**17**

**Implementing and Integrating Security Monitoring**

Enterprises adopt multi-cloud and use cloud services from different cloud providers. These solutions will be securee, but enterprises want an integrated view of the security status on all of their platforms and solutions. This is what solutions such as **Security Information and Event Management** (**SIEM**) and **Security Orchestration, Automation, and Response** (**SOAR**) do.

In this chapter, we will learn why these systems are a necessity in multi-cloud. First, we will discuss the differences between the various systems, and then we will explore the various solutions that are available on the market today. The big question we’re going to answer in this chapter is, *how do we make a choice and, more importantly, how do we implement these complicated solutions?*

We’re going to cover the following main topics in this chapter:

* Understanding SIEM and SOAR
* Setting up a Security Operations Center
* Setting up the requirements for integrated security
* Implementing a security model
* Exploring multi-cloud monitoring suites

**Understanding SIEM and SOAR**

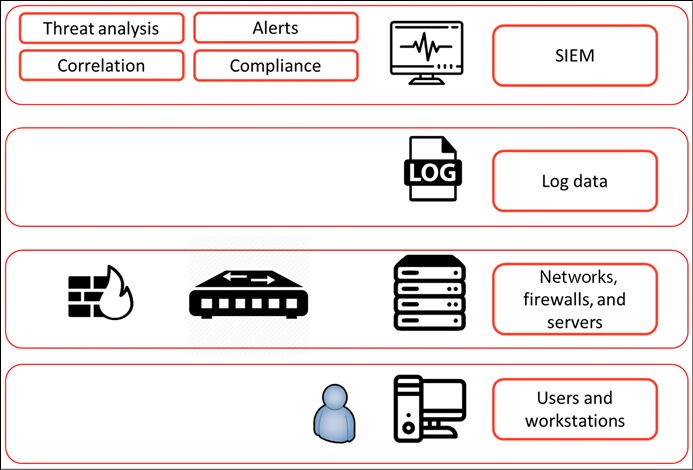
All cloud providers offer native services for security monitoring, such as Microsoft Defender for Cloud, AWS Security Hub, and Security Command Center in Google Cloud. However, companies are going multi-cloud using IaaS, PaaS, and SaaS from different providers. Enterprises want an integrated view of their security in all these solutions. If an enterprise is truly multi-cloud, it will need an integrated security solution with SIEM and SOAR.

Next, the enterprise needs a unit that is able to handle and analyze all the data coming from SIEM and SOAR systems and trigger the appropriate actions in case of security events. Most enterprises have a **Security Operations Center** (**SOC**) to take care of this. In the next section, we will explain what the differences are between SIEM and SOAR, why an enterprise needs these systems in multi-cloud, and what the role of the SOC is.

**Differentiating SIEM and SOAR**

Let’s start with SIEM. Imagine that workloads—systems and applications—are deployed in Azure and AWS, and the enterprise also uses a number of SaaS services, such as Microsoft 365 and Salesforce. All these environments are protected with firewalls in both Azure and AWS, along with on-premises data centers. Traffic is routed through virtual network devices, routing tables, and load balancers. The enterprise might also have implemented intrusion detection and prevention to protect systems in the public clouds and on-premises data centers. All these security systems will produce a vast amount of information on the security status of the enterprise environments.

A SIEM system collects, aggregates, and analyzes this information to identify possible threats. Since it collects data from all environments, it’s able to correlate the data and recognize patterns that might hint toward attacks. For this, SIEM uses machine learning and analytics software. It recognizes abnormal behavior in systems with anomaly detection. A simple example is, if user A logs in from an office in London at 9.00 AM and again logs in at 9.30 AM from Singapore, a SIEM system would know that this is impossible and raise an event or alert. The architecture of a SIEM system is shown in *Figure 17.1*:



*Figure 17.1: The conceptualized architecture of a SIEM system*

SOAR goes beyond SIEM. Like a SIEM system, SOAR collects and analyzes data that it gathers from a lot of different sources, such as public cloud environments. But the added value of SOAR is in orchestration and automation. In SOAR systems, companies can define automated responses to events, using playbooks that integrate with security solutions in the platforms. If a SOAR system detects a threat in a system, it can immediately remediate it by taking actions such as closing communication ports, blocking IP addresses, or putting systems into quarantine. It does that fully automated, including logging and raising tickets to service management systems. This gives security professionals time to investigate the actual threat, without needing to worry about remediation first. That task is taken care of preemptively for them by SOAR.

