Learning from Cloud, Chaos and Scale: Netflix Security Intelligence and Response Team

Alex Maestretti and Swathi Joshi
@maestretti
@swathijoshi
- ‘Baking’ Virtual Machine images, called Amazon Machine Images (AMIs), from source (instead of configuring servers on the fly as you would with Chef/Puppet) provides a strong baseline for forensics.

- Any changes to be made to a server (instance), are made in code, checked into source control, and built into a new AMI - then new servers (instances) are deployed from this new AMI.

- Containers deploy the same way.
Deploying multiple copies of the same AMI not only scales load, but creates a peer group to compare against, allowing us to surface suspicious differences in our fleet.

https://www.spinnaker.io/

https://github.com/Netflix-Skunkworks/diffy
Our corporate model relies heavily on SaaS and the services we do run are launched in our cloud the same way as our product.

We isolate and devalue our user endpoints, then seek to protect our core assets in the cloud.

No lateral network access (LISA), no Active Directory, no network shares (GDrive).
Identity is our perimeter. We seek to control access to our cloud resources through Single Sign On and User Behavior Analytics.

We make access decisions based on strong identity and device health checks.

https://github.com/Netflix-Skunkworks/stethoscope-app
“We strive to respond effectively, and limit blast radius from security events...”
There are some minor exceptions to “context not control” such as an urgent situation.
Good vs Bad Process

- Tooling
- Training
- Tabletops
- Guidelines
Security Learning Organization

- **Observed Issues**
  - Vulnerability Discovery and Remediation
  - Security Incident Response
    - Post Incident Review (PIR)
      - Reflection
        - Enterprise Risk Management
          - Thinking
            - Atomic Red Team Tests
              - Process Improvements
                - Follow-on Remediation
                  - Delay
                    - Security Controls
                      - Detections
            - Security Research
                - Hunt
                  - Simulation (Tabletop, Gameday, Red Team, Automated Test, etc)
            - Hypothesized Issues
              - Security Intelligence
                - Practice
                  - Function
                    - Artifact
                      - Legend
Thank You.

jobs.netflix.com/teams/security

@maestretti
@swathijoshi
Backup Slides.
Freedom and Responsibility

Our goal is to inspire people more than manage them. We trust our teams to do what they think is best for Netflix.

There are a few important exceptions to our anti-rules pro-freedom philosophy. ... keeping our members' payment information safe, have strict controls around access. Transferring large amounts of cash from our company bank accounts has strict controls. But these are edge cases.

In general, freedom and rapid recovery is better than trying to prevent error. We are in a creative business, not a safety-critical business. Our big threat over time is lack of innovation...

Context Not Control

There are some minor exceptions to “context not control,” such as an urgent situation...

Netflix Culture Memo - jobs.netflix.com/culture

1. Encourage independent decision-making by employees
2. Share information openly, broadly and deliberately
3. Are extraordinarily candid with each other
4. Keep only our highly effective people
5. Avoid rules

Our core philosophy is people over process. More specifically, we have great people working together as a dream team. With this approach, we are a more flexible, fun, stimulating, creative, and successful organization.

https://medium.com/netflix-techblog/full-cycle-developers-at-netflix-a08c31f83249