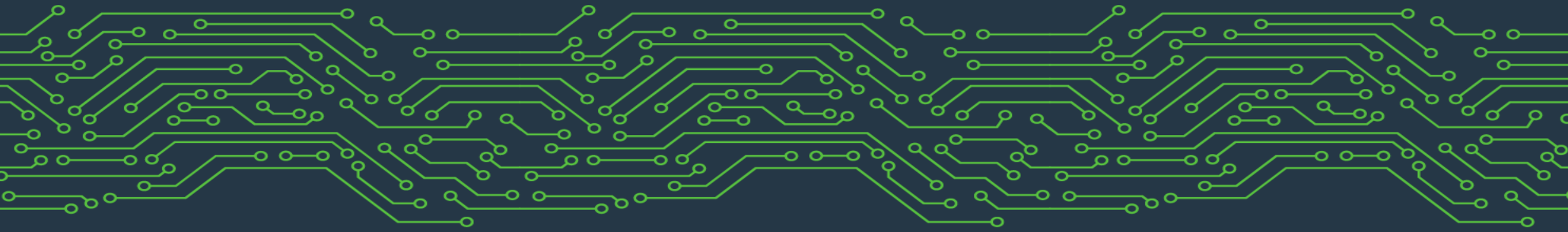
Nationwide®
is on your side

Reimagining Vulnerability Management in the Cloud



Cloud Vulnerability Management

Our Cloud Journey

Cloud Vulnerability Management Lifecycle

The Great Debate: Pets & Cattle

Zero Day Advances

Cloud Native Tooling

Our Cloud Journey – Initial Expectations

- Started journey back in 2018
- Multi-vendor cloud strategy
- Enable Self Service model
- Migrate existing applications
- Focus on speed of adoption
- Embrace DevOps
- No pets allowed mentality, everything CI/CD
- Enable rapid series innovation
- Embedded Security (seamless)
- Process automation

Cloud Transformation • DevOps • App modernization • New Roles & Responsibilities • Continuous Learning & Teaching

Our Cloud Journey – Reality

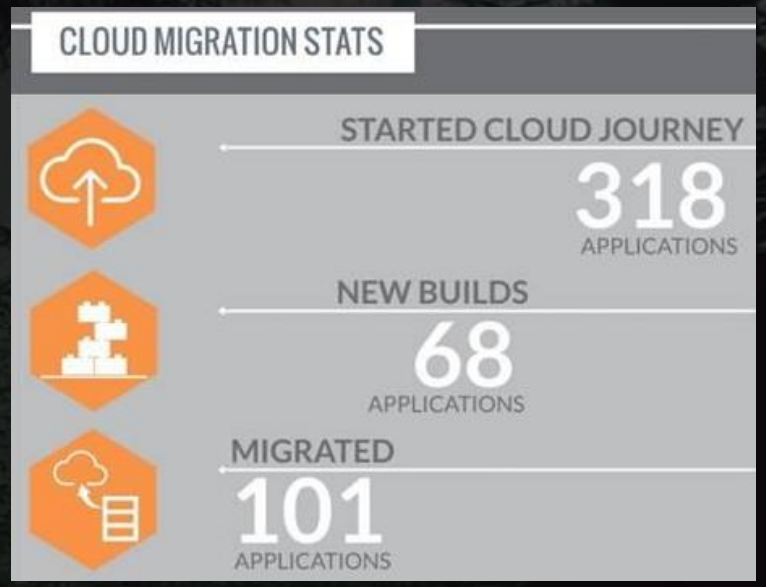
Change is hard.

There is comfort in familiar ways.

Change means being uncomfortable.


"You must be the change you wish to see in the world."
~ Mahatma Gandhi

Our Cloud Journey



2019 Migration Statistics

Our Cloud Journey – A few lessons learned

- Not all applications can reach or need full CI/CD pipeline
- 3rd party applications, vendors need to provide SaaS, Marketplace, or Cloud template solutions instead of migrating non-cloud certified packages
- Container adoption was easier and more broadly accepted
- We now have lots of Pets, but a whole lot of innovation!!!

Pets + Cattle + Ghosts

Pets

Cloud instances that need taken care of.

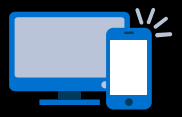
Cattle

Cloud instances built using automated tools and designed for failure.

Ghosts

Cloud instances that existed once and may reappear as a different instance. Instances that are running and no one knows they exist.

