THE /555 GUIDE

CLOUD SECURITY PRACTITIONERS

sysdig.com/**555**

sysdig SECURE EVERY SECOND.

As cloud environments evolve and the attack surface expands, the need for robust and timely security measures becomes imperative. The **Sysdig 555 Benchmark for Cloud Detection and Response** sets the standard for operating securely in the cloud, emphasizing the need for security teams to detect, triage, and respond to attacks within the average time it takes threat actors to conduct them: 10 minutes.

The Sysdig Threat Research Team's **2023 Global Cloud Threat Report** underscored the escalating speed and sophistication of attacks in the cloud, which have been further enhanced through the malicious use of AI and automation. Organizations need tools and processes designed specifically for the dynamic nature of cloud-native environments.

This guide is here to answer why 555 matters, and help your organization achieve it with shared language and operational direction — ultimately enabling faster cloud threat detection.

Table of Contents

People create processes and use tools

The days of the traditional SOC model have come to an end due to the volume and velocity of modern attacks. The tiered model — where analysts watch screens for incoming events, manually triage them, and then escalate or close out tickets — is too slow and cumbersome to keep pace with cloud attacks. The amount of data we expect SOC analysts to consume, understand, and act upon is already unsustainable.

At this point, your SOC must discern which activities and functions should be automated, and which require manual discretion and intervention. This may vary based on the individual structure and priorities of your SOC, but there is no excuse for not embedding automation in at least some part of your security processes.

Consider a pilot flying a plane with autopilot. The plane, with the help of autopilot, is making thousands of adjustments in real time; the pilot is occasionally validating the telemetry and switching to manual control for landing or if something goes awry. Similar to the plane in this analogy, your SOC must be as automated as possible if your organization wants to outpace attackers.

To that end, you only have a few minutes to find and stop a cloud attacker. Automate your initial response processes. Then, you'll have more time to follow up, analyze, and understand the data and events so you can discern an appropriate response or remediation. During a cloud security investigation, you may have event logs from multiple service providers, environments, endpoints, and more. These logs may all be related, but their relationship might be unclear at first glance.

» You only have a few minutes to find and stop a cloud attacker. Automate your initial response processes. Then, you'll have more time to follow up, analyze, and understand the data and events so you can discern an appropriate response or remediation.

Unite SOC and DevOps expertise to accelerate cloud security operations

In some sense, DevOps is responsible for the pain of expanding the SOC's scope into the cloud. However, DevOps SMEs and their skill sets can also make the greatest contribution to improving the SOC's efficiency and success in legacy, modern, and hybrid operating environments through an expanded perspective and automation.

DevOps expertise in the SOC provides several benefits. Knowledge of cloud, SaaS, and development processes is critical for dealing with events and incidents involving these environments. This alternative perspective could also highlight missing telemetry and other unidentified risks that might otherwise lead to an attack. 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. How many analysts in your SOC understand which functions are normal for build software, such as Jenkins? Do they know how to spot abnormal behavior there? If not, how can you work with them to start learning today?

The 2020 SolarWinds incident 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. Here, 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 be 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

Elevate existing security processes

One of the most challenging aspects of being a security professional today is the sheer number of environments and technologies that organizations are using, and the pace at which new technologies are being adopted. To help security analysts (and therefore the organization as a whole) succeed, experts from teams outside of security should be included in decision-making and onboarding processes, such as the addition of a new data source into their SOC.

For example, to properly secure and monitor Kubernetes, include DevOps and application teams during the implementation process. Without their input, the SOC may struggle to understand and appropriately deal with events that come from Kubernetes and the applications that it hosts, whereas developers have an intimate understanding of these technologies. Including SMEs in the development of cloud and workload security processes creates a common understanding — not just for the security analysts, but also so DevOps and application developers can understand what the SOC needs and why. Formalize this collaboration by establishing a checklist or common standards for when these teams onboard new systems or software.

This collaboration will enable the SOC to respond more quickly to events and incidents because they will have a greater understanding of what they are looking at, and it will also give them insight into who owns what. During an investigation or incident response, a lot of time is wasted trying to determine what something is and who needs to be brought in to help. In this example of securing and monitoring Kubernetes workloads, clear identification via namespace organization and tagging will help simplify and expedite investigations and responses.

To properly secure and monitor Kubernetes, include DevOps and application teams during the implementation process. Without their input, the SOC may struggle to understand and appropriately deal with events that come from Kubernetes and the applications that it hosts.

