Presents

Pragmatic Database Security: Security Program Development

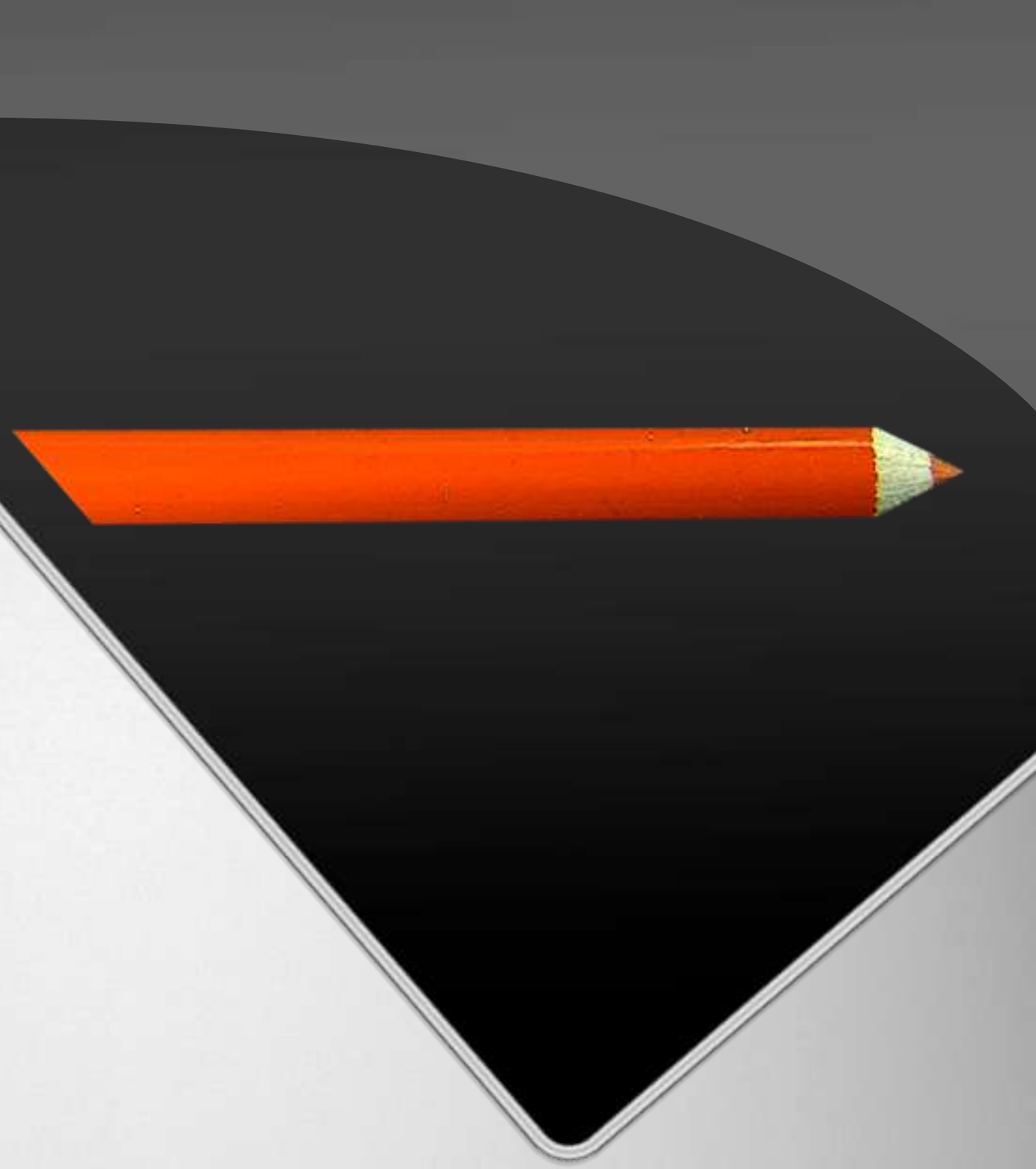
Adrian Lane, CTO/Analyst

alane@securosis.com

Twitter: @AdrianLane

Outline

- Problem Space
- Use Cases
- Program Outline
- Recommendations



How do I create a database security program?

