning opportunities rather than failures. Organizations must prepare stakeholders for the operational disruptions that come with a Zero-Trust approach to incident response.

The Three Pillars of SOC Systems

To build a scalable and resilient SOC, we categorize our systems into three groups:

Behavioral Systems:

The habits and mindsets that define how your team thinks, acts, and communicates. These are the “tribal” aspects of a team.

Administrative Systems:

The policies and documentation that standardize security operations.

Technical Systems:

The tools, processes, and automation that optimize security workflows.

Administrative Systems – Operationalizing Security

Administrative systems create standardization and consistency across your SOC operations. These systems ensure that investigations, escalations, and remediation efforts are efficient, repeatable, and well-documented.

TECHNICAL WRITING: SECURITY INCIDENT HANDLING GUIDES (SIHGS) AND TECHNICAL SUPPORT GUIDES (TSGS)

A well-documented SIHG or TSG should leave no room for ambiguity.

- **SIHGs help organize the investigation procedures and actions into a logical topography to enable each member of your SOC team to perform high quality and consistent investigations.**
- **Guides should be written under the assumption that the reader has zero prior knowledge of the procedure.**
- **Documentation should be structured, step-by-step, and actionable.**
- **Security teams should prioritize clear, repeatable processes that minimize errors and training time for new analysts.**

The Three Pillars of SOC Systems

To build a scalable and resilient SOC, we categorize our systems into three groups:

Behavioral Systems:

The habits and mindsets that define how your team thinks, acts, and communicates. These are the "tribal" aspects of a team.

Administrative Systems:

The policies and documentation that standardize security operations.

Technical Systems:

The tools, processes, and automation that optimize security workflows.

PROTOCOLS: FEEDBACK LOOPS AND STAKEHOLDER COMMUNICATION

If your SOC team falsely escalates an incident to a stakeholder at 4 AM on a weekend, frustration is an expected response. False escalations will happen—but how they are handled defines your SOC's credibility.

To maintain stakeholder confidence and team morale, each false escalation should:

- **Trigger an internal review to identify why the escalation occurred.**
- **Improve procedural documentation, such as refining escalation protocols, updating SIHGs, or whitelisting known entities to reduce false positives.**
- **Close the feedback loop with the affected stakeholders, explaining what was learned and what changes were made.**

A SOC team's ability to demonstrate responsiveness and continuous improvement in handling false positives is critical to stakeholder trust.

The Three Pillars of SOC Systems

To build a scalable and resilient SOC, we categorize our systems into three groups:

Behavioral Systems:

The habits and mindsets that define how your team thinks, acts, and communicates. These are the “tribal” aspects of a team.

Administrative Systems:

The policies and documentation that standardize security operations.

Technical Systems:

The tools, processes, and automation that optimize security workflows.

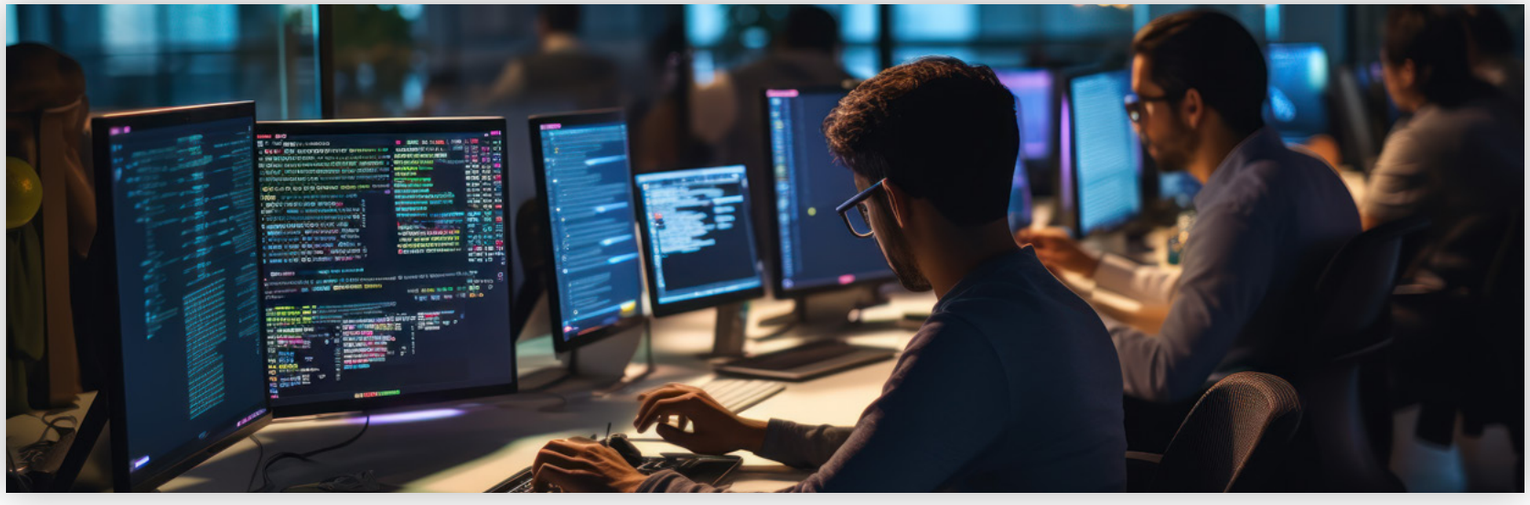
Technical Systems – Tools and Automation

