Modernizing SecOps for Cloud

Version 2.0

Released: February 5, 2024

Securosis, L.L.C. 515 E. Carefree Highway Suite #766 Phoenix, AZ 85085 **T** 602-412-3051 info@securosis.com www.securosis.com

Author’s Note

The content in this report was developed independently of any sponsors. It is based on material originally posted on the Security Boulevard site but has been enhanced, reviewed, and professionally edited.

Special thanks to Chris Pepper for editing and content support.

Licensed by FireMon

FireMon Cloud Defense is a real-time cloud security operations platform that natively monitors your cloud deployments. Changes in your cloud environments instantly trigger a suite of configuration, security, and compliance assessments to reduce risk, monitor activity, and detect potential malicious actions. Cloud Defense generates enriched alerts to help discern external attacks, malicious insiders, or innocent mistakes. FireMon Cloud Defense eliminates the need for static credentials or long-term permissions with just-in-time IAM approvals, out-of-band visibility, and granular session restrictions for responders and teams. Learn more and sign up for a lifetime of free CSPM at https://defense.firemon.cloud.

Copyright

Table of Contents

Modernizing SecOps for Cloud

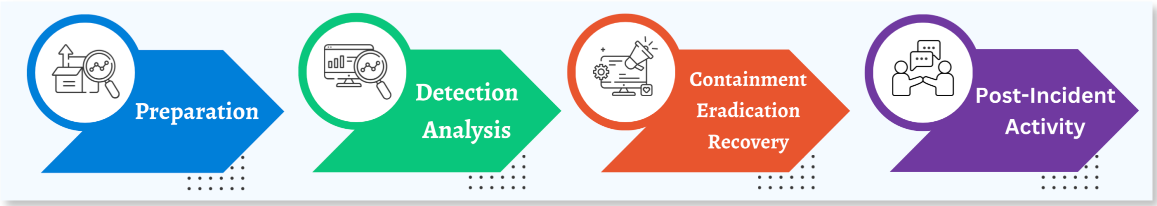
Security Operations, SecOps for short, has been one of the more difficult security domains to modernize for cloud. It requires a combination of new subject matter expertise, new technologies, process updates, and even a slightly different mindset. Cloud impacts SecOps in ways both obvious and subtle, and because most organizations still have datacenters and offices, teams need to add new skills and update operations while still supporting everything already on their plates. It's a daunting challenge, but one that can be made much easier to tackle by distilling down, into the core of how cloud changes things, and taking lessons from the successes of early adopters.

This paper will detail the impact of cloud on SecOps, review the core technical capabilities needed to respond, and highlight techniques for successfully modernizing security operations to support cloud operations. We will finish up with example processes you can use as templates for your own operations.

Defining SecOps for Cloud

There isn't one universal definition of SecOps, but it typically refers to detecting and responding to potential security issues like exposures or attacks, which bridge from security into IT operations. In some organizations the SecOps team is a different name for an incident response team, but others take a broader view, so SecOps may cover any activities where security affects and integrates with IT operations. For our purposes we will limit ourselves to the cycle of monitor, detect & analyze, communicate, and respond & remediate.

We've based this on a combination of the NIST Cybersecurity Framework (CSF) and the NIST incident response cycle. NIST CSF includes Identify, Protect, Detect, Respond, and Recover. It's meant to cover the entirety of information security domains and is thus broader than our focus. The NIST incident response lifecycle includes Preparation, Detection and Analysis, Containment, Eradication and Recovery, and Post-Incident Activity.



We aren't proposing a new definition of SecOps, but cherry-picked phases that work well to explain the key areas we need to adapt for cloud. We also aren't focused exclusively on responding to attacks — we include managing incidents, vulnerabilities, and misconfigurations — because these tend to overlap more in cloud, as we will explain below.

