Scaling security, one human at a time

Eric Brandwine
Distinguished Engineer, AWS Security
AWS
Tell me about the tools that you have, purchased or built, that enable you and your team to scale up to handle security for all of AWS
Bananas for scale
Bananas for scale
Culture
**culture** *(n)*

- the customs, arts, social institutions, and achievements of a particular nation, people, or other social group

- the attitudes and behaviors characteristic of a particular social group
Tenets
tenet (n)

- one of the principles on which a belief or theory is based
- an axiom
Our tenets

(unless you know better ones)
We lead in preventing unauthorized access to AWS resources: our customers’ or ours. We continuously assess our systems, identify exposures, evaluate risks, and relentlessly drive mitigations.
We constantly provide visibility to senior leadership into the biggest potential risks, backed up with data and carefully prioritized.
We escalate appropriately yet aggressively to ensure that security issues are resolved promptly and with high judgement. If in doubt, we will escalate.
We are guardians of customer privacy and trust. We advocate for our customers in all security engagements.
We own security for all of AWS, including third-party and open-source software. We take nothing as a given and extensively test all of our components, even those built by other parts of the company. If something doesn’t work for us, we will move off of it.
Rejected Takeoff

2139:59 PIC  (steer) lock is on.
2140:02 PIC  (steer) lock is on.
2140:03 PIC  (steer) lock is on.
2140:04 PIC  (steer) lock is on.
2140:06 PIC  (steer) lock is on.
2140:07 PIC  (steer) lock is on.

Engine Pressure Ratio

<table>
<thead>
<tr>
<th>Engine Pressure Ratio</th>
<th>Left</th>
<th>Right</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Speed 160 kts

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.
A review of data from the airplane’s quick access recorder revealed that the pilots had neglected to perform complete flight control checks before 98% of their previous 175 takeoffs in the airplane, indicating that this oversight was habitual and not an anomaly.
“The gradual process through which unacceptable practice or standards become acceptable. As the deviant behavior is repeated without catastrophic results, it becomes the social norm for the organization.”
We own security for all of AWS, including third-party and open-source software. We take nothing as a given and extensively test all of our components, even those built by other parts of the company. If something doesn’t work for us, we will move off of it.
We are the one-stop shop for all security questions within AWS. In cases where we don’t own the answer, we own getting the question answered.
We drive our work to focus on the most critical security risks for the business. They will be prioritized first for the business and then for the service teams. We will ensure each expectation is well-understood, actionable, and supported by appropriate tooling.
What would someone in AWS Security do in this situation?

How should I make this tough choice?
Other teams’ tenets

(unless you know better ones)
AWS Cryptography

1. **Trust** is hard to earn and easy to lose. To maintain trust, we prioritize security, durability, and availability – in that order – over building new features.

2. **Durability** – We never lose a key, but will delete a customer’s key when the customer asks us to do so.
1. **Scalable** – We scale availability, speed, throughput, capacity, and robustness to support an unlimited number or variety of web-scale applications. We design our systems to use scale as an advantage so that system growth increases, not decreases, our availability, speed, throughput, capacity, and robustness.

2. **First use matters** – Our largest customer tomorrow may be using our services for the first time today. We balance our investments and aren’t afraid to self-disrupt to ensure our services remain differentiated and compelling for these customers.
Our tenets (unless you know better ones)

1. We lead in preventing unauthorized access to AWS resources: our customers’ or ours. We continuously assess our systems, identify exposures, evaluate risks, and relentlessly drive mitigations.

2. We constantly provide visibility to senior leadership into the biggest potential risks, backed up with data and strictly prioritized.

3. We escalate appropriately yet aggressively to ensure that security issues are resolved promptly and with high judgment. If in doubt, we will escalate.

4. We are guardians of customer privacy and trust. We advocate for our customers in all security engagements.

5. We own security for all of AWS, including third-party and open-source software. We take nothing as a given and extensively test all of our components, even those built by other parts of the company. If something doesn't work for us, we will move off of it.

6. We are the one-stop shop for all security questions within AWS. In cases where we don’t own the answer, we own getting the question answered.

7. We drive our work to focus on the most critical security risks for the business. They will be prioritized first for the business and then for the service teams. We will ensure each expectation is well-understood, actionable, and supported by appropriate tooling.
Thank you!