Securosis

- All security is reactive
- When someone complains
- Squeaky wheels -- reduce security
- Head’s down, silo-ed approach
  - DBA’s, security, operations and audit all have different priorities
- When you fail an audit

When working without a plan …

Securosis

Use Case: Large Financial

- Many different types of databases
- Management segregated by database type/geography
- DBA in charge of security
- Security group understands security
- The two groups don’t talk
- Security expectations not consistent
- No configuration standard

Use Case: Mid-sized Enterprise

- We know that we're under attack
- Hackers? Crazy foreign governments? Does it matter?
- They are after the data

- ISP gave us PCI checklist
- Don’t understand requirements
- Said our databases were vulnerable
- DBA says we are patched

Use Case: Small Enterprise

Securosis

Use Case: Large Health Care

- Many different types of databases
- HUGE data volumes.
- Do security tools scale?
- How do we set configuration standards across groups/systems?
- How do we tell which users are accessing data?

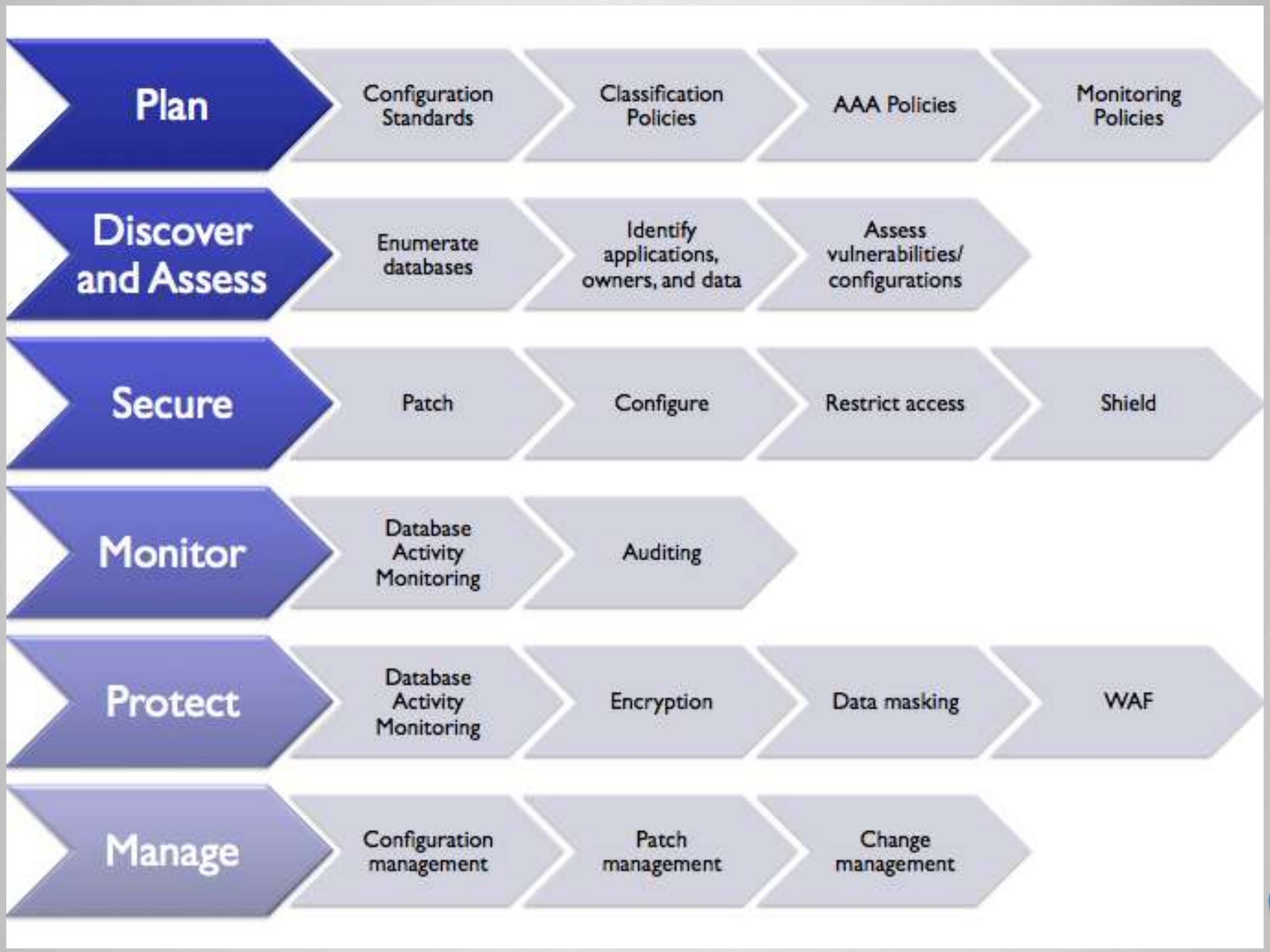
Trouble is most firms do not have policies, procedures or defined responsibilities

- What do you have?
- What are you accountable for?
- What do you not know?
- Chicken or the Egg:
  Monitoring vs. Assessment

Where do I start?