How Cloud Impacts SecOps

At a high level there are three key ways cloud impacts the entire range of security operations:

- **Cloud operations and management are decentralized.** Different teams not only manage their own applications stacks, but their own infrastructure stacks. These are spread across multiple cloud deployments or even providers. Much of security operations historically relied on centralized management and consolidated infrastructure which don't exist in cloud.
- **Administrative functions are consolidated into unified consoles which run on the Internet.** While individual deployments operate in their own decentralized cloud environments, all the administrative functions to manage them are consolidated into a single unified management plane for each provider. This management plane is on the Internet, controlling all infrastructure down to the (virtual) wiring of the virtual networks; and we access it with a username, password, and perhaps MFA. These management planes are ripe targets for attackers, and they don't need to break Amazon, Microsoft, or Google — all they need to do is steal the right credentials from one admin.
- **Most resources can be configured to be on the Internet.** It's called "public cloud" for a reason, and nearly any resource you can create at any provider can be configured to access or be accessed via the Internet. This is a radical departure from building and deploying resources in datacenters.

This combination of decentralized operations with a central management plane on the Internet, capable of exposing any and all assets to the Internet, forces a shift in SecOps focus and priorities. The situation isn't *worse* than SecOps in a datacenter — we also gain advantages like better centralized visibility and more agile response capabilities — but it is different. Attackers are more likely to use stolen cloud credentials and API calls to expose data directly via the management plane without ever creating a malicious packet on a monitored network.

> *"This combination of decentralized operations with a central management plane on the Internet, capable of exposing any and all assets to the Internet, forces a shift in SecOps focus and priorities."*

Understanding and Embracing SecOps for Cloud

This paper will dig deeper into some technical aspects of cloud that affect SecOps, how to expand core capabilities to ensure proper coverage, and then how to adapt SecOps processes across the incident response cycle. Key questions we will address include:

- **Monitor:** What telemetry sources does cloud add, and what are the best ways to collect and manage them?
- **Detect and Analyze:** What new kinds of detectors and activities are needed to identify cloud security issues? How do the analysis process and priorities change for cloud?
- **Communicate:** How do we organize and communicate issues and further response?
- **Respond and Remediate:** Who handles response in cloud? How do we assure access and coordination? Who decides on and implements remediation?

Our focus will be on practical approaches which don't require you to suddenly become a cloud unicorn. They can be integrated over time and don't require sudden radical re-engineering of operations. Existing processes and skills are still completely relevant, because cloud incidents easily spill into traditional areas of SecOps. We will show you how to modernize, expand, and integrate SecOps to improve your processes for cloud.

Building Core Capabilities to Modernize SecOps for Cloud

Our first section highlighted the top ways cloud impacts security operations, but we stuck to a high level and avoided getting into specific mechanics. Diving a little deeper, some additional characteristics of cloud directly impact SecOps and can guide how we expand our core capabilities to support program modernization.

Let's dig into the details to identify where we should look at making technology changes to support cloud-modernized processes.

Cloud Disruptions

The best way to think about cloud computing is as a completely alien technology on the inside which looks the same on the outside. Yes, cloud is built on the same technical building blocks as your own datacenters, and many of the things we build in cloud look the same on the surface. But the layers of abstraction in the middle create something wholly original which works completely differently once you scratch the surface.

These create behavioral and structural differences which guide how we build our SecOps support infrastructure and capabilities:

- **Velocity:** Cloud deployments change continuously. And we mean ***continuously.*** Resources are commonly created, destroyed, and reconfigured every few minutes, if not seconds. That server with that IP address might not be the server that had that IP address tied to an attack indicator in the logs. By the time an admin or responder sees an alert that resource might no longer exist, or look completely different than it did when the issue was detected. However fast you think cloud moves, it moves faster.
- **Distribution:** An average small or mid-sized organization early in its cloud journey can typically have 10-15 different cloud deployments (our term, which includes provider-specific environments like AWS accounts, Azure subscriptions, and Google projects). Resources are scattered across these deployments — some connected and some isolated. Larger organizations may routinely leverage hundreds or thousands of deployments, managed by dozens or hundreds of different teams. While these all share a management plane; they don't automatically share a single top-down view, security telemetry plane, or security and

management tooling. No central team manages everything, able to distribute core architectural and practical knowledge across teams.

