LEARNING MADE EASY

Mitiga Special Edition

Cloud Threat Detection, Investigation & Response

for dummies®
A Wiley Brand

Improve threat detection

Lower response times

Build resilience

Compliments of

MITIGA

Dan Sullivan

About Mitiga

Mitiga closes this cloud gap for SecOps teams — because it's time to do for SecOps what CNAPPs did for DevOps.

Mitiga is the industry's only complete solution for cloud threat detection, investigation, and response — built by investigators, for investigators. Mitiga supercharges today's SOC teams with the cloud era capabilities that enterprises have been missing, delivering broad visibility across clouds and SaaS, automation that speeds investigations, and rich context that informs cloud threat detection, hunting, and response. Together, Mitiga's capabilities minimize breach impact and enhance enterprises' cyber resilience.

www.mitiga.io

Cloud Threat Detection, Investigation & Response

Mitiga Special Edition

by Dan Sullivan

for dummies®
A Wiley Brand

Cloud Threat Detection, Investigation & Response For Dummies®, Mitiga Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-28143-5 (pbk); ISBN 978-1-394-28144-2 (ebk); ISBN 978-1-394-28373-6 (ePub)

Publisher's Acknowledgments

Development Editor: Rachael Chilvers

Project Editor: Tamilmani Varadharaj

Acquisitions Editor: Traci Martin

Editorial Manager: Rev Mengle

Business Development Representative: Jeremith Coward

Introduction

As a professional who's likely been along for the ride or even helping to direct your enterprise's digital transformation journey, you understand some of the challenges that come with protecting your increasingly complex cloud estate. However, you're likely less clear about the leading-edge practices and approaches you can adopt when those painstaking protections are breached.

When an inevitable cloud breach does occur, your organization — and perhaps even your team — becomes responsible for detecting the threat, determining the scope of the attack, containing adverse effects, and restoring normal operations. Doing this effectively requires planning and preparation. This book helps you understand everything that work entails.

In this context, our book serves as your guide, offering insights into the intricacies of cloud threat detection, investigation, and response. Whether you're a seasoned cloud security expert or just beginning your journey in this realm, our comprehensive resource equips you with the knowledge and strategies needed to navigate the evolving cloud security landscape confidently.

About This Book

This book explains the capabilities of cloud threat detection, investigation and response, and how they differ from on-premises. It begins with an overview of the capabilities and how digital transformations and the adoption of cloud technologies adds complexity to security operations.

Preparing for cloud investigations means confronting some common challenges. You have less visibility into activities and operations in the cloud than you do on-premises. Security logs are spread across servers controlled by various cloud providers. You need a way to collect, integrate, and analyze that data. The chapters on security data lakes, threat detection, and hunting give an overview of what those technologies and practices look like. We conclude with an overview of incident response, with an eye toward elevating organizational resilience.

Foolish Assumptions

We make some assumptions about you, the reader, so we can compile the most useful insights for you. We assume you're a security leader such as CISO, SecOps director, director of security, or cloud architect. We also assume you have knowledge of investigations and challenges in detecting threats. You may have some experience with cloud architecture and its impact on cloud investigations, but we assume that's a fairly new area for you.

Icons Used in This Book

This book uses icons in the margin to draw your attention to certain kinds of information. Here's a guide to the icons:

We use the Tip icon to highlight anything that'll make your life a little easier.

When we tell you something important, we mark it with the Remember icon.

We use lots of examples in the book to make the information relevant and relatable.

Beyond the Book

If, after reading this book, you'd like more information about cloud investigation, threat detection, and response, head to `www.mitiga.io`.

IN THIS CHAPTER

- Defining the capabilities and the environments they cover
- Understanding why you need these cloud security capabilities
- Learning who's involved in these areas of cyber, and why
- Knowing the differences between cloud and on-premises investigations

Chapter 1
What are Cloud Threat Detection, Investigation, and Response Anyway?

If one thing has become clear to security professionals during the cloud era, it's that the security landscape is changing. New threats and risks, new infrastructure with evolving demands, and new ways of investigating and responding to security incidents are emerging. As someone concerned with protecting your organization's information services and resources, it's important to understand how cloud adoption is reshaping how you prepare for, detect, and respond to a new class of threats.

Your Eyes in the Sky: Defining the Core Capabilities

To better understand cloud threat detection, investigation, and response, picture your data floating in the digital sky, vulnerable to threats you can't see — from cyber criminals to malware storms. Cloud threat detection watches over the digital clouds using special technologies and tools to find odd things going on,

like attempts to get in without permission or strange data trends, before they can damage your important data.

REMEMBER

Cloud investigation is like putting on your detective's hat and picking up your magnifying glass. It's about looking into strange behavior, gathering hints, and putting together the puzzle of what happened. These steps include looking at logs and network data to find the threat's source and stop it from happening again. Cloud incident response is like the SWAT team that swoops in to stop the threat and limit the damage. This means quickly isolating the systems that are being attacked, putting in place security steps to stop the attack in its tracks, and getting things back to normal as soon as possible. Being ready for the worst and taking quick action to protect your data and assets is what cloud incident response is all about.

The Alphabet Soup of Cloud Environments

In addition to security capabilities, you'll encounter a host of cloud environments in this guide, starting with the cloud service providers (CSPs) themselves. A CSP offers a range of services for delivering computer, storage, networking, security, and other digital capabilities. For example, identity providers have services for creating, managing, and monitoring identities and associated authentication mechanisms. Cloud services are commonly grouped into three broad categories:

- **Infrastructure as a Service (IaaS)** is a collection of compute, storage, and networking services managed by the provider's customers. IaaS offerings deliver a high degree of control over virtualized resources, such as virtual machines and virtualized storage. They also require the most of customers in terms of system administration.
- For those who'd rather focus on application development, **Platform as a Service (PaaS)** providers offer support services for deploying applications that reduce the amount of infrastructure management on users of the service.
- In the **Software as a Service (SaaS)** model, you have access to applications for functions like human resources, customer

resource management, financial management, and collaboration. One of the distinguishing features of SaaS is that users of these applications don't have to manage infrastructure.

These providers, whether or not you realize it, have become your partners in security.

Knowing Why You Need These Cloud Security Capabilities

With the adoption of a wide variety of IaaS, PaaS, and SaaS technologies, you're moving more of your information assets outside the perimeter of on-premises systems into cloud platforms that have different types of security controls.

REMEMBER

You need the ability to detect, investigate, and respond to activities across platforms. Attackers won't limit themselves to just your on-premises infrastructure or one SaaS provider. You need the ability to understand what's happening in the entire range of your applications, services, and infrastructure.

Who's Who in Cloud Investigation and Response

Cloud investigation involves a wide range of stakeholders with different skill sets, accountabilities, and interests related to company security, so it's best to understand everyone's roles and needs up front:

- **Security operations (SecOps) teams** are responsible for threat monitoring and detection, incident response and mitigation, vulnerability management, and security operations center (SOC) management.
- **Chief information security officers** (CISOs) protect the organization from internal and external cyber threats. They're responsible for effectively monitoring and maintaining the security of their organization's applications, databases, computers, and websites.

