CloudSec Fundamentals: Getting shit done

Pablo Vidal @ Segment
whoami

Pablo Vidal

Cloud Security Engineer @ Segment

Previously:

Cloud Security @ Zenefits

Security Engineer @ Hootsuite

Find me on LinkedIn

Pablo with a fresh haircut
Agenda

- What is Cloud Security?
- Planning
- Getting shit done
- Reporting
- Low hanging fruit examples
What is Cloud Security?

Cloud Security focuses on protecting the data and applications running on cloud infrastructure.

As a cloud security engineer, you need to know how to best use the services offered by your cloud provider.
Cloud Security Challenges

- You can’t make high impact changes on your own.
- Not enough planning leads to focus on low risk items.
Planning...
Planning: First steps

- Engage with other teams.
- Get their input. They’ll have security concerns.
Planning: Scenarios

With the knowledge you currently have, how would you hack your company?

Each scenario should have two metrics:

- Facepalm rating 😑 salarié
- Company ending scenario ☠️☠️☠️☠️

Share this scenarios with your peers. They’ll have valuable input on these scenarios.
Planning: Create projects based on scenarios

Create projects to mitigate the scenarios.

Two new metrics on these projects:

- Level of Effort: ☹️☹️☹️☹️
- Risk Mitigated: 🔥🔥🔥🔥🔥
Planning: Add projects to the roadmap

How to prioritize?
Sort by: Risk mitigated - Level of effort

Examples:
Enable MFA on AWS Root accounts:

- Level of Effort: 
- Risk Mitigated:

Service to Service Authentication:

- Level of Effort: 
- Risk Mitigated:
### Roadmap

<table>
<thead>
<tr>
<th>Epic</th>
<th>JUN</th>
<th>JUL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MFA on AWS Root accounts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrate AWS with Okta</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify Data stores with PII</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove all IAM Users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service to Service Auth</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Getting shit done...
## Getting shit done: Start taking on projects

Iterate fast and try to stay away from going down rabbit holes.

Keep solutions as simple as possible and don’t reinvent the wheel.

<table>
<thead>
<tr>
<th>Epic</th>
<th>JUN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MFA on AWS Root accounts</td>
<td></td>
</tr>
<tr>
<td>Integrate AWS with Okta</td>
<td></td>
</tr>
<tr>
<td>Identify Data stores with PII</td>
<td></td>
</tr>
</tbody>
</table>
Getting shit done: Finding new fires

As you know more, you’ll also identify new issues on your system.

How to deal with a new issue?

- Timebox exploration to learn about the issue or the possible solutions.
- Add it to your scenarios and create a new project.
Getting shit done: Don’t go deep, go broad

When working on a solution for a problem:

- Know what good enough is.
Reporting
Reporting:

How to measure the changes you’ve made on the first year?

- Your scenarios document + roadmap is your metric.
Side effects

Cloud security is great because of the freedom you have.

- Not only focus on security problems, but use that flexibility to focus on other areas.
- Think of the contributions you can make:
  - Save $$$ with S3 lifecycle policies.
  - Turn off legacy systems/unused resources.
Low hanging fruit examples
Low hanging fruit examples (AWS)

S3 (Simple storage service):

- S3 Bucket Policies.
- S3 Lifecycles.
- S3 Access logs.
Low hanging fruit examples (AWS)

IAM (Identity and Access Management):

- How are engineers interacting AWS?
- How are services interacting AWS?
- Bonus points on multi-accounts: IAM Analyzer.
Low hanging fruit examples (AWS)

EC2 (Elastic Compute Cloud)

- Have a dynamic inventory of which resources have internet exposure. EC2/RDS/ALB/Redshift etc.
Low hanging fruit examples (AWS)

AWS GuardDuty

- Generates alerts based on Flow Logs + DNS queries + AWS Cloudtrail logs
- Cheap compared to other third party solutions.
- Regardless of the size of your security team, enable it.
Conclusion

- Spend enough time planning.
- Go above and beyond your duties. Leverage your freedom.
- Go broad, don’t get too deep in the weeds.

Links:

- acloud.guru
- segment.com/careers/
I would like to thank Segment’s Security team. They’ve helped me a lot putting this together.
Connect with us on Linkedin: https://www.linkedin.com/company/segment-io/