

Threat Detection and Remediation

Workshop

Module 4 – Review, Discussion, Questions & Cleanup

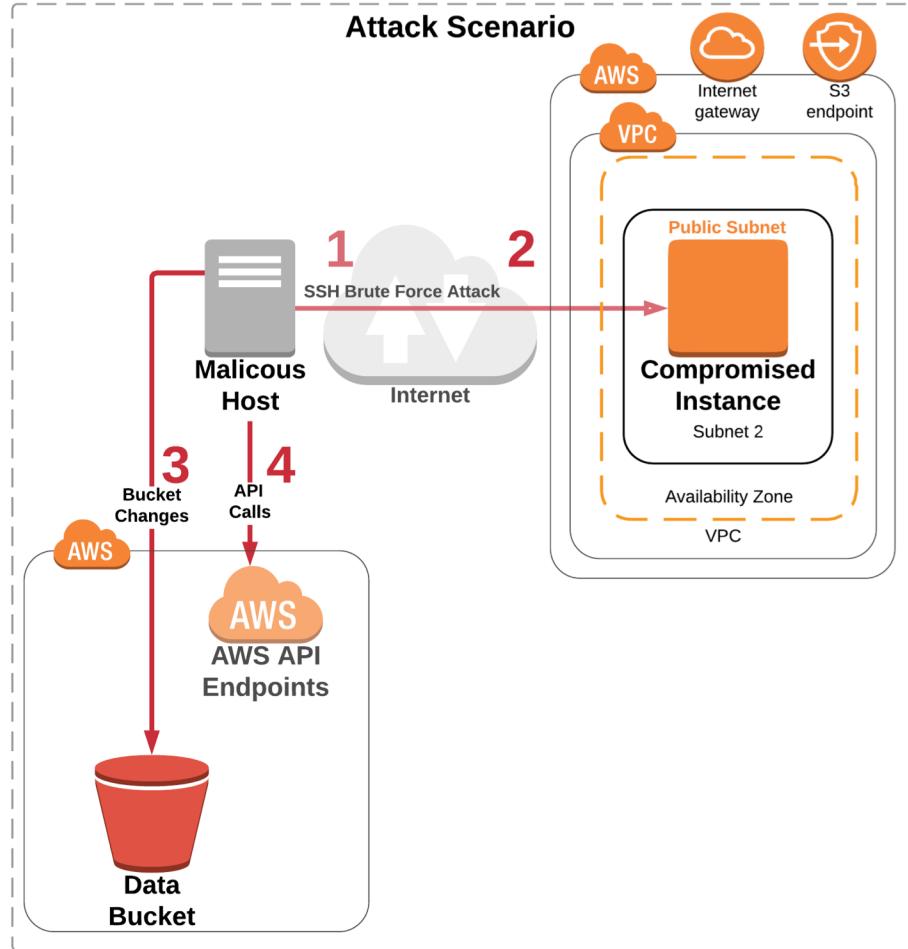
Agenda

- Review & Discussion – 5 min
- Questions – 15 min
- Cleanup

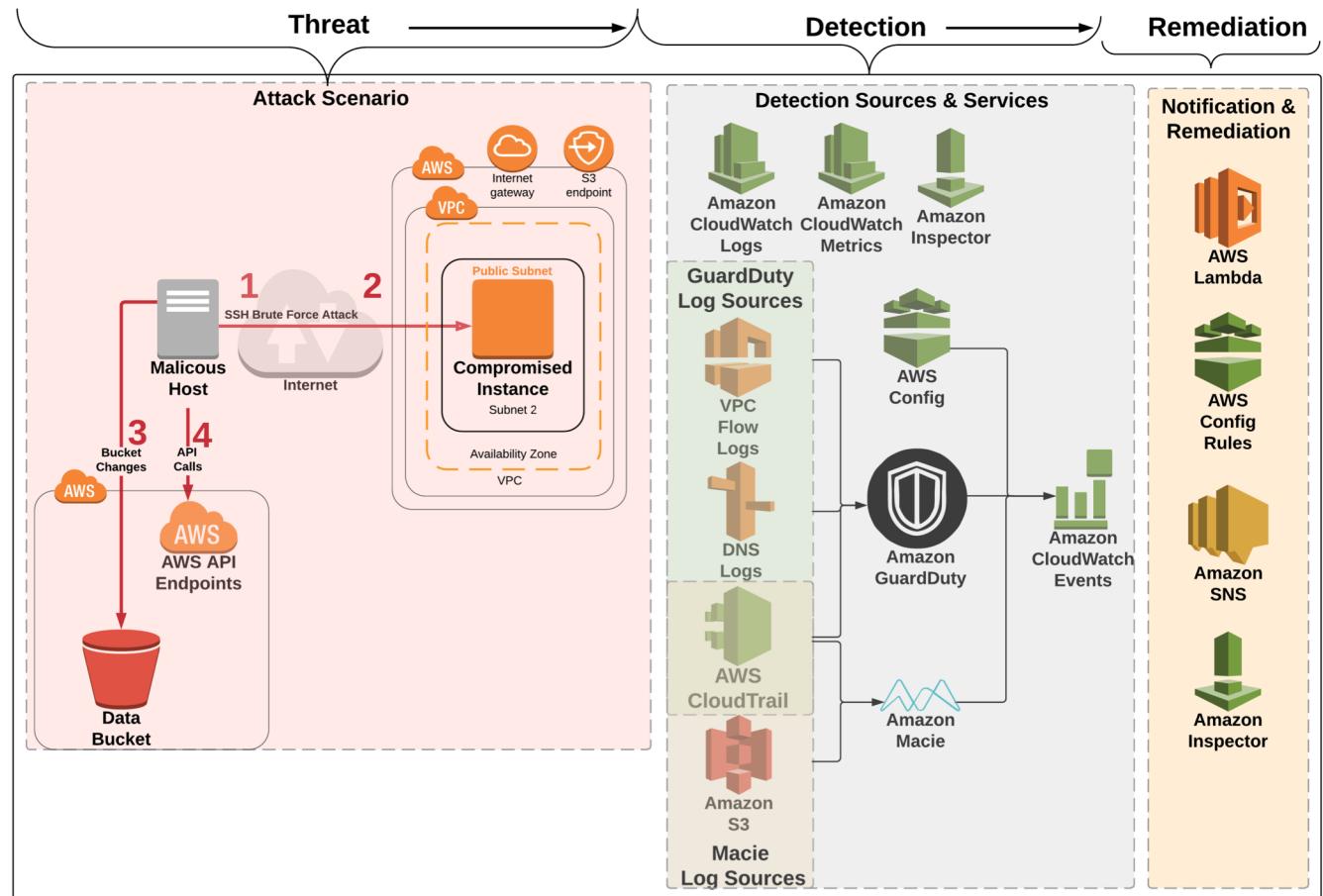
Review & Discussion



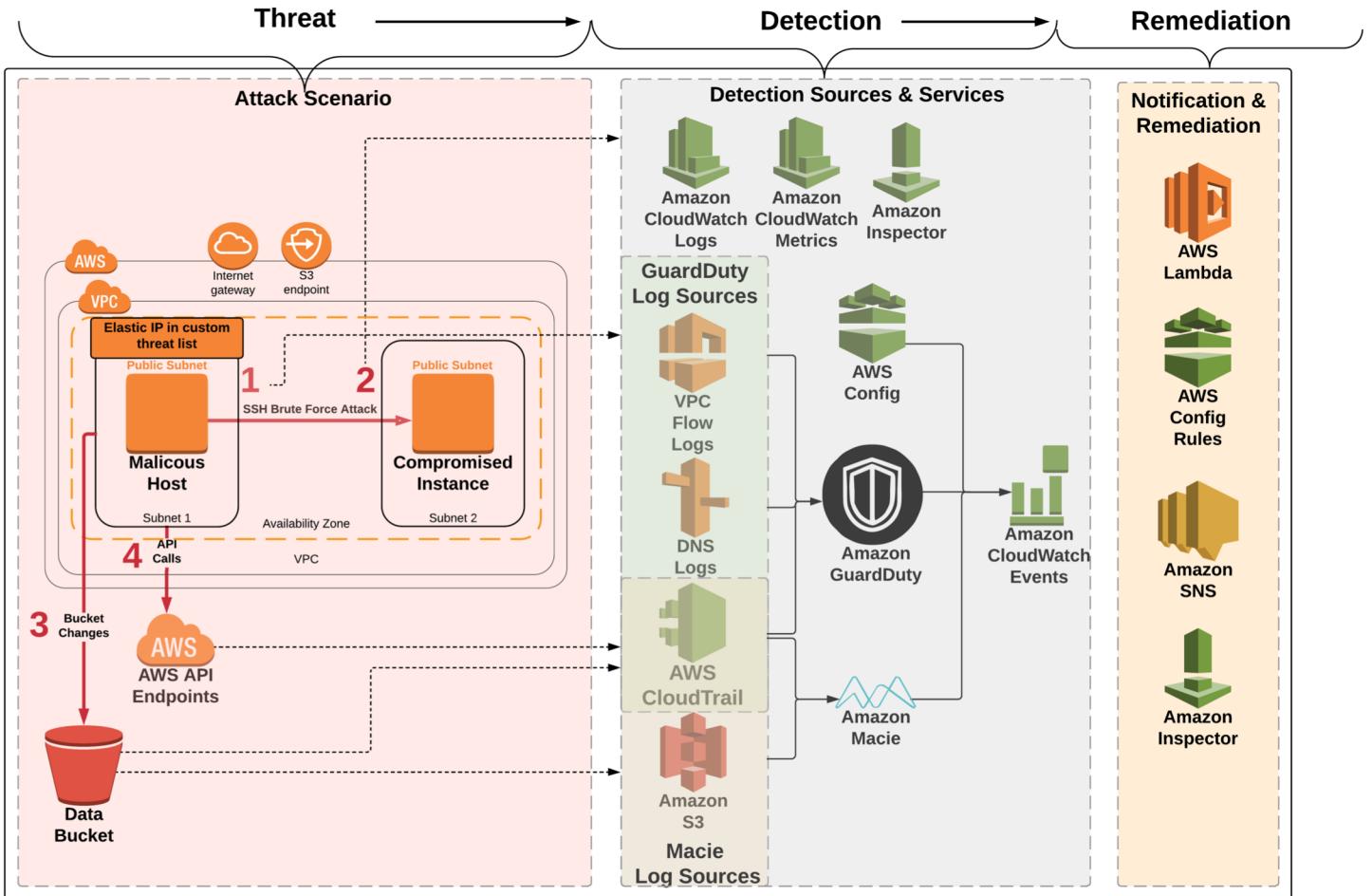
The Attack



Module 2 setup



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?)

Workshop questions

- Which two AWS service provide a historical configuration change audit?
- Which of the two is really designed (and much easier to use) for analysis of 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 whom?

Workshop questions

We use Inspector as part of a remediation pipeline. Is Inspector a protect or detect service (or both – or other)?



<https://www.nist.gov/cyberframework>

© 2018, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Workshop questions

- Would you consider a single SSH brute force attack finding by itself be enough to kick off an automated action to add an ACL to block the source of the attack?
- What combination of data points would lead you to consider automatically terminating the compromised instances?

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 actually publicly accessible?
- What about the encrypted objects in the bucket?

Cleanup

Links we discussed

<https://aws.amazon.com/security/>

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

<https://www.nist.gov/cyberframework>

https://d0.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf

https://www.forbes.com/forbesinsights/bmc_security/index.html

Thank you!