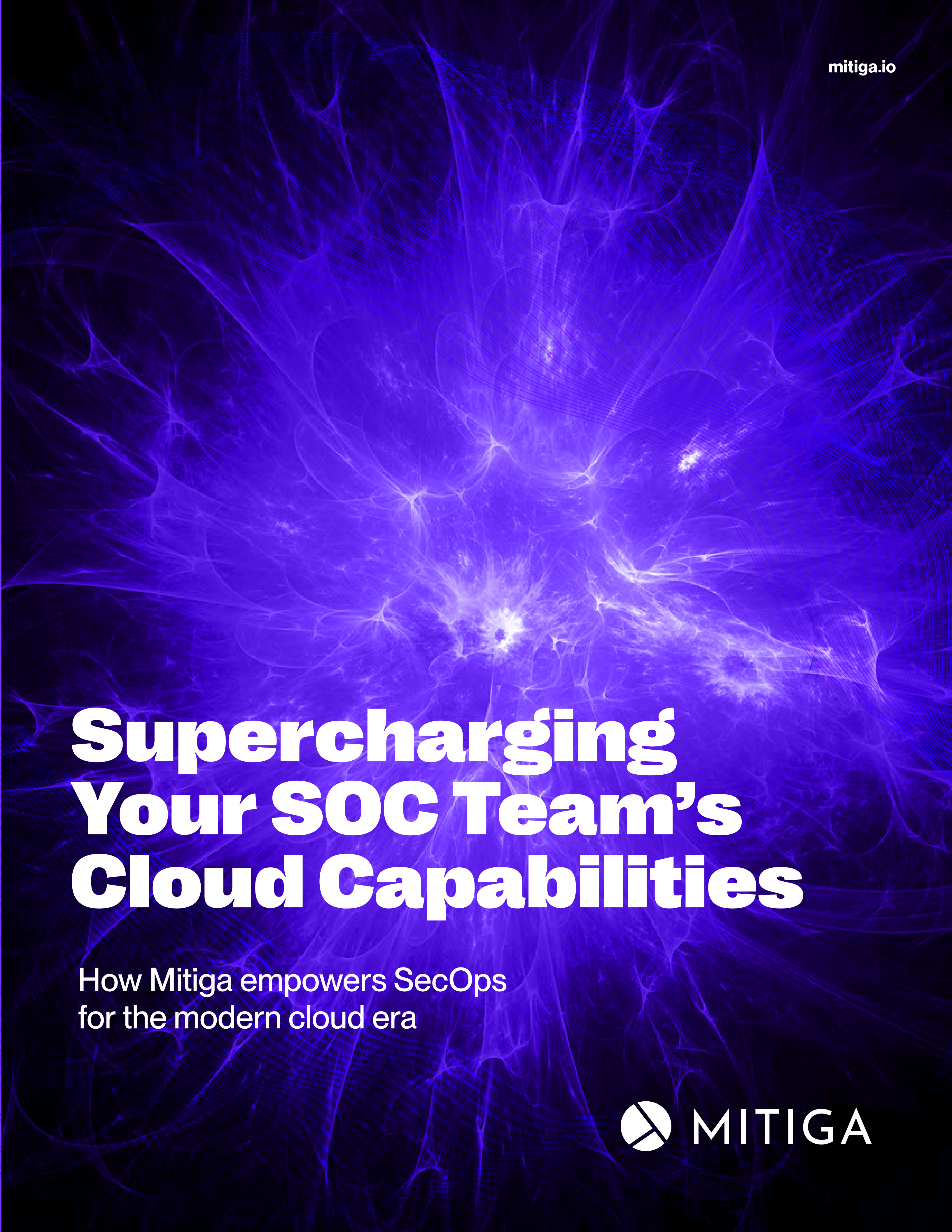
mitiga.io



Supercharging Your SOC Team's Cloud Capabilities

How Mitiga empowers SecOps
for the modern cloud era

MITIGA

Contents

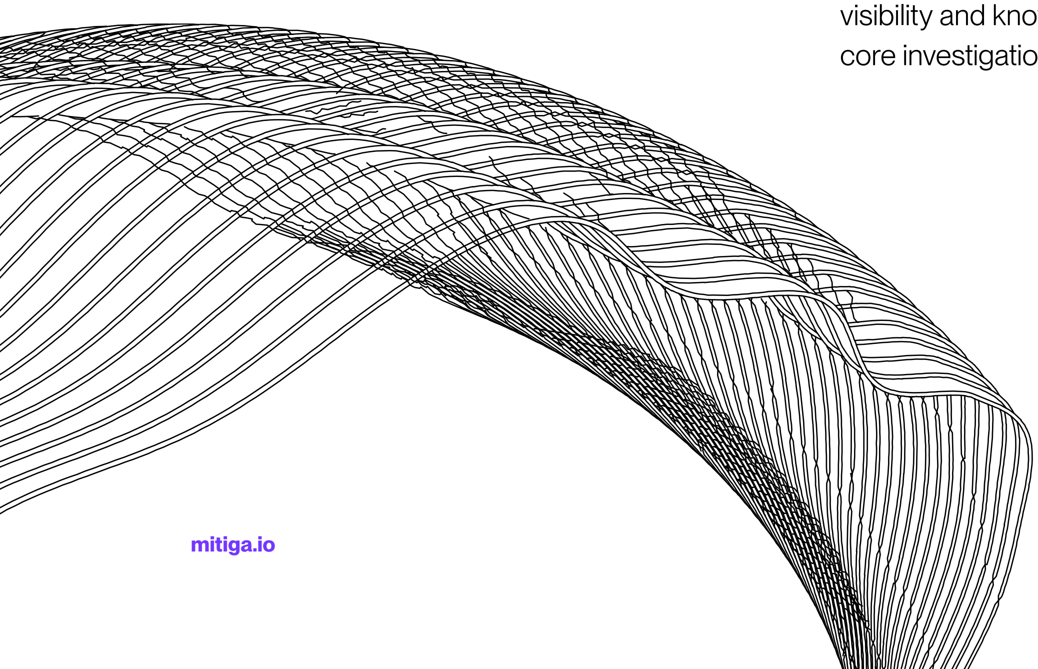
Security Operations Centers (SOCs) have long been at the bedrock of enterprise security, with teams of analysts who are relied on day in and day out to maintain the security of core business operations. It's the SOC that's relied on to handle functions like monitoring alerts and working to remediate immediate risks.

SecOps (Security Operations) is a broader term that often encompasses the SOC plus additional teams like incident response and threat hunting. Gartner defines SecOps as security operations technologies and services that defend IT/OT systems, cloud workloads, applications and other digital assets from attack by identifying threats and vulnerability exposures.

When we look at the traditional on-premises world, SOC and SecOps capabilities and requirements are reasonably mature. The use of SIEM (Security Information and Event Manager) technology is well established, as is vulnerability management and patch management technology. When it comes to the cloud however, the legacy toolset of SOC capabilities is hardly sufficient to help manage the risk that modern SecOps must mitigate.

As organizations rushed to accelerate their cloud transformations during the COVID era, IT infrastructure transformed. Staunchly protected data centers became multiple decentralized clouds filled with applications and workloads. Yet SecOps teams' day-to-day functions and the practices and tools that support them didn't morph at the same rate as the rest of the business. On the contrary, teams are racing to keep pace with the depth of the changes and provide the security tooling and insights they need for cloud environments. This has set up a significant security challenge that enterprises are now having to wrestle with to remain resilient.

This whitepaper explores the specific challenges SOCs currently face related to cloud and SaaS. It details why further evolving detection and response functions is critical, and how Mitiga's modern solution empowers SecOps cloud investigation and response capabilities by closing visibility and knowledge divides, while speeding core investigation and response functions.



The Current State of SecOps for Cloud

Up until recently, most SOCs have been security monitoring their organization's on-prememises systems and related endpoints, with a broad set of responsibilities including detection, investigation, response and remediation.

The rise of cloud platforms and software-as-a-service (SaaS) applications has demanded new detection, investigation, and response functions to be deployed. This shift requires both a reskilling of teams and a rethinking of tried and true processes.

