Essential SecOps skills

In this reading, you'll explore more about the components of Security Operations (SecOps), including why SecOps was developed and some best practices you need to know about as a cloud security professional.

The need for collaboration between teams

Security Operations (**SecOps**) is the practice of combining people, processes, business, and technology to effectively protect an organization's data and infrastructure. SecOps arose to address the issue of the *isolated* nature of security teams. Traditionally, security teams worked independently, with little communication or collaboration with other teams and departments like operations. This caused many pain points across organizations, because teams were siloed from one another, and because security and operations teams can sometimes have conflicting goals. Operations teams are responsible for managing the day-to-day activities of an organization's technology services, so they prioritize uptime, efficiency, and speed. In contrast, security teams focus on meeting security standards and prioritize minimizing risk.

SecOps takes a collaborative approach by combining the expertise of security and operations teams to address the concerns of both security and operations. SecOps integrates security practices into day-to-day operations, with security and operations teams collaborating to ensure a unified approach to protecting assets and maintaining operational continuity.

Note: You might come across the term *SecDevOps*, which is a collaborative approach that integrates security practices into the software development lifecycle and operations.

The components of SecOps

Recall that the main components of SecOps are:

- Logging and monitoring
- Incident detection and management
- Incident response
- Incident recovery

Logging and monitoring

Logging and monitoring a cloud environment are integral responsibilities of a SecOps team because it helps detect anomalies and mitigate security incidents. Before you can monitor a cloud environment for suspicious activity, you need access to this activity through logs. **Logging** involves recording events occurring on computer systems and networks. Once

activity is logged, you can better monitor everything that's happening in your cloud environment. You must be able to interpret a variety of different log formats and monitoring metrics to identify security threats.

With cloud scalability, organizations can instantaneously deploy new resources. This can cause organization activity to quickly grow, and security teams need a way to efficiently log and monitor all of this. Security tools centralize this large volume of activity and provide you with improved visibility into your cloud environment. Some examples of centralized logging and monitoring tools in Google Cloud Platform are Cloud Logging and Cloud Monitoring.

Incident detection and management

Incident detection and management is the process of quickly identifying and prioritizing potential security incidents. This is a critical component of SecOps that involves the monitoring, analysis, and correlation of log data to identify malicious behavior and activity. By closely monitoring system activity, you can promptly prioritize security incidents.

This process includes analyzing log data, correlating events, and prioritizing incidents based on severity and potential impact. By detecting incidents quickly, you can minimize the damage and prevent further escalation. Examples of incident detection and management tools are Chronicle SIEM and Google Cloud Platform's Security Command Center, which uses specialized detectors built into the Google Cloud infrastructure to detect vulnerabilities and threats.

Incident response

Once a security incident has been identified, the security team activates the incident response process. A key document that's used during incident response is an **incident response plan** which outlines the procedures to take in each step of incident response. It defines the roles and responsibilities of each member in the security team to ensure that everyone understands their role during response. Communication protocols are also outlined to establish guidelines about information sharing and exchange within the security team and with external stakeholders such as regulatory bodies, legal teams, and more. Effective communication is essential to help security teams coordinate actions, share information, and make informed decisions. Chronicle SOAR is an example of a cloud platform you can use for incident response.

Incident recovery

Incident recovery includes actions for restoring affected systems back to their original state by repairing damage, evicting adversaries, hardening systems, and implementing new security measures to mitigate similar attacks from happening in the future. Examples of recovery actions include:

- **Resetting passwords**: If an account has been compromised during an incident, then you must require the password be reset to prevent any unauthorized access to the account.
- **Scanning for malware**: During an incident, malicious actors may install malware. By scanning your systems for malware using anti-malware software, you can identify and remove any malicious applications from your affected systems to prevent further damage.
- **Reviewing system logs**: Logs contain the details of the activity or event on a system. By reviewing these logs, you can identify additional signs of malicious activity including the extent of the damage so that you can take steps to appropriately respond to it.
- **Implementing security controls**: To mitigate and prevent similar incidents from occurring, you may need to improve existing controls or implement new security controls like restricting administrator privileges to dedicated administrator accounts only.

Google Cloud Backup and Disaster Recovery is an example of a cloud tool that SecOps can use to carry out recovery actions.

Best practices

Here are some best practices for SecOps to consider:

- **Update and improve incident response plan**: A well defined incident response plan contributes to a well orchestrated and highly organized incident response. It's important that SecOps teams regularly update and improve their incident response plans to adapt to evolving threats and apply what the teams learned from previous security incidents.
- **Utilize feedback and metrics**: Implement measurable metrics and key performance indicators to assess SecOps' effectiveness and efficiency. Analyze these metrics and actively seek input from team members, stakeholders, and incident post-mortems to find what areas need improvement.
- **Automate security processes**: Automating processes can help to free up security teams to focus on more strategic work. It can also help to improve the efficiency and effectiveness of security operations.
- **Stay up to date on emerging threats**: The threat landscape is constantly evolving, with new threats emerging constantly. This makes it crucial for SecOps teams to stay up to date on emerging threats so that they can be prepared to defend against them. This can be done by subscribing to threat intelligence feeds, newsletters, blogs, risk advisory feeds, or attending security conferences.
- **Improve monitoring and alerting**: SecOps teams must improve their monitoring and alerting capabilities to align with emerging threats and changing business goals. For example, subtle deviations from normal user patterns can be identified using advanced monitoring like behavioral analysis. Alerts provide timely awareness of problems in your

cloud environment. SecOps teams must work to create a well-defined alerting policy so that they are not inundated with excessive or irrelevant alerts and can focus on high-priority incidents.

- **Maintain a robust identity access management (IAM) strategy**: Everything in your cloud environment operates on a set of permissions which need to be managed properly to strengthen your security posture. Limiting and managing access plays a critical role in incident detection and response. For example, with IAM logs you can identify security incidents by tracking events like unauthorized access to cloud resources. It also plays a role in incident response as you can use IAM to revoke access and reset passwords to help contain damage caused by an incident.

Key takeaways

SecOps teams detect security incidents and mitigate their operational impact. By understanding how SecOps teams combine security and operations together to improve detection and efficiency, you can better protect cloud assets from security threats.

Resources for more information

Here are some resources if you'd like to learn more about SecOps:

- Google Cloud's SecOps Community offers a forum for security professionals to connect and share information and collaborate on projects.
- Google Cloud's SecOps Blog provides content on cloud security, technical deep dives, and more.
- A Youtube video playlist on SecOps.