- **DevOps engineers and system administrators** understand infrastructure, services, and workloads. They oversee and monitor application and infrastructure planning, testing, and development. DevOps ensure that the development and release pipeline leads to more reliable services for enterprise and customers.
- **Chief information officer** (**CIO) and other executives** lead the management, execution, and usability of IT. They're responsible for multi-year IT planning, programming, and budgeting, as well as successfully implementing the information and computer an organization's technology systems to maximize its capabilities.
- **Application owners** bridge the technical and business realms and know how applications are used and which business operations are impacted by the disruption of application services. While many of those involved in cloud investigations are also involved in on-premises investigations, you'll see that what they're tasked with and how they collaborate often change as you move to the cloud. Plus, you'll still need to keep in mind the traditional stakeholders, like boards of directors, regulatory bodies; and risk, legal, and communications departments who all seek answers when an incident happens.

This Is Not Your On-Premises Investigation

How you conduct investigations is influenced, in part, by the technologies you have available. Within on-premises investigations, you have complete access to the operating system, application, and network logs. You control identity management and authentication systems. You define the network perimeter and control the flow of network traffic within the on-premises network.

REMEMBER

Cloud investigations function in a different environment. Cloud and SaaS providers expose different levels of control and different logging. You don't have access to logs from provider-managed infrastructure. In cloud investigations, you may have to integrate data from multiple SaaS providers. Tools that you've used on-premises, such as log collection tools, may be of limited use with SaaS providers.

IN THIS CHAPTER

- Understanding the ripple effect of digital transformation
- Dealing with the reduced visibility with cloud and SaaS
- Sharing responsibility with cloud vendors

Chapter 2
How Digital Transformation Upended Traditional Investigation

Digital transformation hasn't simply gone about remaking how enterprises operate and transact. It's substantially revamped the IT infrastructure that enables all of it. And, you guessed it: That impacts security.

Digital Transformation's Ripple Effect

As application and systems development moved to clouds and SaaS, corporate IT was faced with a whole new set of problems — especially the challenge of adapting to new ways of securing information assets and infrastructure. This transformation isn't a point in time but a continuous process. Cloud footprints continue to expand and change, and new applications can be spun up all the time. It's a dynamic new way of operating.

Enterprises are adopting a range of delivery models in cloud computing. Some are using IaaS to run workloads in the cloud in ways similiar to how they run them on-premises. Many are turning to Platform-as-a-Service (PaaS) providers for development and application services.

The vast majority are turning to scores of SaaS providers for targeted functionality that's essential to keep the business operating and can be done more efficiently and effectively by a specialized provider.

The cloud era requires acquiring new security capabilities, processes, and tooling to answer the needs of scale, complexity, diversity, and dynamism of the cloud footprint. After all, most cloud attacks move laterally and impact multiple, disparate environments. Most SecOps teams, however, are still working with legacy tooling and technology that's more suited to on-prem.


TIP

The rise of new cloud security capabilities and tech has been the answer to this increasingly urgent need. The first step in all of that is finding a way to make the invisible visible in all your cloud and SaaS environments.

Cracking the Code on Cloud Visibility

You can't investigate what you can't see. Ensuring comprehensive visibility across your cloud estate is vital. However, getting this unified vision is easier said than done when the average enterprise is running on an average of three public clouds and hundreds, sometimes thousands, of SaaS applications. On top of that, what's contained in a single cloud changes all the time.

It's an incredible amount to keep track of, especially for a security operations team that isn't associated with spinning up these new workloads and may have most of their security experience in on-premises environments that behave differently. Also, the kinds of visibility required for cloud detection, investigation, and response are extensive. It's not only about seeing a current snapshot. It's also about looking into the past and across sources to piece together a story of what happened and how.

REMEMBER

You likely won't have detailed performance data or access to information about what operating system is used or what security patches have been applied to the system. Information that you might have depended on when investigating on-premises security breaches are no longer available to you.

The way you investigate security incidents must change to meet the challenges and limitations of the new normal of multi-cloud and multi-SaaS providers.

Sharing Responsibility with Cloud Vendors

REMEMBER

Cloud providers and their customers share responsibility for security in the cloud. That sounds like, "we're all in this together." However, in reality, shared responsibility acts more like split responsibility:

- **Cloud providers** are responsible for securing the infrastructure, hardware, and software of the cloud. This includes securing data centers, providing physical access controls, securing virtualization systems, and isolating customers' environments from one another.
- **Cloud customers** have their own set of responsibilities. These include securing applications they run in the cloud and configuring and patching operating systems when using IaaS-provisioned resources. Customers are also expected to employ security services provided by cloud vendors, such as web application firewalls, encryption services, and firewalls as needed. Data security is another area that's a top responsibility in relation to access controls, properly classifying data, implementing data lifecycle management policies, and complying with regulations specific to their industry.

Investigating cloud incidents falls into the realm of both cloud providers and customers, although they have distinct responsibilities. (We delve more into those details in Chapter 3.)

Internal Decentralization and Cloud Investigation

Step into a time machine, go back a couple of decades, and you'd likely find standardized desktops running corporate-approved software with network access to servers in the on-premise data center.

If you want to run a new application on a server, you'd first have to get approval from someone in IT. No problem, right? Just fill out a form, justify the budget needed, answer a few questions, and your request lands in the queue with all the others in the IT backlog. And if something bad happens on that desktop, the problem is likely to be contained and resolved quickly by the team down the hall.

REMEMBER

Today is different. The cloud offers better ways to innovate — but without the guardrails offered by on-prem. You can provision a virtual machine in one of several major cloud providers and run your software there. If you need a database but don't have a database admin available, you can use a PaaS-based database service. If you need to analyze a large data set that's too much for your on-premises resources, you can create a cluster, upload your data, run your analysis, and shut it all down faster than it would take an overloaded centralized IT team to get to your request.

Cloud computing has reduced the need for centralized control over limited IT infrastructure. Organizations are adapting to this with decentralized decision making about what compute resources to use for various projects. While nobody misses the overhead and delays of centralized IT bureaucracy, many miss the added security knowledge and support of the on-prem days.

EXAMPLE

If your finance department analysts develop custom predictive models related to customer buying habits, they may not have sufficient experience with security to understand the risks of moving data to the cloud, how to secure access to servers, or how to use role-based access controls or other security measures to protect enterprise assets and IP. When an incident arises and it's time to investigate it, these gaps can present big problems for the organization's response and resiliency.

IN THIS CHAPTER

- Determining who owns what in your cloud estate
- Overcoming the data gaps of shared responsibility
- Bridging expertise gaps to conduct cloud investigations

Chapter 3
Building Partnerships and Processes for Successful Investigations

The adage that good fences make good neighbors has a corollary in cloud services: Well-defined security boundaries make for a good understanding of respective responsibilities. The idea of shared responsibilities can be fairly well understood in principle, but there are differences among providers. Different levels of clarity and different rules can be challenging to track. Regardless of the difficulties, you need to work through these challenges to support cloud investigations in multi-cloud and multi-SaaS environments. But, before you strengthen those areas of your posture for investigations, you need to get clear on the basics.

What Makes Up Your Cloud — and Who Owns It?