**Initiating a Security Operations Center**

Since the world is moving to digital, companies are increasingly threatened by digital threats. It also seems that hackers are always one step ahead of the companies themselves in protecting their digital assets. It takes a lot of skills to keep up and counter these attacks. Therefore, enterprises rely more and more on specialized groups where security expertise is bundled—a SOC. Enterprises can have these in-house or outsourced to specialized companies.

The SOC is responsible for monitoring and analyzing the security state of an enterprise on a 24/7 basis. A team of security engineers will use different technology solutions, including SIEM and SOAR, to detect, assess, and respond as quickly as possible to security incidents.

A SOC plays a vital role in securing multi-cloud environments by providing centralized monitoring, incident response, threat intelligence, vulnerability management, compliance and regulation, and security automation. Let’s work that out in more detail. The SOC:

* Monitors and analyzes security events from multiple cloud platforms to detect potential security threats and breaches
* Leads the incident response process when a security breach or threat is detected, including investigating the incident, containing the breach, and recovering systems and data
* Gathers and analyzes threat intelligence from a variety of sources to better understand and respond to emerging security threats
* Works with the security and operations teams to identify and remediate vulnerabilities in multi-cloud environments
* Helps organizations ensure compliance with regulations and standards, such as ISO, PCI-DSS, and HIPAA, by monitoring and auditing cloud environments
* Uses security automation and orchestration tools to streamline and automate security processes, such as incident response and vulnerability management

In a multi-cloud environment, a SOC is crucial, since organizations will operate a combination of on-premises, public cloud, and private cloud infrastructure to run their applications and store their data. Then it’s essential to have maximum observability across these different platforms. But observability is not enough. An enterprise needs to know what its vulnerabilities are and where it is at risk so that it can develop and implement plans to avoid, deter, or mitigate risks when they materialize.

In the next section, we will explain how an enterprise can set up a SOC. In the last section of this chapter, *Exploring multi-cloud monitoring suites*, we will explore some major SIEM and SOAR solutions that companies can use to protect their systems in multi-cloud environments.

**Setting up the requirements for integrated security**

Before a company gets into buying licenses for all sorts of security tools, security architects will need to gather requirements. That is done in the following four stages that a security team needs to cover:

1. **Detect**: Most security tools focus on detecting vulnerabilities and actual attacks or attempts to breach systems. Some examples are endpoint protection, such as virus scanners and malware detection, and **Network Traffic Analyzers** (**NTAs**). In multi-cloud, architects need to make sure that detection systems can operate on all platforms and preferably send information to one integrated dashboard.
2. **Analyze**: This is the next phase. Detection systems will send a lot of data, including false positives. Ideally, security monitoring does a first analysis of events, checking them against known patterns and behavior of systems and users. This is the first filter. The second phase in the analysis is prioritization, which is done by skilled security staff. They have access to knowledge base repositories of providers and security authorities. They have the information that enables them to give priority to potential threats, based on relevant context. Remember one thing—where there’s smoke, there’s usually a fire. The question is, how big is the fire?
3. **Respond**: After a threat is detected and prioritized, the security team needs to respond. First of all, they need to make sure that the attack is stopped and exploited vulnerabilities are identified. The next step is remediation— preventing systems from enacting (further) damage or data breaching. The final step in response is recovery—restoring systems and making sure that the data is safe. Be sure that processes for following up security events are crystal clear. Who needs to be informed, who’s mandated to take decisions, and what is the escalation path?
4. **Prevent**: SIEM and SOAR systems can do a lot in detecting, analyzing, and responding to security events. However, security starts by preventing vulnerabilities from being exploited in the first place. Security teams need to have continuous visibility on all the platforms that an enterprise uses and must have access to security reports, assessments, and threat detection scans from the providers. It’s also essential that recommendations from Azure, AWS, GCP, VMware, or any other provider are followed up. These providers issue security updates on a regular basis and give recommendations to improve the state of security of environments that are deployed on their platforms. These recommendations should be followed.

