THE /555 GUIDE

# FOR CISOS

**Better, faster threat detection in the cloud**

sysdig.com/**555**

sysdig SECURE EVERY SECOND.

The Sysdig **555 Benchmark for Cloud Detection and Response** sets the standard for operating securely in the cloud. We have found that on average, cloud attacks go from initial network access to business impact in 10 minutes. 555 challenges organizations to detect threats within five seconds, correlate and triage data within five minutes, and then respond within five minutes.

This benchmark is supported by evidence presented in the Sysdig Threat Research Team's (TRT) **2023 Global Cloud Threat Report**. The team found that cloud attacks are increasing in speed and sophistication, spurred by the malicious use of automation techniques and AI capabilities. For example, as reported in the **SCARLETEEL** cloud attack campaign discovered by TRT in July 2023, attackers took less than four minutes to steal proprietary data from their victims.

Legacy security tools are trying to keep pace, but can only support a fraction of today's security problems. They were built to secure on-premises environments where attackers take several days or weeks to move through the kill chain. Organizations must have tools and processes designed for the dynamic nature of cloud-native environments. A successful cloud security program will develop from the orchestration of the right people, processes, and tools. **There is an incredible business value in a security team that drives organizational resilience aligned with business strategies and initiatives.**

# Table of Contents

Breaches are incredibly painful to bear at the executive level, but maturing your SOC to the point of a 10-minute response will reduce the chance that you feel that pain. Paired with **The 555 Guide for Cloud Security Practitioners**, this guide will support you and your organization achieve faster cloud threat detection and response by providing prescriptive guidance and actionable next steps. **This guide will tell you where and how to mature your cloud security operations, and get you on the same page with your practitioners through shared language and operational direction.** Simultaneously, you will improve your organization's operational resiliency and reduce the burden, stress, and fatigue of incident response across your security teams.

Even with so many tools, platforms, and dashboards claiming to solve your security problems, it is ultimately your team's expertise, capabilities, and preparedness that will save you in the event of a real attack. With threat actors increasingly enhancing and improving their techniques, Sysdig is collaborating with organizations to level up and be prepared for modern cloud security risks and attacks.

Through the use of innovative and adaptive tooling and automation, cloud risk can be addressed proactively. This guide will help you get there.

Imagine the material implications for every hour or day an attacker has access to your enterprise network beyond that first ten minutes. Depending on an organization's size and industry, **the cost of unplanned downtime can vary between $138,000 and $540,000 per hour.** That means a critical service outage spanning the length of an average workday could cost a business upwards of $5M during recovery.

# Bring a fresh perspective

**You can bridge security gaps and reduce risk by seamlessly integrating developer and security mindsets.** The ideal way to do this is by bringing the DevOps skill set into both your SOC and your broader organizational security operations. DevOps, developer, and infrastructure teams often have greater visibility and a better understanding of an environment than security teams, simply because they are continuously in the environment. Whereas the SOC team, almost by definition, are the ones reacting to anomalies. A developer can provide a different perspective of cloud, SaaS, and the development process that is critical in dealing with incidents involving these environments, and involving developers in security will pay dividends in operational resiliency.

It can be challenging for traditional SOC analysts to identify and understand what is normal and expected in the cloud, since these environments require very different technology stacks and processes than those they are familiar with, such as object storage, serverless computing, container orchestration, and runtime image scanning. Collaboration between DevOps and SOC teams will highlight missing telemetry and other unidentified risks that might otherwise lead to an attack.

The 2020 SolarWinds incident, which resulted in the **loss of $40 million** in just the first nine months and litigation against the company's CISO, provides an interesting example of the knowledge gap often present between security and development. The threat actor in this example compromised the vendor's build pipeline and planted malicious code, which was then unknowingly passed to customers. The SOC analysts were unfamiliar with how the build pipeline normally worked and unaware of what data even needed to be collected from the build servers above the operating system layer. **Someone with DevOps knowledge would have been much better equipped to support the SOC in this case, potentially leading to a less damaging outcome.**

**SOC analysts typically have the following expertise:**

- Knowledge of attacker motivations and techniques
- Skill in monitoring network traffic and system logs, and in detection engineering
- Deep understanding of vulnerabilities, malware, and intrusions
- Experience in cybersecurity best practices, security compliance requirements, and organizational security policies and procedures
- Up-to-date cybersecurity threat and trend awareness