A well-rounded response should be predetermined

Traditionally, the first response to an incident was just to unplug the ethernet cable. While this solution is effective on-premises, it's rarely quite that simple with the new technologies and services being deployed in the cloud. Instead of strategically shutting everything down, more tactical approaches have become the standard. Isolation techniques can be automated in the cloud and should be front and center for security teams, with pre-defined criteria for when this isolation occurs in an automated fashion.

By establishing and following predefined criteria, certain high-risk activities — such as a machine running an unapproved process or communicating with unknown IPs — can be automatically isolated for incident response. For example, instead of killing entire Kubernetes nodes or clusters, you can choose to start your response and quarantine the incident by automatically killing or pausing a single container. Tactical response efforts like these might allow companies to continue business as normal to some extent, but they first require additional knowledge and foresight of the actions' broader effects before implementation. The plethora of options available may also make a proper response less obvious to less experienced team members.

A well-crafted response plan should be organized and coordinated by those who are directly involved in incident response actions. Your incident response plan must include communication channels and collaboration between security personnel, developers, senior leaders, and other pertinent departments. There is a good chance you already have a plan in place, but now is the time to review and improve it as necessary. Begin with an exercise to determine whether you can meet the speed necessary to respond to modern cloud attacks — if not, your plan should be adjusted to allow for proactive mitigation. It should also include standardized reporting templates, ready-made communication channels, and automation to streamline the incident response process according to the 555 Benchmark.

» Begin with an exercise to determine whether you can meet the speed necessary to respond to modern cloud attacks — if not, your plan should be adjusted to allow for proactive mitigation.

Response processes should also include team members with development expertise, such as DevOps, to better understand environmental issues. While it may not be practical to include them in the decision to respond, they should be included in the development of the process.

Though your security team should be prepared to provide immediate response to an incident, post-incident information sharing across an organization is equally crucial. A post-incident workflow involving developers and engineers ensures comprehensive data sharing for thorough remediation throughout your environment.

Cloud attackers are already automating processes

SCARLETEEL was an attack that took place across runtime and cloud environments, occurred in just a few minutes (3:42 to be precise), and resulted in the loss of proprietary data. There are multiple points at which this attack could have been detected and stopped, but each of them happened very quickly. In the runtime environment, for instance, the attackers used curl to steal credentials from the EC2 IMDS endpoint. This is a fairly common activity, but the credentials stolen had an over-permissioned policy that provided read-only access to the entire cloud account. A robust detection tool should understand this, in context, as a "risky" policy and alert someone, like a SOC analyst, who can immediately understand the danger and work to mitigate it.

The cloud was built for speed and simplicity, so it makes sense that the attackers rely heavily on automation. Once the SCARLETEEL attackers had access to the cloud they ran automated scripts to conduct reconnaissance. Reconnaissance is often a very noisy process, but what made this example particularly strange was that the identity being used belonged to an EC2 instance. The attackers exploited the over-permissioned credentials to move laterally through the environment. Can your detection technology understand this movement and correlate the two events? If not, responding quickly and effectively becomes impossible since, by the time all of this information has been brought together manually, the attack will be complete.

While you may read the above example and think there is no way you can stop the attack in time, **the same technologies leveraged by attackers can also give us quick and effective response actions.** Attackers aren't the only ones who can take advantage of the cloud's speed and simplicity at scale. When the attacker first stole the over-permissioned credentials, an analyst (or automated process if you like to live on the edge) could have been used to reduce the privileges on the policy, thereby effectively quarantining it, and preventing the entire attack. The same could have been done during the attacker's reconnaissance stage. Alternatively, the affected EC2 instance could have had an assigned security group policy to cut off all network access. The options available to defenders for cloud response actions are much more extensive and precise than those offered by traditional EDR tools.

Complement existing tools with new ones to maximize visibility and response speed

To rapidly detect and respond to cloud attacks, a collaborative tech stack that is fully integrated across your environment is a necessity — there is no room for detection gaps or lag. We are constantly defending against new innovative cloud tactics and techniques, and the time is long past for SOCs to be more innovative in their defensive posture.

Cutting-edge tools

Modern problems require modern tools. Leaders must consider tools and platforms that integrate with their existing ecosystem and satisfy compliance and technical requirements to keep their cloud-native workloads and data secure. CNAPP and CDR tools offer more than a check in the compliance box; they provide a common platform that extends traditional detection and response. They also engage both the security and non-security teams (i.e., legal, HR, engineers) to build a shared responsibility model. These teams will better grasp unforeseen risks and be more prepared to address emerging threats.