Foundational Vulnerability Management Lifecycle



Prepare – Asset Management

Identify – Detection

Analyze - Reporting

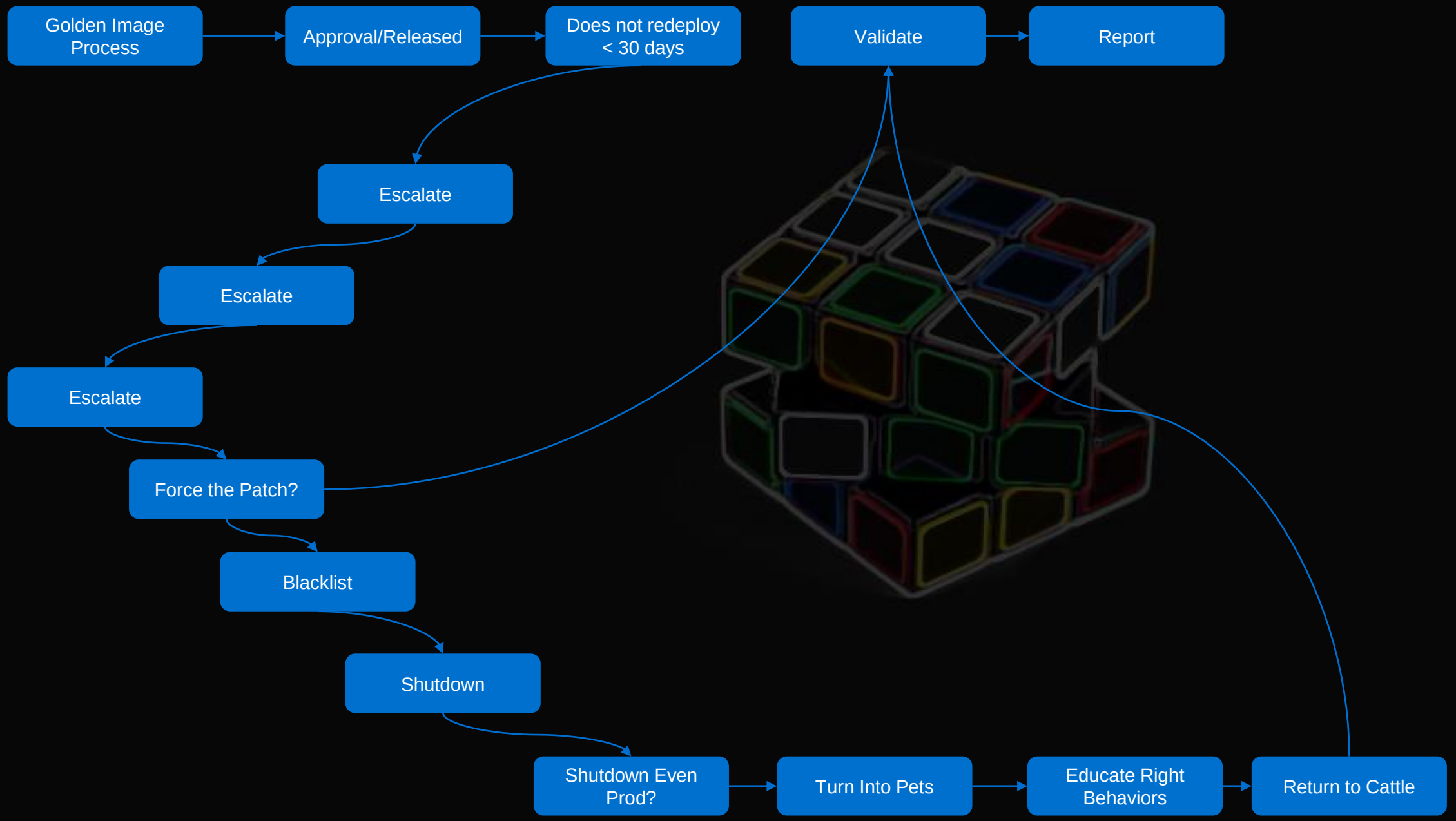
Communicate – Planning

Remediate - Patching

When cloud vulnerability practices are operating as expected

Golden Images – produce new images that meet security standards (patches) on regular basis
Approve Images – have cloud team approve images prior to publishing
Communicate that redeployments need to occur every “x” number of days
Validate – redeployments are occurring as expected
Reporting - review reports to show progress

When cloud vulnerability practices are not operating as expected



10 Things that you should consider for cloud vulnerability management

1. Accurate inventory of cloud assets
2. Determine scanning / detection tooling across CSP's
3. Test zero day response plan
4. Integrate data into reporting tools
5. Address containers differently than EC2, etc
6. Patch tooling and support (disk space, access, etc)
7. Process map all vulnerability management processes for cloud and document
8. Clear communication on roles and responsibilities and pets vs cattle
9. Plan for Non-Compliance – escalate, blacklist, shutdown?
10. Review vulnerability reporting on regular basis

Automation for the win!