Market analyst Gartner predicts that by 2024, 80 percent of all SOCs will have invested in tools using artificial intelligence and machine learning. However, Gartner analysts also conclude that these investments will not necessarily bring down the amount of time that security teams have to spend on investigating security events. So, what would be wise investments in terms of security tools and systems?

First, leverage what providers already have. Azure, AWS, GCP, and OCI all have security suites that gather a lot of information on the health and integrity of systems. In almost all cases, it’s a matter of ticking the box to enable these security systems, although security engineers will have to set a baseline to which the tools monitor the systems. This was discussed in *Chapter 14*, *Defining Security Policies*.

**Implementing the security model**

A lot of companies already have a multi-cloud setup. For example, they use AWS to host websites and have Microsoft 365 from Microsoft, a SaaS solution. In AWS, security teams will work with AWS Inspector and GuardDuty for monitoring security. In Office 365, they might use **Microsoft Defender**, for example. The challenge for security teams is to have an integrated vision of the full IT environment. How do companies get there?

Security models often start with the concepts of zero trust and security by design. What is meant by that? We must realize that with cloud and multi-cloud, the need for security is growing. Organizations collect a lot of data and aggregate it in the cloud, often in vast data lakes that hold petabytes of raw data, making it very attractive for criminals to try to get hold of. That data is constantly exchanged, being used across multiple applications, likely operating on different platforms or at least communicating between different platforms. Multi-cloud environments are more complex and dynamic, making it harder to secure all the various components. As a result, organizations are turning to zero trust and security by design concepts to help ensure that their multi-cloud environments are secure.

Zero trust assumes that any user, device, or network component may be compromised and, therefore, requires multi-factor authentication and continuous verification before access is granted. This approach assumes that the trust level for all access requests is set to zero and that security measures must be in place to protect the organization’s assets from malicious actors.

Security by design incorporates security considerations into the design and development of systems, applications, and infrastructure. This approach ensures that security is built into the fabric of the technology and that security is a consideration at every stage of the development process. In multi-cloud architectures, we combine the two concepts, which is the best practice. By doing that, we address security at the foundation of the technology. Enterprises can implement a defence-in-depth approach that includes multi-factor authentication, encryption, and continuous monitoring. Security by design ensures that security is built into the development process and that security considerations are integrated into all aspects of the technology.