Detection and response currently exists in a perpetual state of coevolution with organizational environments. On-prem environments necessitated SIEM (Security Information and Event Management), IPS/IDS (Intrusion Detection System/Intrusion Prevention System), and EDR (Endpoint Detection and Response) — among other specialized tooling — to effectively detect, investigate, and respond to threats.
The next evolution in organizational environments is cloud native. Cloud native provides an organization with exponential gains in speed, cost, scalability, and innovation. But with these advancements, security teams face challenges such as exponential increases in data volume, ephemeral workloads, faster attacks, and complex compliance scenarios.

CNAPP and CDR tools provide a common platform that extends traditional detection and response. They also engage both the security and non-security teams (i.e., legal, HR, engineers) to build a shared responsibility model.

The fewer dashboards you have to log into during incident response, the better. It's too time-consuming and inconvenient to have to log into multiple tools in multiple windows to access different capabilities. You should streamline your security processes and correlation capabilities by using a one-stop shop, such as a CNAPP (Cloud-Native Application Protection Platform). It is a platform built out of cloud-native necessity on the standard of runtime security. A CNAPP will correlate events for you in near-real-time across multiple sources and hand it to you on a silver platter, all in one place. Visualizing an attack path accelerates response actions and allows for immediate review of a workload's configuration and vulnerability status without having to click or script anything.

Organizations deploy hundreds or thousands of containers and other workloads in production, and security teams need visibility and context across the entirety of the environment. Cloud threat detection encompasses not only workload runtime security, but also cloud services, human and machine identities, and software supply chains. A CNAPP not only enhances visibility, it also provides better security control by helping security teams use automated policy enforcement, risk awareness, compliance, and more.

Classic tools

Your cloud detection tech stack may already include some of these familiar names: SIEM for data aggregation; CIEM (Cloud Infrastructure Entitlement Management) for cloud identity context; SOAR to correlate data, contextualize information, and automate response actions; and CSPM (Cloud Security Posture Management) capabilities for context, root cause analysis, and understanding how to remediate flaws at their source.

First, SIEMs must have access to relevant data if they are going to help detect security threats and vulnerabilities before they disrupt operations, and there are enough memes about their cost to know that isn't always monetarily feasible. Second, a SIEM needs to understand the data it is receiving, but as quickly as new applications and services come online, it is not always guaranteed that a SIEM's data ingestion and parsing is up to snuff. This also assumes the data wanted or needed can even be sent to a SIEM in the first place.

In the cloud, permissions are everything — for developers and attackers alike. Tools like CIEM and CSPM can provide insights into granted permissions, the extent to which they're used, and how secure they actually are. These tools, in addition to interacting with your SIEM, need to have detection content built for new data and a rule engine that can make proper sense of this data very quickly. This all comes before tackling the response part of the "detection and response" equation.

Automation is key for speedy cloud threat detection and response. This goal can be met using a SOAR, a set of technologies that was wrapped into a single platform concept around 2017 (like CNAPP). It can help streamline security operations through automated detection, investigation, and mitigation of security threats. In light of the speed of cloud attacks, now is the time to bring a SOAR into your SOC.

Advance with agility

Tools alone are not enough to detect and respond to cloud attacks in real time. You must also adopt new mindsets about security — new skills, an updated outlook, and refined finesse.

The 555 Benchmark set a new standard for cloud security agility, and it aligns with the current pace of cloud-native environments and threats. As a practitioner, embrace the benchmark as a guiding principle for improved cloud security collaboration, tooling, and processes.

For example, how long does it take for an analyst to pull the alarm following an alert about a potential incident? How long does it take your security team to find and correlate data that is potentially related to the initial event and tell the story of what is happening? What are your response actions and how quickly are they implemented following the determination of a true positive? Who is notified and who then supports an incident? If your answers to these questions are in hours or days, your incident response efforts need an overhaul.

The 555 Benchmark offers an opportunity for you to actively collaborate with your senior security staff and establish a plan for meeting this cloud threat detection and response challenge. Approach this task by first determining what your established processes and timelines are. Test and evaluate those processes by running mock incidents and responding according to your current response plans. If you have either access to or the capacity to pay for third-party or internal red teams or penetration testers, use them to launch these attacks. There are also open source PoC available that will walk you through safely launching an attack in a sandbox. Debrief following your tests and set a cadence so you can continue to refine and test your processes. Review your findings with your security teams and CISO and make modifications and improvements as we've laid out in this paper. Equipped with speed, agility, automation, and an informed team, security defenders are armed to beat attackers at their own game.

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-011 REV. A 5/24