A first step to ensuring successful cloud threat detection, investigation, and response is understanding what you have in the cloud. This can be a long list, and that goes way beyond cloud workloads. It typically includes:

- Compute resources, including virtual machines, containers, and clusters
- Storage resources, including databases, object storage, and network attached storage devices
- Virtualized network infrastructure, such as routers, routing tables, firewall rules, web application firewalls, and virtual private networks
- Identities of users as well as service accounts and their associated roles and permissions
- Data about pretty much everything in your organization
- Workflows and pipelines for applications

Some of these elements are clearly within the realm of cloud provider responsibility, such as storage devices and servers. Others, such as user identities and their authorizations, are the responsibility of cloud users. These distinctions are important because the ability to monitor and observe them comes with responsibility for these elements.

EXAMPLE

For the most part, cloud customers are probably not too interested in which cloud provider employees are allowed in particular server rooms and which aren't. That's just too much of an implementation detail that doesn't directly influence the customer in most cases. Similarly, a cloud vendor typically doesn't have an opinion about which of your employees should have read access to particular database tables.

What you can observe in the cloud from a security and performance management perspective varies with the type of cloud you're using. You have more access to implementation details in an IaaS environment than you do in a SaaS environment. Sometimes, getting the data you need for cloud investigations means hopping over fences to see to the other side — and for that, you need to work with your cloud provider.

Overcoming the Data Gaps of Shared Responsibility

The shared responsibility model recognizes that both cloud providers and cloud users have a role in security. It also complicates investigations where the need for information spans boundaries of responsibility.

EXAMPLE

Imagine your organization uses a SaaS service that supports the collection of detailed information about your customers. Some of that data is considered private, and access to that data is governed by regulations. As a user of the SaaS application, it's your responsibility to determine who in your organization can read, update, or delete that data. You may also be required to demonstrate that you have controls in place that ensure you're meeting regulations. For example, you may need to produce audit logs showing who updated sensitive information in the database during some period of time.

One question that may come to mind is, *how can I can log who's updating information in a database that I don't control?* Yes, you control who's authorized to update information, but unless you have access to database application code and database management configuration details, you may not have a way of creating an audit change log. For that, you depend on the SaaS provider to collect the information and make it available to you as needed.

EXAMPLE

You may need other details as well. Let's assume an authenticated user with proper permissions updated sensitive information, but you believe that user's login credentials were compromised in a phishing attack. You want details about the authentication process used around the time the sensitive data was changed. For that, you may need to go to a third-party identity provider that provides the single sign-on service to your SaaS application.

You can see that something as simple as determining who updated a record in a database can quickly turn into a task that involves multiple organizations with different responsibilities and different mechanisms for meeting those responsibilities. Now imagine, it's not one user at one point in time, but tens or hundreds of users over an extended period of time that you need to investigate. Welcome to the world of cloud investigation at scale.

Bridging Expertise Gaps: SecOps Meet DevOps

The complicated nature of cloud investigations requires a broad range of specialized knowledge and skills to resolve each incident. Typically, gaining those requires calling on both DevOps and SecOps teams because neither one currently holds all the cards when it comes to cloud threats.

DevOps teams are well-versed in practices and processes for application development. Those usually emphasize automation, incremental improvement with continuous integration, and continuous delivery, which are all highly relevant to cloud operations. DevOps may have built up some knowledge of security measures and tools related to protecting the CI/CD pipeline, but they don't possess the same experience or knowledge banks as SecOps professionals.

SecOps teams have a deep understanding of security but often possess less experience working with cloud technologies. When dealing with on-premises investigations, SecOps teams have access and capabilities to take the actions needed for an investigation. In the cloud, that isn't generally the case. SecOps teams often don't have permissions or cloud infrastructure knowledge to respond and instead depend on DevOps teams to help with investigations.

This distributed responsibility can be challenging to manage because each team has different skill sets, and lines of authority are rarely clear. In practice, the result is often a lack of clear accountability and processes, which can significantly slow response times. SecOps for the cloud relies on your teams breaking down silos to envision new ways of working together to investigate cloud threats.

TIP

The practices of DevOps are also applicable to security and cloud investigations. Collaboration between security and operations professionals is crucial when investigating incidents. Knowing what systems are used for authentication, authorization, encryption, and logging is essential. Knowing how to extract data from these systems and integrate that data is also a necessary skill. These are skills that DevOps professionals have developed working with software engineers. Bringing these valuable skills to cloud investigations is one of the ways you can mitigate the complications that arise when operating in a multi-cloud and multi-SaaS environment.

IN THIS CHAPTER

- Being prepared for cloud investigations
- Understanding cloud logging and its importance
- Identifying which data to collect, how to find it, and how long to keep it

Chapter 4
Why Preparation is Essential to Cloud Investigation and Response

There's a lot to be said for on-the-job training, but the last thing you want is to learn what you need for a cloud investigation while you're in the middle of a breach. The time you spend preparing your staff and partners, getting your processes and procedures in place, and deploying the right tools will provide the essential foundations to detect threats across your cloud estate, conduct swift cloud investigations, and respond effectively to attacks.

To be crystal clear, if you don't invest the time to understand what data you'll need for a cloud investigation in advance and actively, continually collect it, the chances that data will be available when you need it are virtually nil. Zero. It's rarely going to happen. And when it does, it occurs with significant time and cost.

What Being Prepared for Cloud Investigations Really Means

Here are some key tasks to keep in mind when it comes to being cloud-breach ready:

1. First, know what cloud resources you have and where they are. Don't forget to catalog the SaaS platforms you're using, too.
2. Next, determine where you have visibility gaps. The SecOps team will know where your visibility problems are.
3. Once you understand your visibility gaps, you can activate log sources. Storing logs costs money, so you need to prioritize which services and environments you want visibility into. Certainly, your production finance environment should have detailed logs retained, but you may not need as much logging in your development environments.
4. Plan for collecting and analyzing logs. Will you use a SIEM? If so, plan to monitor continuous ingestion into the SIEM so you don't drop data because storage has filled up or there's a problem with the ingestion pipeline.
5. Finally, test your tools against different cloud sources. Be sure you can collect forensic data from the infrastructure and applications you use. Understand how to analyze logs from different sources.

Sounds easy, right? Well, actually, it may not sound easy, but it can be done!


TIP

Cloud investigations require a range of technologies for collecting and storing data, analyzing patterns in data, and searching for significant events and activities. So, part of the planning process should also include assessing what tools to have in place and how they'll function together. Will they be effective for cloud speed and scale? Or, will they take forever or cost too much to effectively sift through cloud data? (More about this in Chapter 5.)

Understanding the Basics of Logging

Whether you're using on-premises, IaaS, or SaaS technologies, you depend on logs from these systems for insights into the state of operations, as well as a view into user and administrator activities. Cloud investigations depend heavily on logs. This, in turn, means you need access to logs with sufficient detail, the ability to analyze a wide range of log formats, integrate information across log sources, and identify activity patterns within this integrated view of your systems.

Collecting data: What and for how long?

When it comes to cloud investigations, log data is your new best friend. As you plan for cloud investigations, consider the variety of sources you have for log data, what kinds of activities the log data describes, and what kinds of information may be missing from the data sources you've identified.

Challenges of cloud logging

Cloud logging is fundamental, but it's not simple. Here are some factors that can make it hard.

Complex data collection

Data collection sounds straightforward: A lot of business data fits neatly into well-organized rows and columns. How hard can this data collection thing be? Apparently a lot harder than many people think.