Technical systems ensure scalability, efficiency, and accuracy in security operations. Without the right automation, even the most well-trained SOC team can be overwhelmed.

DETECTION ENGINEERING AND SIEM OPTIMIZATION

Strong detection engineering forms the backbone of any mature SOC.

- **Fine-tune detection rules to reduce noise while maintaining high coverage.**
- **Leverage automation in SOAR platforms to enrich alerts and reduce manual workload.**
- **Continuously test and validate detections by correlating them with real-world attack techniques.**



The Three Pillars of SOC Systems

To build a scalable and resilient SOC, we categorize our systems into three groups:

Behavioral Systems:

The habits and mindsets that define how your team thinks, acts, and communicates. These are the “tribal” aspects of a team.

Administrative Systems:

The policies and documentation that standardize security operations.

Technical Systems:

The tools, processes, and automation that optimize security workflows.

ADAPTIVE SECURITY CONTROLS

To stay ahead of threats, SOCs must move beyond passive alerting and adopt automated defensive actions.

- **Implement automated containment mechanisms for high-confidence alerts.**
- **Ensure incident response playbooks are updated as new threats emerge.**
- **Use threat intelligence feeds to enhance detection logic in real time.**

CONTINUOUS TESTING AND RED TEAMING

No system is complete without validation. Continuous testing ensures that your SOC’s defenses are effective under real pressure.

- **Run controlled attack simulations to validate detection and response effectiveness.**
- **Test escalation pathways to ensure incidents are routed to the correct stakeholders.**
- **Conduct tabletop exercises to refine SOC readiness.**

Technical systems aren’t just about the tools you choose—they’re about how well those tools are integrated, automated, and validated. A mature SOC doesn’t rely on guesswork. It relies on tested, adaptable systems that evolve with the threat landscape

CONCLUSION:

BUILDING A RESILIENT SOC IS AN ITERATIVE PROCESS

Security is no longer a luxury or a compliance checkbox—it's a continuous, operational necessity. For organizations striving to build or mature their SOC, it doesn't happen overnight.

The challenges are real: balancing unplanned work with strategic progress, drowning in alert fatigue, and navigating the complexities of security in a fast-evolving landscape. These struggles aren't signs of failure—they're signals that your systems need to adapt.

Through our journey growing CloudFit's SOC and running SOCs for our customers, we've learned that success doesn't come from a single tool, a superstar hire, or a one-size-fits-all solution. It comes from building behavioral, administrative, and technical systems that are designed to evolve. It comes from embracing failure as a catalyst for improvement. And it comes from instilling a mindset where planned work is born from unplanned chaos.

The capabilities of CloudFit's SOC also comes from having opportunities to run SOC (and other Managed Services) for hundreds of customers across millions of devices across all sectors and verticals including Defense, Federal, State and Local, Law Enforcement, Intel, Energy, Nuclear, Financial, Healthcare, Manufacturing, Construction, Cloud Providers and Independent Software Vendors. We have the benefit of scale: both breadth (lots of customers and lots of regulated verticals) and depth (customers ranging from five users to well over a millions users).

The most resilient SOCs are not the ones that prevent every breach—but the ones that are prepared to respond rapidly, recover intelligently, and continuously improve. Whether you're just starting your security transformation or refining an established operation, the systems you build today will define your security posture tomorrow.

Start small. Build smart. Iterate often. And most importantly—assume breach, learn fast, and lead with discipline. That's how modern organizations stay secure in a world that never stops changing.

Resilient security operations aren't built overnight—they're engineered through small, deliberate improvements that adapt with your organization's growth and challenges. Whether you're starting from scratch or fine-tuning an existing security program, CloudFit is here to help you design systems that scale, respond, and improve over time.

CONTACT US

LET'S TALK ABOUT WHAT'S NEXT FOR YOUR SOC.

CONTACT US →

| getfit@cloudfitsoftware.com

ABOUT US →

| cloudfitsoftware.com/aboutus

CLOUDFIT SOFTWARE