Asset Inventory – system that can pull asset information automatically on regular basis

Scanning / Detection – Configure automated scanning, daily, weekly, or monthly basis. Use cloud native services where possible

Golden AMI - Implement an approval process before images are released. Have security team review standard installed software (security agents) and review vulnerability reports

Automation

Automate deployments, require app teams to rehydrate their applications every “x” days per your policy

Review your processes, look for opportunities for automation / efficiencies

Automate with blacklisting, don’t allow images to run if they are out of compliance

Automation

Integrate scanning tool outputs into your reporting mechanisms

Put accountability back on the application teams to redeploy in order to maintain compliance

Zero Day Advances

So you've discovered a new zero day..

So you've discovered all impacted assets..

So you think you've patched everything ....

Now you've reported all vulnerabilities have been mitigated...

But wait, there's more....

Cloud assets are dynamic in nature. New instances spin up and down all the time...

Example Tooling using Cloud Native Services

Amazon DynamoDB

Asset Management

AWS Lambda

Security Automation

Amazon Inspector

Vulnerability Scanning

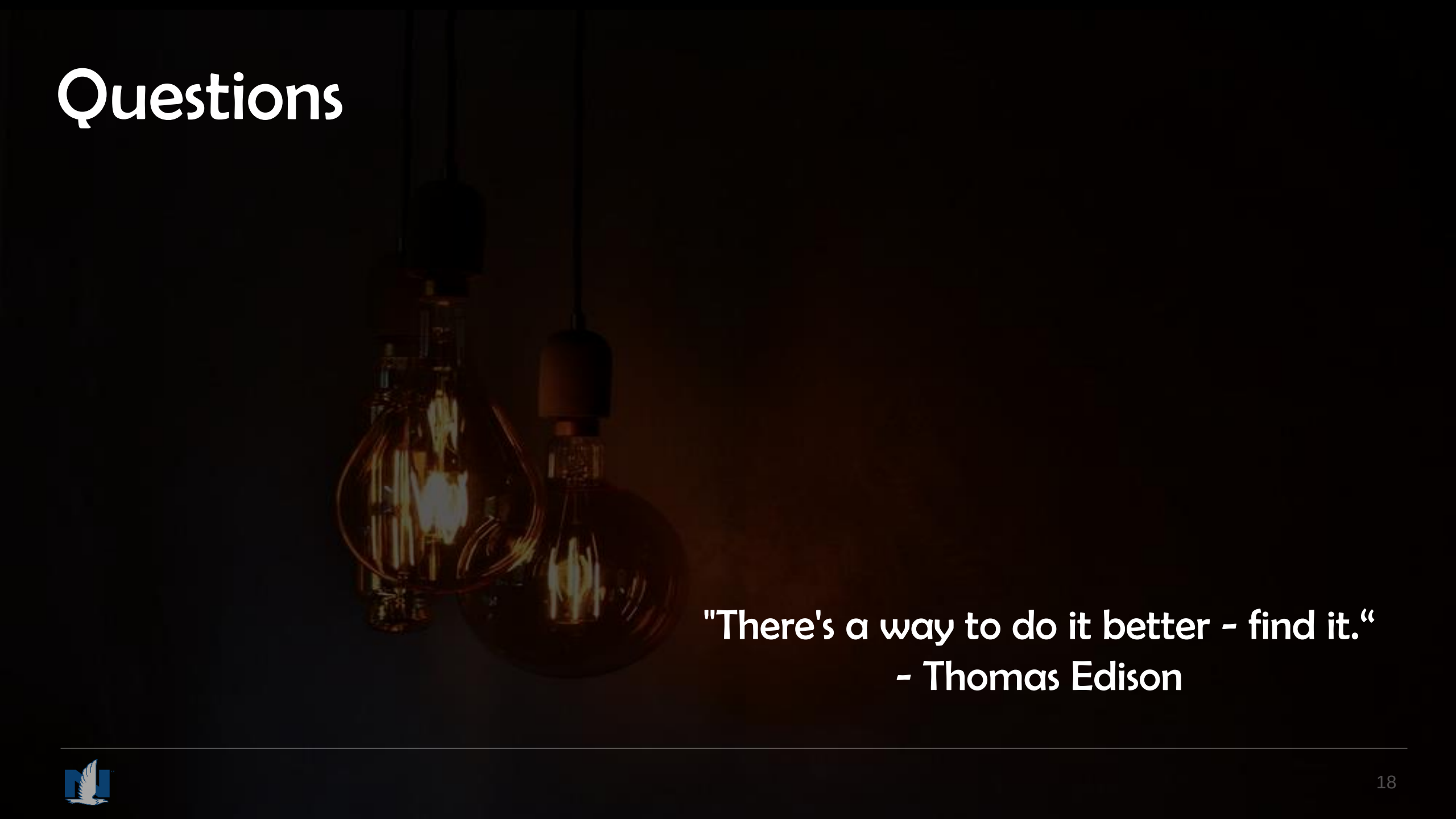
AWS Security Hub

Tool Integration

Amazon QuickSight

Reporting

Questions



"There's a way to do it better - find it."
- Thomas Edison