Log data is a prime example of semi-structured data. There's some structure to log lines, but extracting the interesting relevant parts can be difficult, especially at scale.

Too much data

In addition to the complexity of data, you have to address the issue of data volumes. This requires you to target what you want to collect so you aren't storing and sorting more than you need to.


EXAMPLE

Planning for cloud investigations requires attention to data lifecycle management. You want to keep the data you need for investigations as long as it could be of value. For example, consider an attack that goes undetected for months. An investigation into how

the attackers were able to compromise the system will require data at least as old as the attack itself. If you don't have it, you can't search it.

Collaborating with cloud providers

Given the shared responsibility model of cloud security, you need to have procedures in place for working with cloud providers in order to gain access to data needed for cloud investigations.

Once you have everything ready concerning your data, there's another very different aspect of preparing for cloud incidents: ensuring your team is clear and ready.

Preparing Your People for Cloud Investigations

There's a reason every airplane flight begins by going through the handout that details security measures in case of an accident. A crisis is not a teaching moment.

To keep a cloud breach from becoming a crisis, relevant people throughout your organization need to know the importance of cloud investigations, the processes involved, and the specific role they'll play.

If you're not already, begin undertaking ongoing organizational cloud breach preparedness activities. These include executive-level drills and tabletop exercises focused on cloud threat vectors. They may also involve some training for broader staff. You'll want to review organizational processes and procedures to identify gaps and dependencies in your incident response planning.

REMEMBER

No one person will have all the skills and time needed to conduct even modestly complicated cloud investigations. Hybrid teams made up of internal security and DevOps professionals and outside experts will be the norm to ensure the enterprises possess the capabilities and capacity required in multi-cloud and multi-SaaS environments.

IN THIS CHAPTER

- Understanding SIEMs: their value and limitations
- Seeing how a cloud security data lake differs from a SIEM
- Taking on the challenges of creating a cloud security data lake
- Knowing the key features of an effective cloud security data lake

Chapter 5
The Vital Role of Cloud Security Data Lakes and What Came Before

When working with logs, the analogy of searching for a needle in a haystack comes to mind. For the most part, SecOps teams have turned to security information event management (SIEM) to help with searching for those needles.

Now, in addition to those proverbial log needles, for cloud investigations, you need to search through many other types of data that exist across a thousand cloud and SaaS haystacks. For this, security professionals are adopting cloud security data lakes that can store a wide range of data and allow for more effective and efficient searching.

SIEM: Close but Not Sufficient for Cloud Investigations

SIEM systems are widely used platforms for monitoring, managing, and analyzing security event data. SIEM systems were developed to collect and aggregate log data from a variety of sources,

including servers, applications, networks, and security devices. The data is normalized using specialized plug-ins and integrated for analysis, so the system can provide for continuous monitoring and alerting. (Note: New log types require their own plugins.) The alerting is based on pattern detection methods that identify anomalies indicative of security events. While they serve an important role in securing information systems, they have significant limitations.

EXAMPLE

A SIEM can identify user patterns associated with an insider attack. (Note, this assumes the security team understands how to tie together which events should alert on such an attack.) SIEMs are the ideal tools for supporting some security workflows and have well-developed integrations with complementary services, like ticketing applications. They were not, however, designed to gather cloud history data for forensic investigations.

REMEMBER

In real-world practice, SIEMs' value for investigation is also limited because of how long they can reasonably store data, due to cost and performance concerns. Keeping data for 30 to 90 days isn't uncommon with SIEMs. With these constraints, SIEMs are appropriate for real-time security monitoring, incident detection, and compliance reporting. Cloud investigations, however, require more history and added functionality.

Seeing How Cloud Security Lakes Differ from SIEM

Cloud security data lakes have evolved to meet the specific needs of cloud investigations and, therefore, don't suffer from the same limitations of SIEMs when data is needed for detection and response.

Cloud security data lakes, like data lakes in general, store a wide variety of data and don't enforce a particular structure or schema on the data stored. Data lakes typically take advantage of object storage in clouds to hold large volumes of data for extended periods and have lower costs than often found with SIEMs.

TIP

With the ability to store more data, users of cloud security data lakes can take advantage of data intensive methods, such as machine learning, statistical analysis, and user behavior analysis. The breadth of data also enables a broader range of use cases

including threat hunting, incident response, and longer-term security analytics.

Another advantage of cloud security data lakes is that they're built using a distributed data processing platform, such as Spark, which has a variety of analytic and machine learning libraries readily available for processing security data.

Challenges with Creating a Cloud Security Data Lake

Building a security data lake requires a combination of expertise including data engineering, cloud architectures, security analytics, and forensics. It also takes a significant investment of money, time, and skilled personnel. Data lakes are architectural models that require careful design and a focus on the particulars of security and cloud investigation.

TIP

If you were to build your own security data lake, plan on investing time to build pipelines for processing diverse data sources, a comprehensive data governance scheme, and access controls. Also, consider the risks associated with design or implementation problems that can lead to data quality issues, performance bottlenecks, or insufficient security controls in a production environment. Many organizations opt to use pre-built security data lakes to avoid the cost, time demands, and risks associated with building a security data lake from scratch.

What Makes an Effective Cloud Security Data Lake?

It's easy to spot the characteristics of an effective data lake for cloud security. They include:

- The ability to store large volumes of data
- The capability to gather, retain, normalize, and interrogate data from cloud and SaaS data sources

- Affordably retaining years of historical data, not simply a few months at best
- The capability to hunt laterally across data sources and respond to findings
- Automation that speeds aspects of the investigation process to reduce the workload on information security professionals and to accelerate the mean time to respond
- Tools to support analytic workflows and take advantage of complementary technologies, such as machine learning

REMEMBER

Cloud security data lakes are an enabling technology for detection, investigation, and response. With a scalable, integrated platform for collecting and storing security data for long periods of time, you can build tools to support threat detection and hunting, which are the topics we turn to in Chapters 6 and 7.

IN THIS CHAPTER

- Discerning what's unique about threat detection in the cloud
- Overcoming the barriers to real-time cloud threat detection
- Utilizing threat intelligence in the cloud
- Triaging cloud security incidents

Chapter 6
Threat Detection in the Cloud

Malicious actors attack enterprises — now, they attack enterprises' clouds and SaaS. You can prepare for these events with research, planning, and tooling, but that won't prevent all attacks. Another part of preparing for and living with the risk of cloud attacks is being in a position to root out cloud threats early, in order to investigate them and respond to them appropriately. This requires a combination of tools, threat intelligence, and both detection and hunting skills.

Detecting Threats Early and Often

Detection is the process of looking for small indicators at a point in time that may indicate a security threat. The first step in this process is identifying indicators of attack.

Identifying indicators of attack

An indicator of attack (IoA) is an event that may be part of a larger pattern of an attack and warrants further investigation.

EXAMPLE

For example, a user login failure could be an indicator worth investigating. Now, a single login failure followed by a successful login attempt is pretty common. Many of us occasionally mistype our passwords. A series of two or more failed attempts to authenticate, however, is more likely to be associated with an attempt to compromise an account.

An IoA can also be made up of a combination of different types of events. For example, a user logging in from an unusual location followed by a series of file downloads to a device or cloud account not managed by the organization could be indicative of an exfiltration attempt.