Securosis

Database Security Program

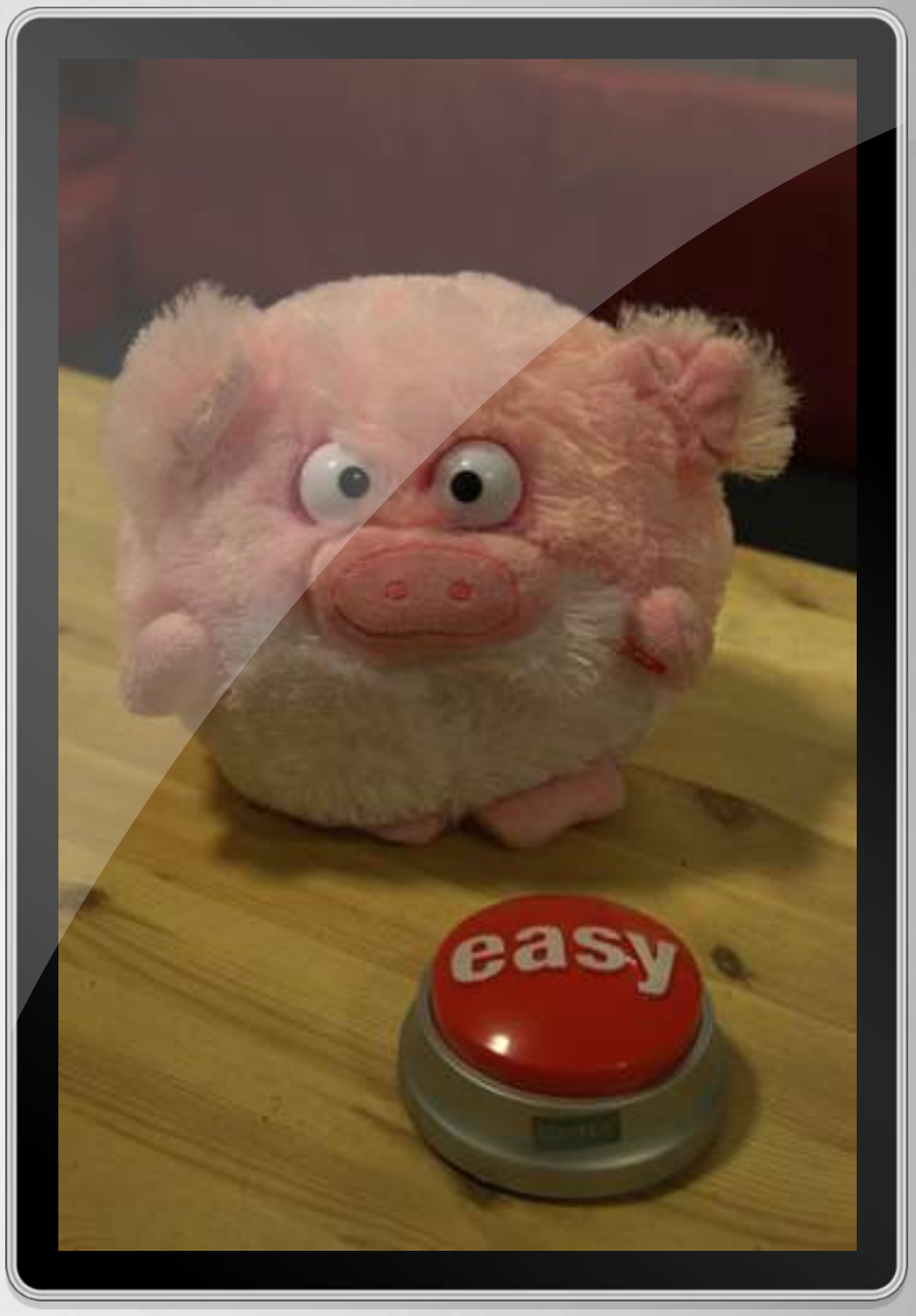


Securosis

*Which is **not** a pragmatic way to start*

Securosis

- Do what's cheap and easy first
- Find some tools:
  - Assessment
  - Discovery
  - Monitoring
- Discover what you have
- Then figure out what to do