- **Identity is the perimeter:** Attackers don't need to break into servers and networks; they can use stolen and exposed credentials to directly access the management plane and re-wire those servers, networks, and more with a few API calls or clicks in a console. When an attacker steals cloud credentials you can't stop them with a firewall or by shutting down access to a server.

- **The Internet is always a click away:** Public cloud is a place to build things when you… might want to make them public. While most providers default resources to being private, nearly all resources can be made public with minimal effort. This is an inherent characteristic of public cloud. Combined with the velocity of cloud, this means the potential for instantaneous public exposure is quite high.

- **Cloud providers update constantly:** The major cloud providers each support at least 200 different services. They perform multiple feature updates across each portfolio on a daily basis. Customers get to choose when and where they use some of these features, but they don't get to choose when the provider enables them for all customers.

- **Knowledge is local:** The average cloud application stack uses dozens of a cloud provider's different services, all using tuned configurations. The entire stack, from front end to network configuration, can be built and customized to meet the needs of a single application. This results in greater contextual application knowledge with the local team, but lower knowledge within central teams.

Things move fast and they are highly distributed, locally managed, and on the Internet. Contrast this with a datacenter where change is slower, more centralized, and behind a perimeter. Once you internalize that, understanding how to update operational security processes becomes more straightforward.

From Core Principles to Core Capabilities

Now that we've narrowed down the general impacts of cloud — at least major ones which affect security — we can distill out some guiding principles to help determine the core technical capabilities we need to support SecOps:

- **Operate in real time:** SecOps has never been a domain for the tardy, but the speed of change of cloud combined with the proximity of the Internet, mean issues may need to be detected and managed within minutes or less — not hours. Speed matters, and tooling needs to run as close to real time as possible.

- **Treat configuration changes as indicators of compromise (IoCs):** When an attacker compromises credentials they use their management plane access to execute attack activity. This is the trigger for malicious configuration change — not exploitation of zero-day cloud provider vulnerabilities. The line between a misconfiguration and an attack comes down to the intent of the credential holder. Tools need to track configurations and identify misconfigurations, while the SecOps team needs to treat misconfigurations as potential indicators of attack.

- **Collaborate:** Local teams — those app and cloud teams that manage their own deployments — have the knowledge to know whether something is a mistake, an attack, or a required configuration. They also know the best ways to remediate issues without breaking their stacks. As a configuration change example, a security team might detect a new public S3 bucket or Azure Blob. The cloud logs let them know who made the change — but how do they determine whether it was a mistake, an attack using stolen credentials, or a necessary update for that application? Security won't have the answers, but the answer is a quick ChatOps message, call, or email away.
- **Focus on IAM first:** The vast majority of cloud-native attacks involve IAM failures: lost, stolen, or exposed credentials. Yes, attacker still compromise vulnerabilities on exposed resources, but we know how to deal with hacked servers and networks. Once an attacker gets their hands on cloud credentials, they effectively break out of the matrix and can rewire your infrastructure. SecOps needs to shift focus, starting with identity-related issues and activities, with playbooks and tools to support them.
- **Optimize your feeds and speeds:** Cloud platforms bring a new range of security telemetry sources. These can be an incredible boon for security due to their broad and deep coverage of nearly all administrative actions; but benefitting requires knowing which feeds to collect, the difference between saved logs and real-time events, when to use which, and how to integrate them into tooling without introducing delays which force responders to work with stale data.
- **Automate:** SecOps should adopt automation to support and speed up processes. For example response playbooks can be highly automated to prioritize and filter, enrich data, communicate with the cloud team, run default queries, and even automate some containment actions. Humans remain in the loop — the automation is just there to provide a speed and efficiency boost.