Yet cloud and SaaS security are not contained in such neat boxes. Responsibilities that were once centralized within clearly defined perimeters of corporate IT ownership now span distributed teams across cloud platforms, SaaS providers, and on-premises infrastructure with varying levels of cloud security expertise. Visibility gaps emerge as threats slip through cracks between disconnected stakeholders.

Traditional security tools also struggle to extract value from the massive volumes of log data flowing in from these new, diverse environments. Formats differ across providers like AWS, Azure, and GCP, making relationships between events difficult to discern without the proper context. Ephemeral compute resources that rapidly spin up and down in platforms like Kubernetes eliminate digital evidence if not properly instrumented from the start while logs that are used for investigation are deleted after a few weeks for most CSPs and SaaS applications.

To maintain effective security in these new environments , SOCs must augment and supercharge existing capabilities with solutions that have been purpose-built for the modern dynamic threat landscape and the operational realities of today's enterprises.

The DevSec and CloudOps Divide

There are a lot of terms and approaches to Development, Operations and Security that have evolved in recent years. The rise of the DevOps movement which aims to bring development and operations closer together, has led to an approach known as DevSecOps, where security is more deeply integrated into the development and operations process. DevSecOps, however, doesn't typically have a strong focus, if any, on the particular needs of cloud security.

Organizations that are going through a rapid cloud transformation process typically have a dedicated cloud team. That cloud team will be familiar with the cloud operations, likely more so than their SecOps teams.

What can often occur in these instances is that the cloud teams assume that because there is a SecOps team in place, security is the responsibility of SecOps. However, the SecOps team may not have the capabilities or tools needed to properly protect the organization's cloud and SaaS environments.

As a result, organizations that have very strong monitoring, detection, investigation and response on-premises, may still have significant gaps related to those same functions for cloud.

The rise of the DevOps movement which aims to bring development and operations closer together, has led to an approach known as DevSecOps, where security is more deeply integrated into the development and operations process.

What Cloud Transformation Left Behind

The first generation of cloud transformation was largely about lift and shift of existing workloads and moving them into the cloud. In that approach, organizations took existing workloads, put them into virtual machines and lifted them into the cloud.

During that first generation, early Endpoint Detection and Response (EDR) technologies began to move to the cloud in a similar lift and shift approach. That was followed by the emergence of the first generation of cloud security solutions with approaches including, Cloud Security Posture Management (CSPM), Cloud Native Application Protection Platform (CNAPP) and Cloud Security Posture Management (CSPM). These approaches focus on primarily on cloud workloads.

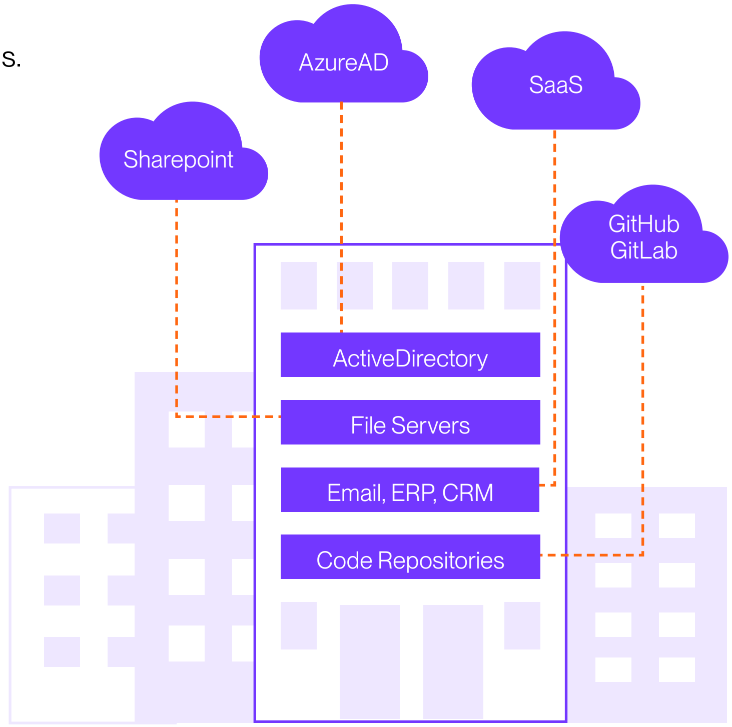
Most enterprises don't yet realize how much risk there goes along with the reliance on SaaS for critical IT and business operations. It's a whole new landscape with different working agreements.