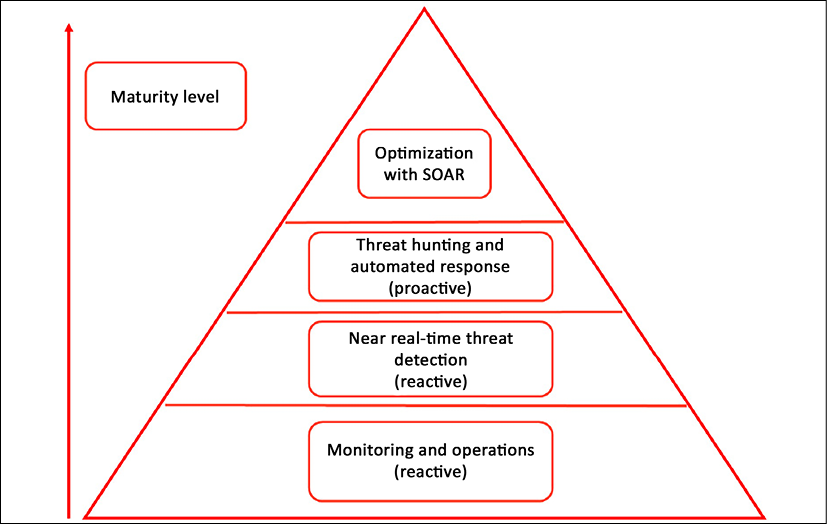
Let’s give an example: we can use **identity and access management (IAM)** solutions to enforce multi-factor authentication and implement a least privilege access model. This helps to ensure that only authorized users have access to an organization’s cloud assets and that their access is monitored and audited. Next, we can encrypt all data by default. All clouds do that already: Azure, AWS, GCP, and OCI encrypt data at entry. We should also use secured networking such as VPNs to ensure that all traffic is encrypted and protected from eavesdropping.

Automation and orchestration tools will help to automate security processes, such as incident response and vulnerability management, and provide a centralized view of security events and alerts from across the cloud environment.

By assuming that all access requests are not trustworthy and incorporating security considerations into the design and development of technology, organizations can help ensure the security of their multi-cloud environments and protect their assets from malicious actors. What steps do we need to take to define and implement a security strategy and associated model?

* **Define a target operating model**: What does the entire environment look like and who’s responsible for all or some of it? Companies must have a clear demarcation model on roles and responsibilities in the management of cloud platforms, services, and systems. The target operating model describes the landscape of components and the owners of these components. Security is a component that the security officer is responsible for.
* **Define workflows and escalation procedures**: This defines the workflow when security events occur. What is the procedure in the case of high-priority events, medium-rated events, and low-risk events? When a high-priority event is detected, it should be raised to the security officer. The security officer decides who needs to be informed and what actions must be taken. These are operational tasks. They may report to the **Chief Security Officer** (**CSO**) or the **Chief Information and Security Officer** (**CISO**). The CSO or CISO is responsible for strategic security decisions.
* **Analyze the capabilities of security tools that are already in place**: Evaluate the tools that are in place already. What do these tools cover? How are APIs configured, and can they communicate with overlaying systems? What are the default baselines that these tools use?
* **Gap analysis**: There will always be blind spots. A common example in batch jobs is whether these are monitored as well from a security perspective. What happens when jobs are stopped? Is communication between systems then halted, and is the integrity of systems still safeguarded? In cloud-native environments, companies should also have a good understanding of how containers and serverless solutions are monitored. Not all monitoring tools can handle these native environments yet.
* **Make a strategic plan**: This is what the CSO or CISO must be concerned with. The first question that must be covered in a strategic plan is the maturity goal of the enterprise. The next question is what the major security concerns are for the enterprise—what are the biggest risks and threats? Hint: it is not always about the loss of money. Reputational damage goes far beyond revenue loss when systems are breached. Finally, the company must be able to identify whether existing tools, processes, and expertise are sufficient and what needs to be done to get to the desired maturity goal.

The following diagram shows a maturity model for security:

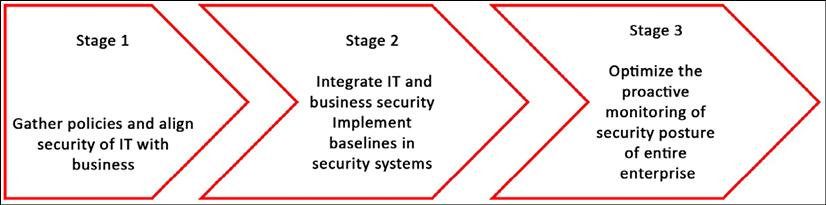


*Figure 17.2: Security maturity model, from reactive monitoring to proactive threat hunting*