TIP

An IoA alone doesn't mean that an attack is underway, but it does mean that someone should investigate to understand more about the context of the indicator.

Your identity is the target

Most on-premises attacks start with malware or exploiting a unpatched vulnerability, but these attack vectors are much less common in the cloud. In the cloud, where there's no perimeter with firewalls, identity is a much more appealing target. Roughly 50 percent of breaches in the cloud start with an attack on an identity, including identity theft and phishing attacks.

EXAMPLE

One of the reasons identities are appealing targets is the wide spread use of single sign-on. Once an identity is compromised in an environment using single sign-on, an attacker can gain access to a range of applications and data sources. For example, an analyst working on personnel cost management might have access to a human resources SaaS application, a finance system, document sharing, email, messaging, and other collaboration tools.

TIP

Multi-factor authentication (MFA) is one way to provide additional protection for identities. Even if an attacker were to get your login name and password for your company's identity management system, they won't be able to log in if they don't have your authentication app or MFA device. That's how it's supposed to work in theory, anyway (see the nearby sidebar for examples of how attackers can sidestep MFA).

UNDER ATTACK – ABOUT TO CRACK

Attackers have devised ways to take advantage of human nature to get around the protections offered by multi-factor authentication (MFA) devices. One technique is known as *MFA push fatigue*.

In this scenario, an attacker compromises login credentials and tries to access your account. The authentication service pushes a message to an MFA device to verify that the login attempt is legitimate. When the message arrives unexpectedly, you decline to authorize and move on with your day. But imagine if those messages kept coming and coming because the attacker was repeatedly trying to access your account. At some point, you might begin to wonder if something's wrong with the MFA system. If the message keeps coming, you might conclude that, yes, something's definitely wrong, and you need to make this stop, so you acknowledge the login attempt as legitimate. This solves the problem of repeated MFA messages, but at the cost of granting an attacker access to your account.

Another form of attack on identity is an *adversary in the middle* attack. In this case, an attacker uses a phishing site that looks legitimate to lure someone into entering their login credentials to an SaaS or identity provider. The attacker then forwards those credentials to the real SaaS site and starts the authentication process. The victim receives an MFA message prompted by the attacker logging in and, since this is expected, acknowledges the message, completing the authentication process for the attacker.

Attacks in the Cloud Are Different

On-premises attacks often exploit a weakness in software but as you move to the cloud, such exploits are less common. This is due, in part, because it's much harder to attack the underlying systems that are managed by the cloud providers. Instead, attackers find it much easier to "log into" instead of "breaking into." This is because identity is used to determine access. In the past, the network was the perimeter; you needed VPN or Citrix to provide access into the network when attacking. In the cloud era, the perimeter *is* the identity, so once you control an account, you have access.

Today, SaaS companies offer a platform that needs a "non-human identity" in order to work; usually an API key or something similar. If attackers are able to acquire those API keys, they'll likely have access to an identity that isn't tied to a specific employee and won't have any type of multi-factor authentication attached to it.


EXAMPLE

An example of exploiting non-human identities occurred when adversaries compromised a company's code repository, where they found access keys. The attackers used those keys to access an AWS S3 bucket that had client information, including the access keys the victims were using to authenticate to their client's systems.

Context is Everything

Capturing the context of an event can require information from multiple systems, such as identity management systems, authentication systems, as well as activity logs from applications. It's worth noting that SIEM systems don't bring in nearly enough log data to provide a full context of events typically found in cloud investigations. While a SIEM might have connectors to bring in security logs, they're not designed to capture details about emails sent, documents updated, features of applications used, or other activities. Integrating logs from a range of applications and services is challenging because logs have different formats and carry different types of information.

Real-time Cloud Threat Detection Has Barriers

The need to detect threats as soon as possible has led to real-time detection on-premises. Unfortunately, real-time detection isn't available in the cloud. This is because it takes time from an event occurring until it's processed by the providers and then shipped into the logs, and that change in the logs is provided to the client. The fastest logs in the cloud today are at least 5–10 minutes behind. So, even before you bring in any solution that focuses on getting the main content from your logs, the provider is delaying their shipment. These are good facts to understand when setting team KPIs and executive expectations. To detect any cloud threat you need more than speed; you need intelligence.

WHY LEGACY SOLUTIONS ARE INADEQUATE FOR CLOUD THREAT DETECTION

Most of the legacy solutions for threat detection were built, designed, and used for different types of technology and different types of threats. Cloud technologies bring new attack paths and new threats. Many existing detection tools can't be used with object storage, serverless functions, or SaaS platforms. Also, the composition of applications today is more varied. In the past, most systems were very similar, often using some combination of Active Directory, Windows, and Linux systems. Now, a variety of vendors offer similar technology, but using completely different log structures, each requiring their own mechanisms for analyzing those logs.

Using Threat Intelligence in the Cloud

Threat intelligence is the process of collecting, analyzing, and sharing information about security threats to an organization. Threat intelligence includes:

- **Strategic intelligence** includes high-level information about threats and risks. This type of threat intelligence is typically used by executives.
- **Tactical intelligence** provides technical details on threats and indicators of attack.
- **Operations intelligence** provides information about the motives and intents of malicious actors and potential attacks.

Cloud investigations benefit from all forms of threat intelligence. Threat detection and hunting in the cloud benefits from security tools and platforms that integrate threat intelligence with detection and hunting capabilities.

Triaging Security Incidents

Knowing that a security incident has occurred or is in progress immediately triggers the question, what should be done? This is where triaging comes in. Triaging is the process of assessing and prioritizing events and then assigning resources to mitigate the impact of the adverse event.

How you triage depends on what details are available to you at the time. Threat intelligence about a type of attack combined with log data about how the attack was executed in your environment will help you assess the potential impact of the attack and determine the appropriate level of resources to dedicate to mitigating and investigating the issue.

Combining Capabilities for Effective Threat Detection

Detecting and responding to attacks requires a combination of resources. You need detection mechanisms to scan large volumes of data looking for indicators of attacks; the ability to search logs using both exploratory and hypothesis-driven procedures; and you also need access to threat intelligence to provide additional context to what's captured in logs. The ability to automate detection, triaging, and responding are also crucial elements of effective cloud threat detection and response. So, let's go deeper and talk about hunting (Chapter 7).

IN THIS CHAPTER

- Identifying different types of threat hunting
- Ensuring effective log collection
- Learning from an example

Chapter 7
The Art of Cloud Threat Hunting

Hunting complements detection. Once you've identified an indicator of an attack, you need to dig into the details. Is that authentication failure a legitimate user mistyping their password? Or, is it an attacker trying to compromise someone else's account? Looking at an indicator in isolation often isn't enough to know for sure when you have a true positive indicator of an attack or when you're dealing with a benign event.

A-Hunting We Will Go

Threat hunting is the process of investigating security events using a hypothesis-driven exploratory analysis and investigation. Cloud threat hunts, as you may have guessed, focus on hunting threats in cloud environments. Cloud hunts entail deep dives into logs using more complicated logic than typically used for detection. With detection, you're willing to generate false positive indicators of attacks rather than miss a potential true attack indicator. Detection uses more lightweight pattern recognition to quickly find targets of interest. When you're hunting, however, you've decided to invest time and resources into investigating

what appears to be an actual attack, which can cause harm to the organization. There are a few different ways to approach hunts.