This isn't an exhaustive list of everything possible. We stayed at a high level, but understanding the impact of cloud helps see how these core capabilities allow a SecOps team to operate more effectively and efficiently.

ChatOps like Slack/Teams is one of the most effective tools for improving SecOps collaboration between teams.

Keys to Adapting SecOps Processes for Cloud

Now that we've modernized core SecOps capabilities, we can start adapting processes. As a reminder, these changes focus on the core success principles for cloud:

- We operate as close to real-time as possible when necessary. While not everything needs to be handled immediately, some things definitely can't wait.
- Security collaborates across teams, also with real-time capability (for when needed). Emailing spreadsheets is not the way.
- We treat misconfiguration as potential adversarial activity until proven otherwise.
- Everything focuses on IAM first: the gateway to the management plane.

Adapt, Don't Replace

One key point mentioned briefly earlier is that our objective isn't to build an entirely new program. Unlike many other areas of security, it can be very useful to keep cloud security operations aligned with existing security operations. Unless your organization is pure cloud, many issues and incidents span both cloud and traditional infrastructure.

For example if you detect a misconfiguration that is then tied to lost/stolen credentials, the investigation and response expand to cover where they originated. This could be a developer's laptop (time for that old-school malware/phishing investigation) or a server in the datacenter (back to network and server forensics).

If your team is big enough, you will likely want some dedicated cloud responders who work shoulder-to-shoulder with the non-cloud team. This doesn't mean you need to shoehorn everyone into the same toolset, but depending on what you already use it might make sense to set up some parallel tooling, if existing tools can't satisfy your integration and speed requirements for cloud.

For example some SIEMs cannot send alerts faster than every 15 minutes, or aren't equipped to handle real-time feeds (they are file-based rather than event-based). Those SIEMs can still be incredibly valuable for analysis and hunting, but may need to be supplemented with something like a Cloud Detection and Response (CDR) tool designed for real-time cloud threat detection. The CDR extends existing capabilities.

Extending Process

The same holds true for processes. To the greatest degree possible we want to adapt and extend instead of replace. This is usually possible by integrating the principles we have been discussing. Let's take the SecOps phases tuned for cloud and review specific options for adapting them for cloud:

Monitor

Expand the monitoring process beyond logs to include the cloud platform, service, and resource configurations (ideally with a real-time inventory). You will want to feed configuration changes into detection and analysis, since a misconfiguration or policy violation might indicate an attack. Monitoring should also expand to cover real-time events from your cloud platform: both activity and events from the cloud provider's security tooling (*e.g.,* GuardDuty, Defender for Cloud, or the Security Command Center).

Detect and Analyze

Detection engineering expands to include cloud native threats associated with the management plane: both specific actions and outcomes (configurations). Detectors need to be tuned for different environments (*e.g.,* dev vs. prod) to improve the signal-to-noise ratio. On the analysis side cloud playbooks should always start with identity and the management plane, before dropping into image forensics and network activity. Analysis should also emphasize the importance of identifying external exposures to the Internet and untrusted cloud accounts.

Communicate

Improving communication between security and operational teams, and even development, is the single most impactful change for modernizing SecOps for cloud. ChatOps has been shown to be one of the most effective means of achieving this thanks to its support for person-to-person and automated messaging. Issues (filtered and prioritized) can be communicated directly to the responsible team for evaluation — and to determine whether it was intentional, accidental, or part of an attack. Then SecOps can validate, create an exemption, or trigger more in-depth response. Lower-priority issues can simply feed into a ticketing system; not everything needs to be communicated immediately.

Respond and Remediate

Two key changes can dramatically improve the response process. ChatOps can be used to coordinate response between SecOps and the team which owns the deployment. This expedites effective response because the cloud team knows what their stack should look like, and how to make changes while reducing impact; while SecOps handles threat hunting, containment, and attacker eradication. The second key is to ensure SecOps has emergency access to all cloud deployments in case a critical response is needed when the cloud team isn't available. You don't want responders running around trying to wake someone up to trigger a change when a customer database is exposed to the Internet.