**DevOps engineers can bring the following skills into the SOC:**

- Deep understanding of cloud infrastructure with specific expertise in relevant CSPs
- Strong knowledge of the secure software delivery lifecycle (SSDLC)
- Expertise in automating deployment and management of IT infrastructure for consistency, reproducibility, and scalability
- Understanding of containerized technologies and container orchestration platforms for streamlined deployment and management
- Skill in implementing CI/CD pipelines to automate the build, testing, and deployment of software applications

# People enhance processes and reduce security gaps

Ensure your security team coordinates with other teams outside of formal incident response processes to share knowledge, capabilities, and tooling. This will give your security team a better understanding of the business, its operations, and where attackers may enter, move, and hide, and will in turn allow your security team to improve their processes.

**Establish lunch-and-learns between cross-functional teams or embed a SOC analyst within a DevOps or infrastructure team for a period of time, and vice versa.** Keep in mind this needs to be proactively managed, otherwise it may not occur. This collaboration with other teams is essentially a "shift left" for improved correlation and context that will make incident response a little less painful.

Ask any security or threat analyst what their favorite part of analysis is, and they will likely say it is digging into a puzzle and uncovering the whole story. Unfortunately, during the cloud threat detection and response process, there is no time for rabbit holes. It takes a lot of time to manually correlate data from multiple endpoints, workloads, environments, and more with legacy tools, and cloud attackers are already automating attack processes. **Time spent doing manual correlation only benefits your adversary. Data correlation during incident response must be high-fidelity and automated.**

Visualization of an attack path allows your security team to see how initial access, permissions, lateral movement, and data collection and exfiltration all connect.

To correlate and triage in five minutes, you need a streamlined process. This will also include dashboard consolidation. **Visualization of an attack path** during correlation is ideal. Your security team needs to see how initial access misconfigurations or vulnerabilities, identity permissions used, movement across workloads or environments, and data collection or exfiltration all connect in near-real time. Furthermore, these details are critical for your after-action review or root cause analysis. There is a good chance that you have all the security infrastructure you need to respond to a breach, but your team's time to respond using all of these tools is likely much more than 10 minutes.

# Improve risk management by maximizing detection efficiency with the right tools

Real-time threat detection is a key step toward reducing mean time to remediate (MTTR). Detection in real time is necessary to gain visibility into ephemeral assets, which are temporary or short-lived resources such as containers, virtual machines, or cloud instances. These assets are often dynamically created and spun down as part of modern computing environments, making legacy security tools and processes insufficient for monitoring and protecting ephemeral assets.

Real-time detection allows security teams to continuously monitor ephemeral assets as they are provisioned and decommissioned, immediately alerting on any security vulnerabilities or suspicious activities. It is your early warning system against evolving cloud threats and it is mandated by many industry and federal compliance requirements. Chances are, you have real-time detection capabilities due to compliance regulations, but using truly cloud-native tooling provides an organization with exponential gains in speed, cost, scalability, and innovation.

A CNAPP reduces the operational complexities that are innate in the cloud and provides the comprehensive coverage that individual CSPs cannot give you.

## Simplify cloud tool complexity

Start with your CSP. You already have it, so use it. The native data and capabilities of your CSP are critical in building a strong cloud security program. However, unless your organization was born in the cloud, you more than likely have a hybrid environment, with a combination of cloud-native applications and legacy applications that were migrated to the cloud. If this is the case, you need cohesive correlation between CSPs, which necessitates a cloud-agnostic tool. You cannot leave these lateral gaps open.

A Cloud-Native Application Protection Platform (CNAPP) tool is the cloud-native solution to your real-time detection problems. It is the combination of multiple necessary cloud-native capabilities in one offering. A CNAPP reduces the operational complexities that are innate in the cloud and provides the comprehensive coverage that individual CSPs cannot give you.

Like a cloud threat detection and response (CDR) tool, a CNAPP offers comprehensive real-time visibility and detection for cloud and hybrid infrastructure and services, providing instantaneous alerts for misconfigurations, vulnerabilities, and compliance issues.

A CNAPP also brings your cloud workload protection (CWPP), identity management (CIEM), and posture management (CSPM) all into a single dashboard alongside your threat detection and response. Leveraging an advanced, comprehensive tool such as a CNAPP enables the proactive incident response that is necessary in the cloud.

In addition, a CNAPP can be used for better security by more than just the security team. In today's secure-first, high-tech business world, shared responsibility for security is necessary. This shared responsibility is supported within a CNAPP with collaborative use cases for legal, HR, engineering teams, and more.