Strategic cloud hunts

A strategic cloud hunt looks at what adversaries do when they conduct attacks. These hunts tend to focus on a particular technology or platform, such as exfiltrating data from a cloud provider's object storage service or compromising the authentication process of an SaaS provider.

Event-driven hunts

Event-driven hunts take advantage of some malicious event that happened to someone else's system. For example, a technology vendor might have had proprietary information stolen using some form of a persistent threat. During event hunts, researchers gather as much information as possible to understand the attack, identify indicators of the attack, and in some cases, try to replicate the attack in a research and development environment.

Continuous cloud hunts

Continuous cloud hunts are ongoing operations running checks in your cloud and SaaS environments against all indicators of attacks. If some malicious activity is identified, then you can run mitigation processes.

Cloud Hunts Depend on Logs

If you've worked with logs in on-premises systems, you've probably seen how easy it is to control the level of detail captured in logs. When you shift to using cloud services, especially SaaS services, it becomes more challenging to capture log data.

One of the issues is that you need access to cloud provider's logs. These aren't always accessible to cloud users. In some cases, the amount of log data available depends on the licensing of a service.

EXAMPLE

For example, an enterprise license for a collaboration tool may provide for logging while the free version of the same product doesn't. Not only is this a problem because logs aren't available for some users, but an attacker can use this two-tiered approach

to logging to their advantage. An attacker could temporarily remove the license from a user, perform some malicious act using that user's account, and then restore the license. The user may never notice the difference, and no logs will be left detailing the malicious activity.

REMEMBER

Another thing to consider when using a PaaS or SaaS, is that there are limits to how long the vendor will keep logs. It's important to capture those logs into a security data lake before they're deleted by the cloud vendor, so you'll have what you need to hunt.

Logs are also a source of information for understanding how attacks proceed. Take, for example, an attack on Microsoft by a nation-state actor (see the nearby sidebar).

EXAMPLE

BEWARE THE MIDNIGHT BLIZZARD

Not long ago, APT29 (a Russian state-linked threat actor) compromised Microsoft in what became known as the Midnight Blizzard. The group managed to use common but simple techniques to obtain access to a cloud development environment owned and hosted by Microsoft. Using a variety of hacking techniques, they escalated their privilege and managed to move laterally into the production tenant of Microsoft. This allowed the attackers to access Microsoft mailboxes and from there, they exfiltrated data from Microsoft executives' mailboxes. Researchers at Mitiga studied available information on the incident and managed to understand the attackers' activities and the correlating logs associated with those activities. This provided the foundation for codifying logic to detect this type of attack. From there, the Mitiga team applied their newly derived logic against all of their clients who were using the same Microsoft Azure service to determine if any had been attacked using similar techniques.

IN THIS CHAPTER

- Knowing where to begin with an investigation
- Looking for answers and collecting evidence
- Having the right people in the right place at the right time
- Employing automation for speed, efficiency, and consistency

Chapter 8
Conducting Cloud Investigations

If you've determined that you've been the victim of a security breach, you need to respond. You need a plan and a team in place that can quickly begin to gather evidence about the breach, identify critical assets that may have been compromised, and notify stakeholders about the incident. The expansive scope of cloud infrastructure requires that much of the incident response tasks be automated to ensure the procedures are implemented efficiently, comprehensively, and consistently.

Understanding Where to Begin an Investigation

Cloud incident response, like on-premises incident response, begins with planning.

Having a team and tools in place

Enterprises need to have a team in place that's ready and capable of collecting evidence about a breach. Ideally, the team will have

tools and consolidated data sources in place, so they can quickly identify assets that may have been compromised and understand what activities or events took place on those devices that could have adversely effect the organization.

REMEMBER

When we talk about an investigation team in the cloud, we mean a team with a combination of DevOps and SecOps. DevOps teams have detailed knowledge of authorization, logging, and other services relevant to collecting forensic evidence. SecOps teams bring expertise in security practices that are needed to direct effective investigations.

Determining the scope of the attack

Along with detecting and identifying the type of security events, the first steps of incident response also include determining the scope of the breach. Was a single executive's SaaS account compromised in a spear phishing attack? Was there a large volume of documents with proprietary intellectual property exfiltrated? Incident response teams need to understand the extent of a breach in order to understand what needs to be done to contain the attack's impact.

This can be more challenging in the cloud because of constraints on visibility into cloud services. It's essential to collect logs from across the range of cloud services in use in your organization, so necessary information is available for cloud investigations.

Containing the attack

You may discover an attack long after the malicious actors have stolen valuable data, or you may discover signs of an attack while it's ongoing. In the latter case, it's especially important to execute steps to disrupt the attack and prevent more attacks from exploiting the same techniques and vulnerabilities.

REMEMBER

Containing an attack can require multiple steps, including:

- Disabling access to compromised assets, whether they're virtual machines or service accounts used with cloud providers
- Preventing exfiltration of data, including scanning data using data loss prevention techniques to identify sensitive information before it leaves your control

- Sharing details of the breach with the cloud provider and collecting additional information from them
- Reviewing cloud configurations that may have incorrect misconfigurations and, therefore, created vulnerabilities that could be exploited in an attack on your systems

REMEMBER

Containment operations will be subject to the shared security model of clouds, and some operations may require collaboration with cloud providers.

With the attack contained, the incident response team can begin to focus efforts on eradicating and recovering.

Eradicating and recovering

The goal of *containment* is to prevent further damage from an attack, while *eradication* focuses on removing vulnerabilities and malicious software that may be left on your systems. The goal of recovery is to return your systems and services to normal operating conditions.

TIP

After eradicating, it's important to monitor and watch for signs of further attack. This may require augmenting your set of monitoring and data collection tools, as well as expanding the set of log and other security-related data you collect. Also, consider additional tools for your team to help them identify vulnerabilities and detect attacks faster in the future.

TIP

Finally, learn what you can from the attack by conducting a post-incident review. This can provide valuable information about areas where you can improve your security controls. You may have opportunities to update procedures as well.

Knowing What Answers You're Looking For

Time is a resource in short supply when responding to an incident. In addition to the need to contain and eradicate malicious activity to prevent further damage, many enterprises are subject to regulations that require them to report significant security incidents in a timely manner. For example, in the United States,

the Security and Exchange Commission (SEC) requires publicly-traded companies to report material cybersecurity incidents within four days.

Finding chains of events

When you collect evidence of a security compromise, it often requires gathering information generated by multiple systems. Attacks are a sequence of events and collecting evidence is a process of reconstructing that chain of events.

EXAMPLE

For example:

1. An attacker may email a phishing lure to an executive. . .
2. Who unknowingly enters their credentials into a malicious site that looks just like their company's human resources (HR) SaaS. . .
3. Which allows the attacker to gain access to the HR service. . .
4. Where they elevate permissions on a service account used for extracting data to load a data warehouse. . .
5. And inject malicious software that behaves like a standard extraction, transformation, and load process. . .
6. Which exfiltrates employee data, including personally identifiable information (PII), to a server controlled by the attacker.