The reality for many organizations is that enterprise IT infrastructure didn't really move to cloud infrastructure, it moved to Software-as-a-Service (SaaS) deployments. Even IT operations management itself has moved to SaaS, with many organizations using services from vendors like ServiceNow and Zendesk.

Who is responsible for the security of SaaS?

The SaaS platform provider is responsible for platform security. However, the platform is not all that might be at risk. This misunderstanding is often to blame for creating gaps in enterprises' security postures and resilience.

Because even if a given SaaS platform is secured, if a user gets compromised the risk can extend deep into an organization's usage of the SaaS provider. In fact it can also extend across multiple SaaS platforms that make use of the same single sign on (SSO) approach enabling an attacker to cause harm across an enterprise's cloud environment. Such scenarios have made Identity and Access Management a critical lynchpin in the SaaS security landscape.



SOC Challenges when Securing Cloud and SaaS

SOCs often measure their success based on metrics like time to patch (TTP) and Mean Time to Recover (MTTR). Today's SOCs also commonly tally and report on the sheer volume of alerts and threats they manage.

To support ongoing transforming, a greater part of an enterprise's security posture, and associated success metrics, must focus on the level of cloud preparedness and response effectiveness and speed.

That said, becoming adept in cloud and SaaS preparedness and incident response has many hurdles for teams that don't exist in on-premises.

Reduced visibility and span of control.
Responsibilities that were once centralized now often span cloud security teams focused on infrastructure-as-a-service (IaaS) environments, DevOps groups managing platform-as-a-service (PaaS) workloads, and the SOC itself, each with varying levels of cloud experience and expertise.

Expanding risks from SSO.
User access to multiple SaaS platforms through SSO (single sign-on) significantly expands potential attack surfaces. Should a credential be compromised, threat actors gain access to a multitude of connected systems, regardless of the security postures of individual providers. Incident containment and eradication across these disconnected systems becomes an arduous process for SOC teams without the right integrations and context.

Highly dynamic and diverse environments.
IaaS environments introduce their own obstacles. Ephemeral compute resources that rapidly spin up and down in Kubernetes eliminate digital evidence within moments if not instrumented to retain forensic data. Understanding relationships between events strewn across provider-specific log formats and APIs requires an in-depth knowledge that isn't often present in a traditional SOC.

Policing valuable data held on SaaS.
Another area of new cloud risk comes from privileged and sensitive information that might be present in a SaaS platform, from corporate secrets to mishandled PII. However, Data Loss Protection (DLP) and prevention technologies are often not part of the mix when it comes to their SaaS, adding more risk for organizations and SOC teams to manage.

To address these challenges, modern SOC teams need broad visibility into organizational operations and associated cloud and SaaS infrastructure, and it can be challenging to acquire. They also need to acquire new skill sets in order to investigate what they see.

Alongside all of these learning curves and new needs, perhaps the greatest challenge organizations face is the belief that teams already possess all the technology, processes and people they require for cloud investigation and response. However, when faced with a significant incident, teams often learn the hard way where their gaps lie.

Gaps in Tools Commonly Used in SecOps for Cloud

SIEM and XDR vendors tout "cloud support," but the reality is their solutions were not designed from the ground up for these new, radically different environments. Connectors may pull in basic logs, but lack the context required to uncover hidden threats and relationships between systems. Analysts are left sifting through logs with little understanding of implications.

Traditional playbooks and response capabilities also require retooling. Blocklists and quarantines don't map cleanly to cloud-native workflows involving both security and DevOps teams. Investigations demand an expertise encompassing identity, infrastructure, and applications that few generalist analysts possess.

Key gaps that exist today

Lack of visibility
Tools often lack required visibility into cloud IaaS and SaaS

Logs without logic
SIEMS might ingest logs, but lack the logic and automation to properly investigate cloud incidents

Diverse data formats
Cloud and SaaS vendor data formats vary, leading to data correlation challenges that existing tools don't handle

Contextual understanding
Even if an analyst gets the right logs into a SIEM,they often lack the context to make the information useful to reduce risk.