Two Practical Examples of Modern Cloud SecOps

We started by detailing the major ways cloud affects SecOps, before delving into updating core capabilities and processes to better manage cloud. Now it's time to show practical examples, both of which we have implemented in the real world.

Example 1: Misconfiguration Remediation

Your tooling finds an S3 bucket is open to public Internet access. This is in an account which does have other public buckets, but this one is unexpected. It's similar to finding a new open file share or SharePoint site which isn't a clear policy violation but is definitely concerning, especially since data may be exposed to the Internet.

Your objective is to detect, analyze, and respond as quickly as possible:

Monitor, Detect, and Analyze

- By monitoring resource configurations in real time (using CSPM or an equivalent) you detect the possible misconfiguration the moment it is opened to public access.
- Your tooling enriches the detected misconfiguration with the before state, after state, who made the change, and the history of that bucket.

Communicate

- This alert routes to the SecOps team via Slack because anything newly public is high or critical severity. It also creates a JIRA ticket for tracking.
- Simultaneously the alert routes to the cloud team who manages that AWS account. All high and critical issues route to the owning team, while medium and below just create backlog tickets.
- Alice, on the cloud team, recognizes that the API call was made using a role assigned to a contractor. She looks at the bucket and sees it does not yet contain sensitive data.

Respond and Remediate

- Alice fixes the bucket policy and has a stern conversation with the contractor.
- The SecOps tooling recognizes the remediation, and clears the alert and the ticket.

- Because the issue was of high severity, SecOps reviews the configuration change history and double checks to make sure no data was exposed.

The issue is detected and remediated in about 15 minutes.

This example shows the value of our core principles. The exposure was detected in real time. It was communicated to both SecOps and the team who owned the environment. Based on the IAM fields of the API call the cloud team recognized the source of the exposure and was able to remediate this issue before it became a serious problem.

Example 2: Incident Response

You just detected a new snapshot of a customer database unexpectedly shared to another account at 3 am. How long has it been there? Is the data sensitive? Is that one of your trusted accounts, or is it an external account under control of an attacker? Was this a deliberate change, an accident, or an attack? This is the cloud equivalent of realizing a database backup was open to the Internet and possibly exported externally.

The process here is similar, but this scenario shifts gear to deal with activity which is more indicative of an attack:

Monitor and Detect

- The monitoring system detects the cross-account sharing API call.
- Your tooling evaluates the configuration of the snapshot. It looks up the shared account ID and sets the issue as critical, since the ID is not known or on an approved list.
- This creates an issue, which is enriched with details of the API call including the IAM entity. In this case it's an IAM user account called "BackupManager".

Analyze and Communicate

- The alert routes to the SecOps team and the cloud team who owns the account.
- Since it's 3 am, the SecOps team initiates their off-hours playbook for a potential customer data exposure.
- SecOps logs into their response tool for further investigation. They see the API call history of BackupManager, and note that this activity occurred at an unusual time, from a new IP address, with a different user agent than normal.
- SecOps also determines the other AWS account is not a known corporate account, and they submit an abuse notice to Amazon via the AWS support portal.
- Our team's responder reviews the current resource configuration of the database in their inventory system and determines that this is a production account with production data, based on the database's name and tags.

Respond and Remediate

- The responder is unable to contact anyone from that cloud account's team due to the late hour, and works through the playbook for an emergency response.
- SecOps triggers their break-glass access, which requires Security manager approval within their tooling. The responder is given a 30 minutes session to access the account.
- The responder disables the sharing and triggers their IAM containment automation script. This locks use of BackupManager to its single approved corporate IP address.
- The cloud SecOps responder engages with colleagues to investigate how the BackupManager credentials leaked (*e.g.,* a compromised datacenter server).
- With the immediate threat contained, SecOps arranges to collaborate with the cloud team when they get to work in the morning for a permanent fix.