In this example scenario, you'd have to chain together events across email systems, authentication services, SaaS providers, as well as data warehouse workflows.

Automating the search for answers

While each attack has its own characteristics, certain patterns of attack can be detected automatically — if you know what to look for. This is where experience with security investigations combined with automated tools for pattern detection can make the difference between finding evidence quickly and missing some important link in the chain of events.

TIP

Use cloud investigation tools with comprehensive catalogs of pattern detection rules to improve your ability to analyze large volumes of diverse log data without risking missing something because humans wouldn't be able to completely analyze such volumes in the time available to them.

Collecting the Evidence, All the Evidence

Much of the evidence in a cloud investigation comes from logs. Some of those logs may be from applications that you've developed in-house and run on-premises, but a majority of the data comes from logs generated by cloud providers.

IaaS and PaaS logs

Consider the sources of logs generated when you use IaaS and PaaS services in a public cloud provider. They include:

- Object storage logs, such as AWS S3
- Event-driven processing logs, such as AWS Lambda
- Virtual machine services, such as AWS EC2
- Relational database services, such as AWS RDS

SaaS service logs

In addition, enterprises use a variety of SaaS services that generate logs useful for cloud investigations. These include:

- Salesforce, for customer relationship management
- Atlassian, for collaboration
- GitLab, software for version control
- Snowflake, for data analytics

Other corporate service logs

Other corporate services that create logs that can be collected for cloud investigations include:

- Azure Active Directory, for directory services
- Microsoft Office 365, for collaboration
- Google Workspace, for collaboration
- Okta, for identity management

VARIETY — THE SPICE OF LIFE?

Log data is considered semi-structured data. There's some structure, such as timestamps; and standardized log levels, such as information, warning, and error. However, much of the valuable content doesn't have a fixed format. A log line from AWS CloudTrail will have a different format than a log line from Google Cloud Logging.

Now, multiply those differences by all the other log sources that you may need to integrate. It's imperative to have tools that can collect, analyze, and integrate these sources, so that you can have access to all of the evidence you need for a cloud investigation.

From these examples, you can see that log collection for cloud investigations requires gathering and integrating a variety of different kinds of data.

Having the Right People in the Right Place at the Right Time

Responding to a cloud security incident requires the skills and authority of people from across an organization. Of course, information security professionals are required, but that's just the beginning of the expertise you need to tap to address all the requirements that arise during a cloud investigation.

Security and IT operations personnel

An incident response is typically led by an incident response manager, who's responsible for the overall process and communicating with stakeholders. Security analysts and engineers have the skills to investigate, collect evidence, and provide tactical direction during the course of the investigation. System administrators, such as network admins, database admins, and application admins bring domain expertise in their own areas.

Other key stakeholders

While security and IT professionals focus on the technical aspects of a security breach, others need to attend to broader organizational issues that arise.

Compliance professionals can help with ensuring incident response activities, including addressing regulation requirements, such as reporting. Legal professionals may also be needed to help determine appropriate communications around notifications.

A team of executives, including the chief information security officer (CISO), chief information officer (CIO), and chief executive officer (CEO) may be needed as well, especially with a significant breach.

Note that in the case of material breaches where internal staff and the public must be notified, human resources and communications professionals may support the executive team as well.

REMEMBER

Planning who'll be involved in the incident response is essential. Knowing who's involved and their roles and responsibilities need to be established as part of overall security planning and operations in an organization. For example, DevOps and cloud teams have the admin access to cloud infrastructure that will be needed to respond to an incident, while SecOps team members will understand what needs to be done to contain the attack.

Keeping Up: Automation is Key

A cloud investigation has many moving parts. Teams are evaluating indicators of attack, assessing the scope of a breach, collecting evidence, following initial leads, and filtering false, irrelevant details. Ideally, these teams are taking advantage of the tools and processes that were put in place as part of security planning and implementation activities. This preparation means there are integrated data stores of consolidated logs as well as query and analysis tools to isolate evidence and help the team formulate an understanding of the attack.

REMEMBER

Ensuring efficient and effective investigations requires automation because there will be:

- Many logs to collect, process, and integrate.
- A wide range of possible attack patterns will have to be constantly applied to data to help detect attacks as early as possible.
- Many questions the incident response team will have that will require support for ad hoc querying over logs data.
- Reporting requirements that will need details on the scope of the attack and the activities undertaken in response to the attack.

Keeping up with the pace at which malicious actors come up with new attacks, the speed at which services generate logs that you need to analyze, and the demands on rapid reporting and transparency around breaches requires well-choreographed automation.

IN THIS CHAPTER

- Remembering why cloud investigations are different
- Building the muscles of cloud-threat readiness
- Getting a handle on cloud threat detection
- Enhancing your resilience with cloud investigation and response

Chapter 9
Ten Truths About Cloud Investigation

This chapter discusses some of the big takeaways from this book, and highlights key skills, processes, and technologies needed to execute effective and efficient cloud investigations.

Cloud Investigations are Different Than On-Premises Investigations

Cloud investigations entail different kinds of threats and attack models than those found in on-premises investigations. Cloud investigations are different in their scale, dynamism, and complexity. Add to those challenges an expertise gap among SecOps teams that are new to cloud technologies.

A further difference is the way attacks are carried out in clouds, particularly in SaaS applications. Rather than target perimeter defenses, attackers focus on identities and gaining access by authenticating as legitimate users.

Cloud investigations, as explained in this guide, are designed to build organizational resilience into an increasing complex security environment.

Digital Transformations have Ripple Effects on Security

Digital transformations can be immensely beneficial for enterprises, but they have ripple effects throughout the organization. Some of these effects are intentional, such as changing a culture to be more adaptive and open to change, but other side effects are inevitable and unplanned, like the ways that transformation impacts your attack surface.

EXAMPLE

For example, adopting SaaS services rather than implementing equivalent operations on-premises can be more efficient and cost effective; however, they introduce new security considerations. Using SaaS services means you're engaging in a shared security model with the SaaS provider. Tools and techniques that you used for on-premises security practices, such as analyzing operating system logs and examining memory dumps aren't available with SaaS services and must be re-envisioned.

Multi-Cloud and Multi-SaaS are the New Normal

The way you deliver IT services changes with the technologies available to you. Centralized mainframe infrastructure and distributed client-server models of computing now compete with cloud-based services. Enterprises adopt cloud-based services when they bring cost advantages, the ability to adapt to changing market conditions, and organizational demands.

REMEMBER

There's no single way to employ cloud computing, but there are three dominant models:

- **IaaS cloud providers** offer infrastructure related to computing, storage, and networking

- **PaaS services** include developer and database services that are ideal for groups who want to manage software infrastructure while leaving hardware and the bulk of networking considerations to a partner
- **SaaS providers** focus on delivering services while taking care of much of the operating software and hardware management

Today, many organizations use a mix of all of these. Turning to various modes of cloud computing has also led to shifts in how you investigate and respond to breaches.

Shared Responsibility Complicates Cloud Investigation

When you choose a cloud provider, you're also choosing a security partner. The responsibility for securing information technology requires coordination between cloud providers and cloud users.

Cloud providers are responsible for the physical security of their data centers, providing secure operating systems and other software within their environment, and providing their customers with tools for additional controls, such as managing permissions to access and use cloud resources in a customer's account.

