Threat Detection and Remediation Workshop

Module 4 – Review, Discussion, Questions & Cleanup

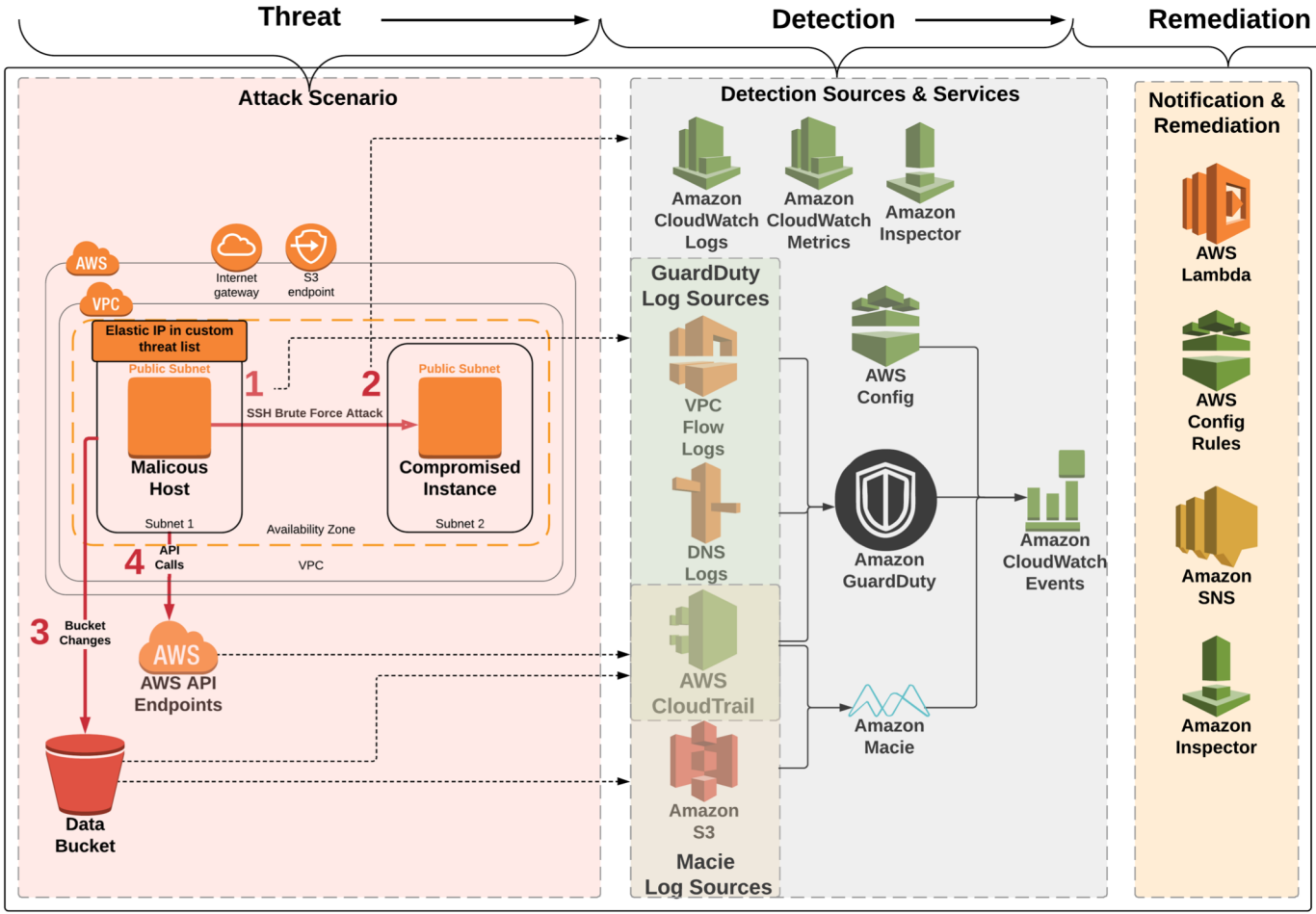
aws

Agenda

- Review & Discussion – 10 min
- Questions – 10 min
- Cleanup

Review & Discussion

What really happened?



Questions

Workshop questions

- Why did the API calls from the “malicious host” generate GuardDuty findings?

Workshop questions

- The lab mentions you can ignore the high severity SSH brute force attack finding? Why? Why is this a ”side-effect” of the simulated attack in this workshop? (hint: how does that differ from the medium severity brute force finding we investigated?)

aws

Workshop questions

- Which two AWS service provides a historical configuration change audit? Which service is easier to use for looking just at configuration changes?

Workshop questions

- Let’s assume the company policy in this scenario is that EC2 instances running Linux can only use certificate authentication. At some point somebody must have enabled password authentication on the web server. How could you determine when this was changed and by who?

Workshop questions

- We use Inspector as part of a remediation pipeline. Is inspector a Protect or Detect service (or both)?

Workshop questions

- Would the SSH brute force attack finding alone be enough to allow an automated action add an ACL to block the source of the attack? What combination of data points in this case would lead you to consider automatically remediating this threat?

aws

Workshop questions

- Macie had an alert for “S3 Bucket IAM policy grants global read rights”. We investigated that bucket in the workshop. Were the objects in the bucket publicly accessible? What about the encrypted objects?

aws

Cleanup

Useful Links

All Findings
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings.html

GuardDuty to Slack Integration:
https://github.com/aws-samples/amazon-guardduty-to-slack

Multi-Account script:
https://github.com/aws-samples/amazon-guardduty-multiaccount-scripts

GuardDuty Testing Scripts:
https://github.com/awslabs/amazon-guardduty-tester

Macie blog with test data :
https://aws.amazon.com/blogs/security/classify-sensitive-data-in-your-environment-using-amazon-macie/

Thank you!