Knowledge gaps
Cloud and SaaS attacks and threats require a specific skill set that most analysts have not yet had enough investigative experience to acquire; even if they are adept in one cloud environment, it's hard to know them all.

Three Cloud Capabilities to Supercharge SecOps

01 Boosting Threat Detection for Cloud and SaaS

SOC professionals are often looking at a seemingly endless feed of events. Certainly there are dashboards across various tools that provide metrics and alerts but it's up to the people working in the SOC that see the alerts on all the dashboards, to decide what to do.

In the past, security budgets often leaned heavily towards prevention technologies that attempt to block risks before they ever enter an enterprise perimeter. That perimeter doesn't exist in the cloud world. With the sophistication and volume of risk in the cloud and SaaS world, the emphasis should not just be on prevention, but also on detection and response.

The faster an organization can detect and respond to a threat, the better. As the speed to detection and response accelerates, a SOC can effectively act as a prevention mechanism, limiting the ability of a threat to proliferate into a large risk.

If the organization can detect and respond rapidly, it's not preventing a security incident but it is preventing the impact that an unmitigated incident creates. In a fashion that's more efficient, because the SOC responds to the actual effect and is not trying to prevent every theoretical attack in the world.

02 Plugging Cloud Visibility Gaps

CSPMs are designed to alert teams of potential threats, but not to aid SecOps teams in deeper investigation. SOCs require a new generation of tools and services optimized from inception for cloud and SaaS security operations. Automated correlation and analytics are needed to connect related events across organizations' diverse and distributed attack surfaces.

Incident investigation demands centralized interfaces providing full context with a single click. Real-time log collection and retention is essential to maintain evidentiary trails in ephemeral environments. Playbooks must evolve beyond basic blocking to orchestrate multi-team responses leveraging cloud-native capabilities.

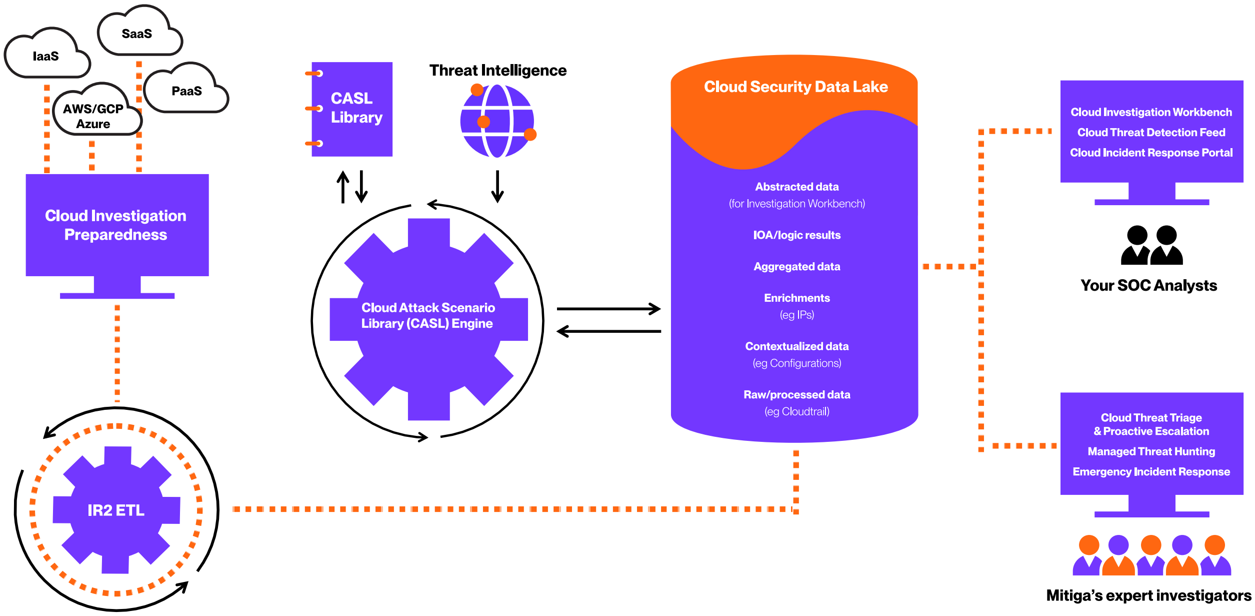
03 Adding Cloud and SaaS Investigation Expertise