It’s strongly advised to set up a security team or SOC. It’s not realistic to have one or two security engineers watching over multi-cloud environments. The difficult part is how to get there. The best practice is to plan the setup in three stages:

* **Stage 1: Get visibility for the business**: In this stage, we gather the security policies and align the security processes between the business and IT.
* **Stage 2: Integrate IT security operations with business security**: This is the stage where security operations enable security monitoring and onboard the security baselines—as defined with the business at stage 1—in the monitoring systems. Part of this stage is a risk assessment of the platforms. It’s recommended to do an assessment of the security baselines of the cloud providers and analyze whether these baselines concur with the security principles of the enterprise.
* **Stage 3: Optimize**: This is the stage where a truly integrated view is created, using one dashboard that covers the entire security state of the IT landscape.

The stages are shown in the following diagram:



*Figure 17.3: Three stages of security onboarding*

Integrated security means that a company has a clear model of processes, tools, and expertise. In multi-cloud, this also means that cloud providers are part of these processes, tools, and certainly, expertise. The security architect will have the task of getting this defined, designed, and modeled. SIEM and SOAR tools can help to get an integrated view of the entire security state—or posture—of an enterprise. In the next section, we will discuss popular solutions for this in multi-cloud.

**Exploring multi-cloud monitoring suites**

Companies have a wide variety of choices when they’re looking for a SIEM solution This is a fast-growing market. Each year, market analyst Gartner publishes a list of leading solutions in different IT domains. For a number of years, Splunk, LogRhythm, and Rapid7 have been named as leading products for SIEM by Gartner.

Splunk is a log management and analysis platform that can collect, analyze, and visualize data from a variety of sources, including all major cloud providers.

LogRhythm is a SIEM platform that can collect and analyze log data from cloud environments. LogRhythm provides a set of pre-built connectors and integrations for all clouds, allowing us to collect and centralize log data from these platforms and use LogRhythm’s threat detection and incident response capabilities to detect and respond to security threats.

Rapid7 is a security analytics platform that provides threat detection and incident response capabilities for cloud environments. Rapid7’s security analytics and incident response capabilities are used to detect and respond to security threats.

To summarize, all of these solutions can work with all major cloud providers using REST APIs. **REST** stands for **REpresentational State Transfer**. A REST API is a programmable interface that connects to a service in the cloud and enables data from that service to be captured and sent to an application. In this case, the SIEM suite uses an API to get security data, such as alerts from the cloud, and transfers it to the dashboard of the SIEM solution.

Splunk, LogRhythm, and Rapid7 have APIs for Azure, AWS, GCP, and OCI. Splunk and LogRhythm integrate with Azure Monitoring and Azure Event Hubs to export logs, coupled with Azure connectors from SIEM vendors that enable the collection of these logs into the SIEM product. In AWS, these tools work with AWS Config, CloudTrail, and CloudWatch to collect data. Splunk can use other cloud-native logging solutions like operations suite for GCP and OCI Logging to collect logs and metadata, which can then be analyzed and visualized in Splunk.

The market for SIEM and SOAR is rapidly growing, also attracting companies that didn’t have security as their main focus but, since 2020, have invested heavily in developing or acquiring security products. It’s a logical move when you realize how fast cybercrime is growing. The Cloud Security Alliance published the *Pandemic Eleven* in 2022, including the top threats in the cloud:

1. Insufficient identity credentials, access, and key management
2. Insecure interfaces and APIs
3. Misconfiguration of resources and inadequate change control
4. Lack of cloud security architecture
5. Unsecure third-party resources
6. System vulnerabilities
7. Accidental cloud data disclosure
8. Organized crime and hackers
9. Cloud storage data exfiltration
10. Misconfiguration and exploitation of containers and serverless workloads
11. Insecure software development

The last two deserve a more detailed discussion, which we will do in the next chapter about DevSecOps.

Good examples of companies that made big investments in security are VMware and ServiceNow.