## Integrate your security tech stack

A CNAPP will integrate well with other tools that might already be in your security tech stack. This includes solutions like SIEM (Security Information and Event Management) for data aggregation, and SOAR (Security Orchestration, Automation, and Response) to correlate data, contextualize information, and automate response actions. These tools, in combination with a CNAPP, will further improve your detection and response efficiency. Be sure to prioritize the simplicity of integrations when building and modernizing your cloud-native tech stack by ensuring the tools are API-driven. Integrations should happen at machine speed, and if they are cumbersome or challenging, they don't help. Don't force your security team to have to log into multiple dashboards.

Integrations should happen at machine speed, and if they are cumbersome or challenging, they don't help.

With an integrated SOAR tool, you can orchestrate and coordinate your toolings, processes, and workflows at the speed necessary for cloud threat detection and response. **Through proactive threat modeling, your security team can establish automated response actions for predetermined attack paths.** All you need are if-then statements: if x happens, then y is triggered. Through threat modeling, x can be anticipated and y can be proactively mitigated or continuously assessed to preclude impact.

For example, Sysdig offers a feature called **drift control** based on this concept. With drift control, security teams can automate responses when workload modifications are detected in production. They can either choose to trigger an alert, pause a workload, or stop it altogether. This idea can be applied to other events as well, allowing security teams to immediately quarantine potential issues as they analyze the situation and buy time to formulate an appropriate response.

It is necessary, however, to consider potential financial implications on the business from unplanned downtime when automating workload stops. A mutual understanding and communication between security and developer teams should avoid operational impact.

# Trust and train your team

You may already have an incident response plan in place. If you do not, the time for your security team to create one was yesterday. If you do, now is the time to revisit it and ensure all elements of your incident response policies and playbooks include considerations for the time pressures of modern cloud attacks. Allow those with hands on the keyboard to either establish an incident response plan or update the one you have.

Your role is to ensure that during your security team's response, you are kept abreast of the important details you need to know and communicate to other executives and board members, such as materiality and business or operational impact. You need to know or determine if the impact of the attack is material and be prepared to report on this. However, with a timely response, there is less chance that there will be a material impact.

Your role is to ensure that during your security team's response, you are kept abreast of the important details you need to know and communicate to other executives and board members, such as materiality and business or operational impact.

# Set the course, collaborate, and listen

Lead your security team in attacking this 10-minute cloud threat detection and response challenge with the goal of streamlining and improving your security processes through automation. **Prioritize automation integrations in the detection, data correlation, and response steps.** It may not be easy, and it will take time to fully implement, but being able to detect, correlate, and remediate threats in minutes will reduce risks, improve resiliency, and keep you compliant with regulations and materiality rules. Automating these tedious manual incident response processes will also remove a huge burden from your security team and free up their time for proactive actions like detections and hunting.

Your job is to foster a strong relationship and a regular cadence of communications between your security team and developers. These two teams need to work closely and understand each other's processes so they have better visibility, understanding, detections, and response.

- Drive this collaboration by communicating with security and engineering leaders, and initiate regular team calls with a call to action for organizational change.
- Lead the discussions with the need for collaboration and automation to reduce risk and improve processes.
- Follow up and continue to be an active voice in the push for faster threat detection and response.

» Being able to detect, correlate, and remediate threats in minutes will reduce risks, improve resiliency, and keep you compliant with regulations and materiality rules.

Furthermore, start with a test and establish a baseline, so you know where your SOC stands and where it needs to improve. Use an offensive security team if you have one, a third-party vendor, or an open-source capability, and test your organization's security incident response plan against a real cloud threat. Cloud attacks take minutes, so this exercise and a debrief should not take more than a few hours. Review your response actions and timelines, and highlight where excessive time was spent or what important information was missed. Use these 555 Benchmark guides to improve your efforts, and then try again.

# Conclusion

Cloud attacks will continue to happen at breakneck speeds as attackers continue to innovate and automate, and we need to be prepared to stop them. By following the 555 guides for practitioners and leaders, you and your team will improve your organization's overall security posture and reduce your risk of a material attack. **Many business processes are automated. Now is the time to automate security processes.**

## About Sysdig Secure

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

To learn more about Sysdig, visit sysdig.com

REQUEST DEMO →

sysdig

WHITE PAPER


WP-010 REV. A 6/24