Let's make this easier …

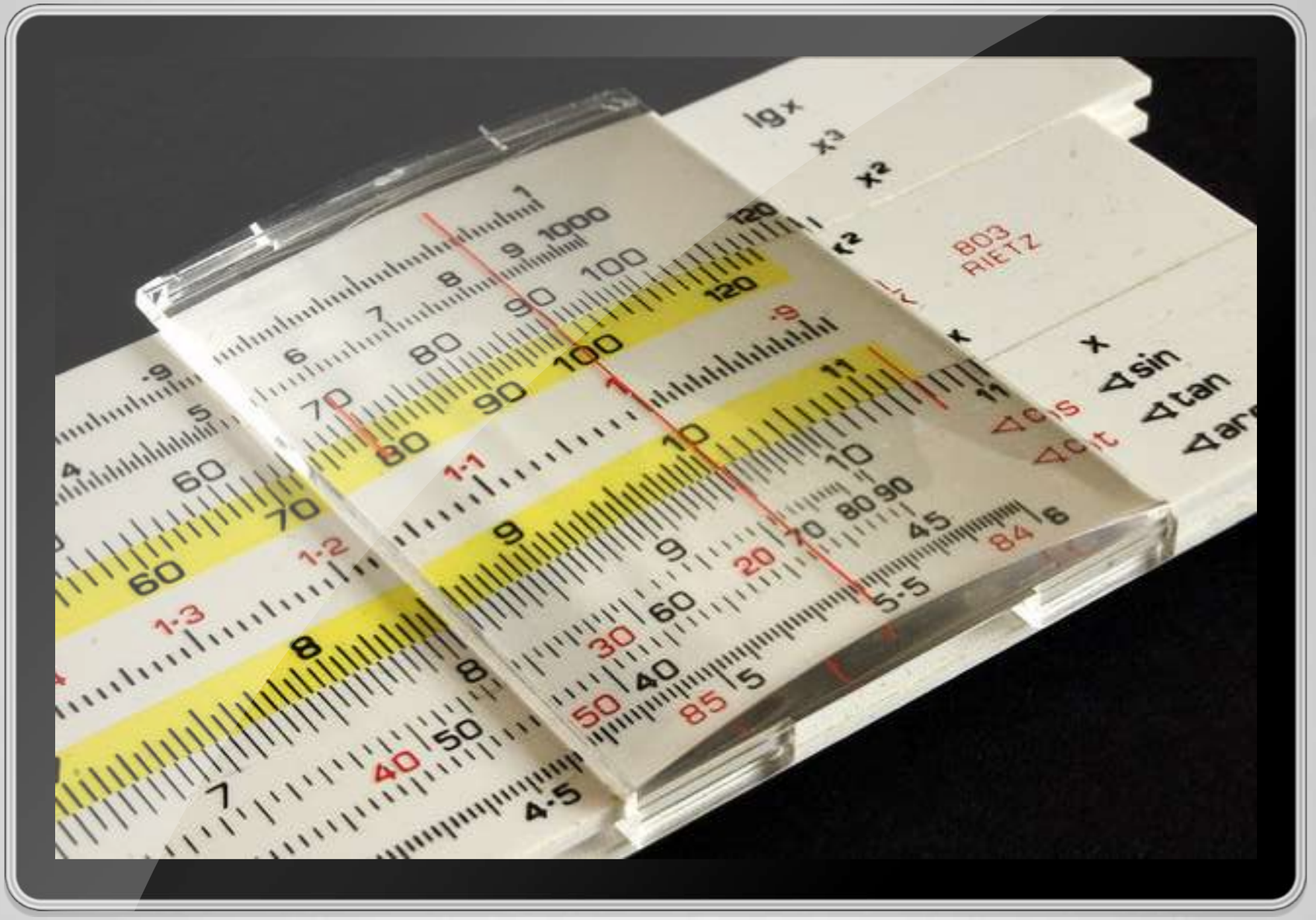
Find some tools ...
Discover what you have ...
Determine what you need to do.

Securosis

- Database discovery
- Data discovery
- Assessment
- Monitoring

What tools are at your disposal?

Securosis



Assessment

Securosis

Assessment tools provide:

- Configuration assessment
- Patch assessment
- Data & database discovery
- Catalog features
- Advise on security best practices
- Usually show roles/permissions

- What queries?
- What applications?
- What are users doing?
- What's failing?