Partnerships with managed services offering deep cloud security expertise can help augment knowledge gaps within analyst teams. Continuous feedback also strengthens detection logic as new tactics emerge. By integrating people and technology optimized for the cloud, SOCs gain the adaptive capabilities required to efficiently manage risk in constantly evolving environments.

Mitiga Empowers SOC Teams

Mitiga's cloud investigation and response automation (CIRA) platform was developed to scale the expertise of our specialized cloud and SaaS investigators, in order to fill the cloud capability gaps transforming enterprises face.

We developed integrated tools that the SOC team can use to automate and simplify complex and time-consuming aspects of cloud preparedness and investigation. Our teams leverage those same tools as a source of insights we deliver to our customers. By blending advanced technology and expert advisory, we deliver the deeper context and velocity that cloud investigation and response requires.



Giving SOC teams the complete visibility, context, and control required to investigate across their cloud and SaaS estate with confidence.

How we do it:

Within our integrated solution, SecOps teams benefit from an advanced tool set and services including:

Cloud Investigation Preparedness Assessment

Provides an evaluation of an organization's log collection strategy and offers quick visibility to where the gaps are and a roadmap on how to close them. Often Security teams are blind to the configurations the Cloud team has selected while that team has chosen to follow "best practice" without knowing what the security team will need. This assessment creates a roadmap for everyone in the organization to develop a plan for collection with the right priorities, so investigation is possible.

CASL (Cloud Attack Scenario Library) Engine

Helps power enterprises' investigations with the latest cloud threat intelligence to detect emerging and hard-to-discover cloud and SaaS attacks. CASL continually incorporates new indicators of attack (IOAs) based on global events, novel findings from Mitiga's Research team, learnings from active investigations. Every new customer investigation strengthens CASL's network effect.

Cloud Security Data Lake

Delivers unparalleled forensic visibility, retaining 3 years of unlimited log sources across 50+ cloud and SaaS adapters. All abstracted and organized for rapid-fire searches.

Cloud Threat Detection Feed

Automated detection leverages our CASL Engine, surfaces a triaged feed of events for SOC teams to investigate, while our investigators simultaneously begin hunts on any serious events.

Cloud Investigation Workbench

Enables SOC teams to create fast, detailed timelines of forensic events to surface contextual insights that correlate related identity, infrastructure and application events across an organization's digital attack surface. Providing security analysts a centralized interface to investigate incidents with full context in a single view significantly supports and speeds retrospective analysis.