VMware transformed itself from a company that virtualized server environments into a company that can perform a central role in managing multi-cloud. In 2019, it introduced Intrinsic Security, which consists of several products, including VMware Secure State. It analyzes misconfigurations of systems and threats, detecting changes that are applied to systems. It calculates the security risk of these systems and is able to automate remedial actions when systems are at risk. In order to do so, security engineers need to load baselines into Secure State, this tool measures the compliance of systems. Secure State is multi-cloud and can be used as a single tool on top of Azure, AWS, GCP, OCI, and hybrid platforms that hold both public and private clouds. The latter does not necessarily have to be built with VMware and can also run, for example, Hyper-V or OpenStack.

In ServiceNow, enterprises can configure the same functionality using SecOps and **Governance, Risk, and Compliance** (**GRC**). GRC can be seen as the repository that holds the security policies and compliance baselines of an enterprise. Next, GRC continuously monitors the compliance of systems, analyzes the business impact of risks, and collects audit data. SecOps is the SOAR module of the ServiceNow suite; it continuously monitors the security posture of the entire IT environment and can automatically mitigate security issues, based on security incident response scenarios that are defined as workflows in SecOps.

A workflow can, for example, include a system being suspended when SecOps detects that software has not been checked for patches in more than 3 months. If the enterprise has a compliance rule that states that software needs to be checked for patches at least once every 3 months, an automated workflow could trigger the action to suspend the use of the software.

One final product that we will review here is Azure Sentinel, the native SIEM and SOAR solution for Azure. Sentinel does what all SIEM and SOAR solutions do: collect data, check it against compliance baselines that have been defined in Azure, and respond to threats and vulnerabilities with automated workflows. It also uses artificial intelligence to detect and analyze possible attacks, by learning the behavior of systems and users. With Sentinel, Microsoft has a very extensive suite of security solutions in the cloud with Defender, Cloud App Security, and Microsoft Defender for Cloud. Although Sentinel is based in Azure, enterprises can also connect, for instance, AWS CloudTrail and GCP to Sentinel using the Microsoft Defender for Cloud Apps, part of Microsoft 365 Defender. This product is a **Cloud Access Security Broker**(**CASB**). Over the years, Sentinel has matured into a more agnostic SIEM, as recognized by market analysts.

This list of tools and suites is, of course, not exhaustive. Enterprise architects and security specialists should, together, start gathering requirements from a business, define the needed security level of systems against compliance frameworks, agree to the security processes between the business and IT, and then decide what sort of security tools would best fit the requirements. SIEM and SOAR solutions are complex. These solutions can add a lot of value to safeguard the security posture of an IT environment, but careful consideration and an evaluation of the business case are needed.

**Summary**

Enterprises use a wide and growing variety of cloud solutions. Cloud platforms, systems, software, and data need to be protected from threats and attacks. Likely, a company will also have a variety of security solutions. To create one integrated view of the security of the entire IT environment, companies will have to implement security tooling that enables this single point of view. In this chapter, we looked at SIEM and SOAR systems, tools that can collect data from many different sources and analyze it against security baselines. Ideally, these tools will also trigger automated responses to threats, after calculating the risks and the business impact.

The functionality and differences between SIEM and SOAR have been explained. After reading this chapter, you should have a good understanding of how these systems can integrate with cloud platforms.

In the last section of this chapter, leading SIEM and SOAR solutions were discussed. The chapter concludes this section of our book about security operations, or SecOps. In the next chapter, we will learn how to integrate SecOps in software and system development using DevOps and how we can mature organizations, using the DevSecOps maturity model.

**Questions**

1. What does SOC stand for?
2. What is a common technology to integrate SIEM and SOAR systems into cloud platforms?
3. Monitoring and operations are the first level in the security maturity model. Rate the following statement true or false: the reason for this is that monitoring and operations are reactive.

**Further reading**

* *Enterprise Cloud Security and Governance*, by Zeal Vora, Packt Publishing