This example relies less on communication and more on automation and responder access. During work hours you might have the cloud account team handle the remediation in coordination with SecOps; but because this was a potential critical exposure security used their playbooks, emergency access, and automation instead. In case you didn't know, sharing snapshots to accounts under attacker control is a common data exfiltration technique.

These examples showcase how to build a modern SecOps process for the most common security operations scenarios: remediating a misconfiguration or vulnerability, and responding to an incident. In both cases we are able to detect, respond, and remediate the issue within minutes. We enabled rapid detection, information enrichment, and communications across silos; all this helps to engage the most knowledgeable team members, and enables supportive automation.

Hopefully you noticed the key differences from how many organizations run existing operations. Assessments are continuous and real-time; we don't rely on daily or even hourly scans which can leave resources publicly exposed for longer windows. We treat misconfigurations as potential attacks, not just mistakes to backlog. Activity (log) data is also timely, and SecOps doesn't rely on slow feeds which force them to operate 15 minutes or more behind attackers. Automated enrichment and routing via ChatOps reduces the negative impact of decentralization by engaging teams across silos, instead of security emailing out spreadsheets of vulnerabilities. Responders have the access and automation to make changes during emergencies and larger incidents, while the teams who own cloud deployments handle most issues themselves.

Through modernizing tools and processes we manage the biggest security challenges of cloud: decentralization, administration via the Internet, and every resource being a few clicks away from becoming public. Using our core principles, tooling and process recommendations, and practical examples, should help any SecOps team improve cloud security operations

About the Analyst

Rich Mogull, Researcher and CEO

Rich has twenty years experience in information security, physical security, and risk management. These days he specializes in cloud security and DevSecOps, having starting working hands-on in cloud nearly 10 years ago. He is also the principle designer of the Cloud Security Alliance training class, primary author of the latest version of the CSA Security Guidance, and actively works on developing hands-on cloud security techniques. Prior to founding Securosis, Rich was a Research Vice President at Gartner on the security team. Prior to his seven years at Gartner, Rich worked as an independent consultant, web application developer, software development manager at the University of Colorado, and systems and network administrator.

Rich is the Security Editor of TidBITS and a frequent contributor to industry publications. He is a frequent industry speaker at events including the RSA Security Conference, Black Hat, and DefCon, and has spoken on every continent except Antarctica (where he's happy to speak for free — assuming travel is covered).

About Securosis

Securosis, LLC is an independent research and analysis firm dedicated to thought leadership, objectivity, and transparency. Our analysts have all held executive level positions and are dedicated to providing high-value, pragmatic advisory services. Our services include:

- **Primary research publishing:** We currently release the vast majority of our research for free through our blog, and archive it in our Research Library. Most of these research documents can be sponsored for distribution on an annual basis. All published materials and presentations meet our strict objectivity requirements and conform to our Totally Transparent Research policy.

- **Cloud Security Training and Advisory, and Technical Services:** Securosis built the Cloud Security Alliance's CCSK and Advanced Cloud Security Practitioner training programs. We also provide custom training tuned to your needs. Securosis is a premier Cloud Security Alliance Training Partner, and provides in-depth strategic and technical assessments and advisory services. We also support a limited number of members in our Cloud Security Coaching program.

- **Retainer services for vendors:** Although we accept briefings from anyone, some vendors opt for a tighter ongoing relationship. We offer a number of flexible retainer packages. Services available as part of a retainer package include market and product analysis and strategy, technology guidance, product evaluation, and merger and acquisition assessment. Even with paid clients we maintain our strict objectivity and confidentiality requirements.

- **External speaking and editorial:** Securosis researchers frequently speak at industry events, make online presentations, and write and/or speak for a variety of publications and media.

- **Other expert services:** Securosis researchers are available for other services as well, including Strategic Advisory Days, Strategy Consulting engagements, and Investor Services. These tend to be customized to meet a client's particular requirements.

Our clients range from stealth startups to some of the best known technology vendors and end users, including large financial institutions, institutional investors, mid-sized enterprises, and major security vendors.