Cloud Incident Response Portal

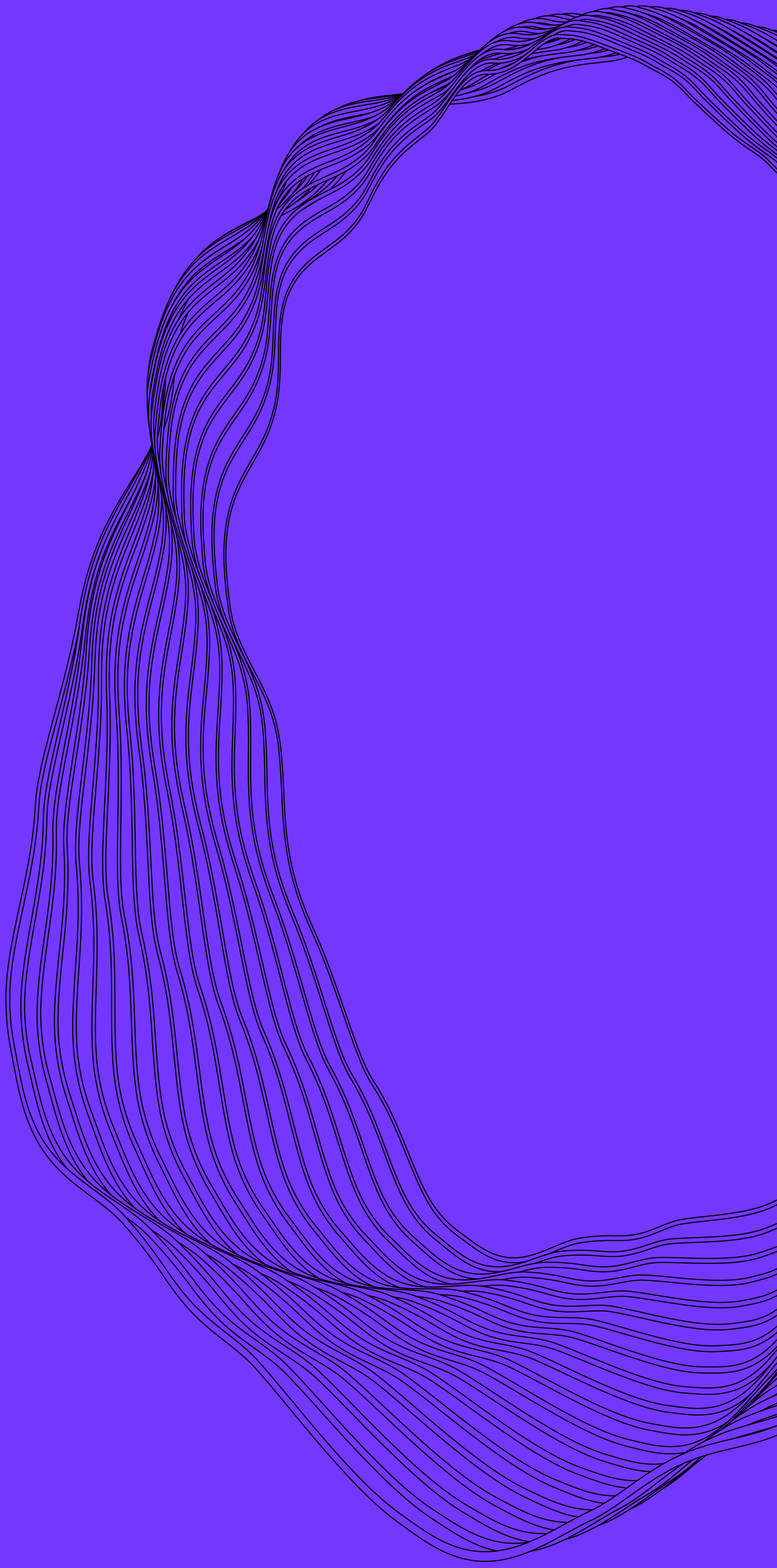
When cloud events turn to incidents our platform distills breach related answers in a single pane of glass, while our investigators are on call 365/24/7 to provide guidance and support to your internal response efforts. Our approach accelerates cloud breach containment 70x.

Mitiga Investigation and Response Teams

Mitiga offers guidance and support at every point as teams require it—from initial data gathering to full emergency incident response. Plus, Mitiga's specialized threat hunters serve as your extra set of eyes, conducting continuous, event-driven and strategic hunts. It's a way Mitiga not only augments SOC capacity but also strengthens SecOps team's internal cloud and SaaS investigation capabilities.

Fundamentally, our approach is designed to empower SOC teams with tools to root out and respond to cloud and SaaS threats and manage cloud risk without having to possess either deep cloud or investigation expertise. Plus, at times when indicents become too complex to manage alone, they have an invested team of experts already on-call.

By fusing security expertise, cloud-native technology, and adaptive services, Mitiga aims to supercharge SOC capabilities. We close visibility divides and empower analysts with contextual insights that drive for more efficient detection and containment of threats in dynamic cloud and SaaS environments.



We’ve got your back

Mitiga's expert teams and cutting-edge tools augment your SOC capacity and capabilities, giving you the confidence to master cloud and SaaS breaches.

MITIGA

For more information, visit www.mitiga.io or email us at info@mitiga.io

US +1 (888) 598-4654 | UK +44 (20) 3974 1616 | IL + 972-3-978-6654 | SG +65-3138-3094