Cloud customers also have a vital and broad range of security responsibilities, including: protecting sensitive data, complying with regulations, defining and managing user identities and roles, monitoring services, and having plans and procedures in place to respond to security incidents.

REMEMBER

Shared responsibility extends to cloud investigations. Cloud providers need to make log data accessible to customers. Cloud customers should collect, store, and integrate log data from IaaS, PaaS, and SaaS providers in their own security data lakes. Log data is essential information for ensuring effective security. Security data lakes and cloud investigation systems help build the resilience of an organization because they capture data and provide the tools you need to effectively respond to security incidents.

Preparation is Essential to Cloud Investigation

Cloud investigations depend on access to data, which is essentially the raw material of a cloud investigation. Imagine a manufacturer that didn't have the raw material on hand to produce products. They wouldn't be in business very long. Similarly, you can't respond to security incidents with a last-minute scramble to collect data, organize it, and think about how to query it to answer key questions.


TIP

As you plan for building your cloud investigation capabilities, consider what data you'll need, determine the full array of cloud vendors you'll have to work with, understand what data is available and for how long, plan to collect and store that data for extended periods, and consider the analysis and investigation tools you'll need to have in place to build both a team and a set of processes that are resilient and adaptable.

Employ Security Data Lakes to Feed Cloud Investigations

A cloud security data lake is an essential requirement for effective cloud investigations for three reasons:

- Cloud security data lakes enable you to collect and store data you deem important for as long as you want to store it. Cloud providers may have short retention periods or require long lead times to respond to requests for log data.
- With a cloud security data lake, you can have all your security data in a single, fully rationalized location. This allows for easier analysis.
- Data lakes are a well-developed architecture pattern with mature tools for building, managing, and monitoring the data store. There are also a variety of scalable tools for analyzing data in data lakes.

You can't anticipate all of the ways malicious actors could attack your cloud environments and systems. But by having a

cloud security data lake, you increase your ability to respond to both known and unanticipated methods of attack by maintaining vital data.

Detect Threats Early and Often

Enterprises face a variety of risks that vary with the technologies they use and the practices they employ to implement those technologies. Attackers are opportunistic, taking advantage of vulnerabilities in software, configurations, and even people where they can find them. One successful phishing lure can leave an administrator account on an SaaS service open to an attacker.

Security researchers and professionals understand how to identify indicators of attack. They have codified these patterns and built systems for analyzing log data from multiple systems to monitor activities and detect threats.

REMEMBER

The ability to detect threats early depends on knowing indicators of attack as well as having data available to analyze. A cloud investigation system is built on interdependent components, such as detection mechanisms and security data lakes, which house and integrate data from multiple applications and cloud services.

Be Ready to Respond to Incidents

In addition to being able to detect security incidents, it's imperative to have a plan in place for responding to such attacks. This also requires preparation and having the right people, tools, and procedures in place before an incident occurs. This means having in place capabilities to:

- Collect and retain forensic evidence, such as audit logs and system activity logs
- Centralize forensic data in a purpose-built security data lake
- Employ tools optimized for cloud forensic analysis, not simply alerting
- Develop and foster cloud response expertise to complement existing security skills in your SecOps team

Responding to incidents is an organizational skill that can enable an enterprise to respond to an attack and reduce the adverse impact on the organization.

Automation is Key to Cloud Investigations

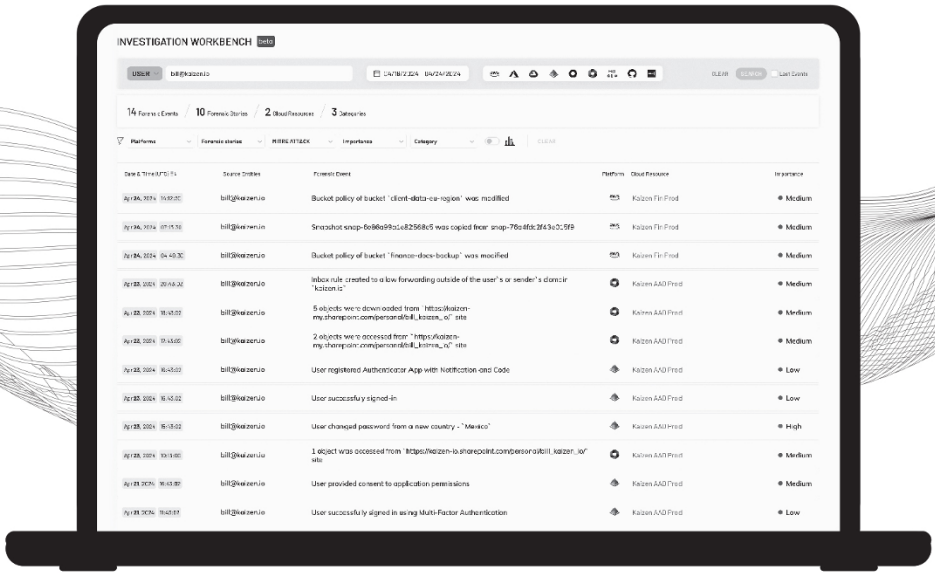
Cloud investigations involve multiple people in a variety of roles performing a wide range of tasks. Some of those tasks will become more challenging as the amount of data or number of systems involved grows. Analyzing a few dozen rows of data in a spreadsheet can be done by a single individual in a short period of time. Collecting, integrating, and analyzing petabytes of security log data requires targeted tools and automated procedures to produce the kind of results needed in the shortest amount of time.

Effective Cloud Investigations Enhance Resilience

Perhaps the most significant takeaway of this guide is the importance of cloud investigation to resilience. Resilience of information systems is the ability of those systems to continue to function even under adverse conditions. Organizational resilience reflects the same meaning at a business level.

Monitoring and detecting cloud attacks and having a response plan and team in place to address them enhances your resilience. Effective cloud investigations complement other practices that enhance cyber resilience, such as leveraging cloud technologies for scalability and elasticity, fostering a culture of security awareness, and developing and testing business continuity plans to allow for continued operations during disruptions. Together, cloud threat detection, investigation, and response close a vital cloud security gap — enabling and advancing modern enterprises.

Supercharging SOC teams for the cloud era



The only complete solution for cloud threat detection, investigation and response

Broad coverage

Enabling full visibility across clouds and SaaS

Fast answers

Automating investigation to accelerate response 70x

Rich context

Connecting the dots for better threat detection

Specialized teams

Unlimited access to experts elevating SOC cloud capabilities

MITIGA

By investigators, for investigators

mitiga.io

Root out and respond to cloud threats

Cloud threat detection, investigation, and response aren't simply about using traditional cyber methods in a new environment. They're crucial modern SecOps capabilities that require different processes, tooling, and expertise. At a time when most data breaches occur in the cloud, they're a must-have for any SOC team.

Cloud Threat Detection, Investigation & Response For Dummies is your guide to acting on cloud threats. Dive in to discover how to lower cloud risk, build resilience, and save resources.

Inside...

- Breaking down cloud investigation
- How to detect threats early and often
- The limits of shared responsibility
- Preparing people, processes, and tech
- How data lakes transform cloud posture
- Tips for triaging cloud incidents
- Skillsets that lower breach impact

ISBN: 978-1-394-28143-5
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.