Monitoring

Securosis

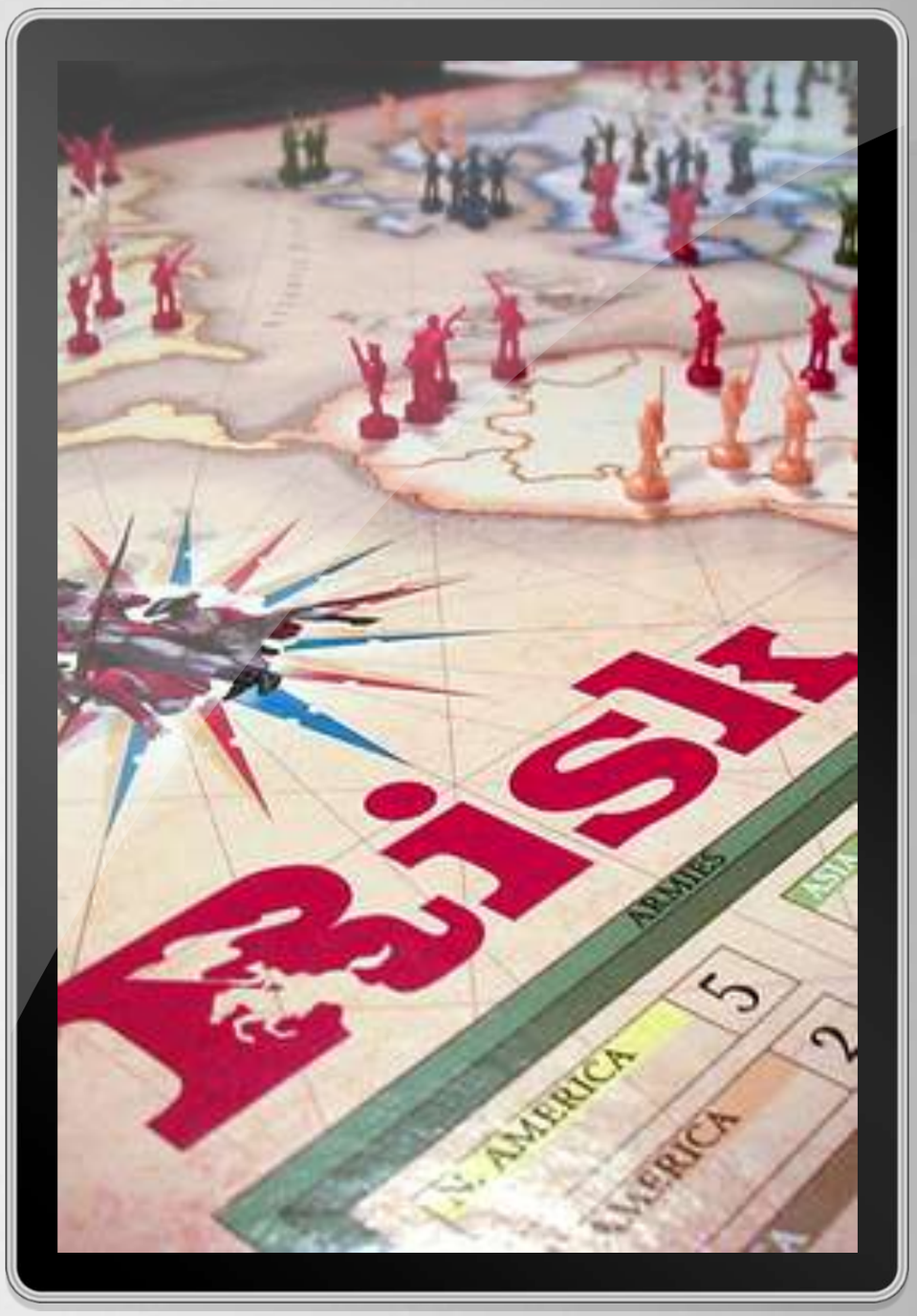
- Which users have access
- User permissions
- Group account access
- Roles
- Admin account setup
- SOD: platform vs. database
- Public access

Identity Management

Securosis

Now that you know what you have, it's time to determine what to fix.

- Answer these questions:
  - What are the security requirements?
  - What are the compliance requirements?
  - What’s the distance between where we are and where we need to be?



What is your “Risk”

Securosis

Planning Process

Prepare

- Determine security & compliance requirements.
- Identify tools
- Get access
- Automate!

Discover

- What databases do you have?
- What data do they contain?
- What's sensitive?

Assess

- How are databases configured?
- How are they patched?
- User Access Rights?
- SOD?

Monitor

- How do users use the database?
- What applications are supported?

Document & Analyze

- What did you find?
- Select remediation steps

Securosis

The tools you used to discover and plan are the same one's you'll use to implement policies.

Securosis

Recommendations

Your success depends on your ability to prioritize

Securosis

Plan For:

Identity and Access

Monitoring

Metrics

Compliance

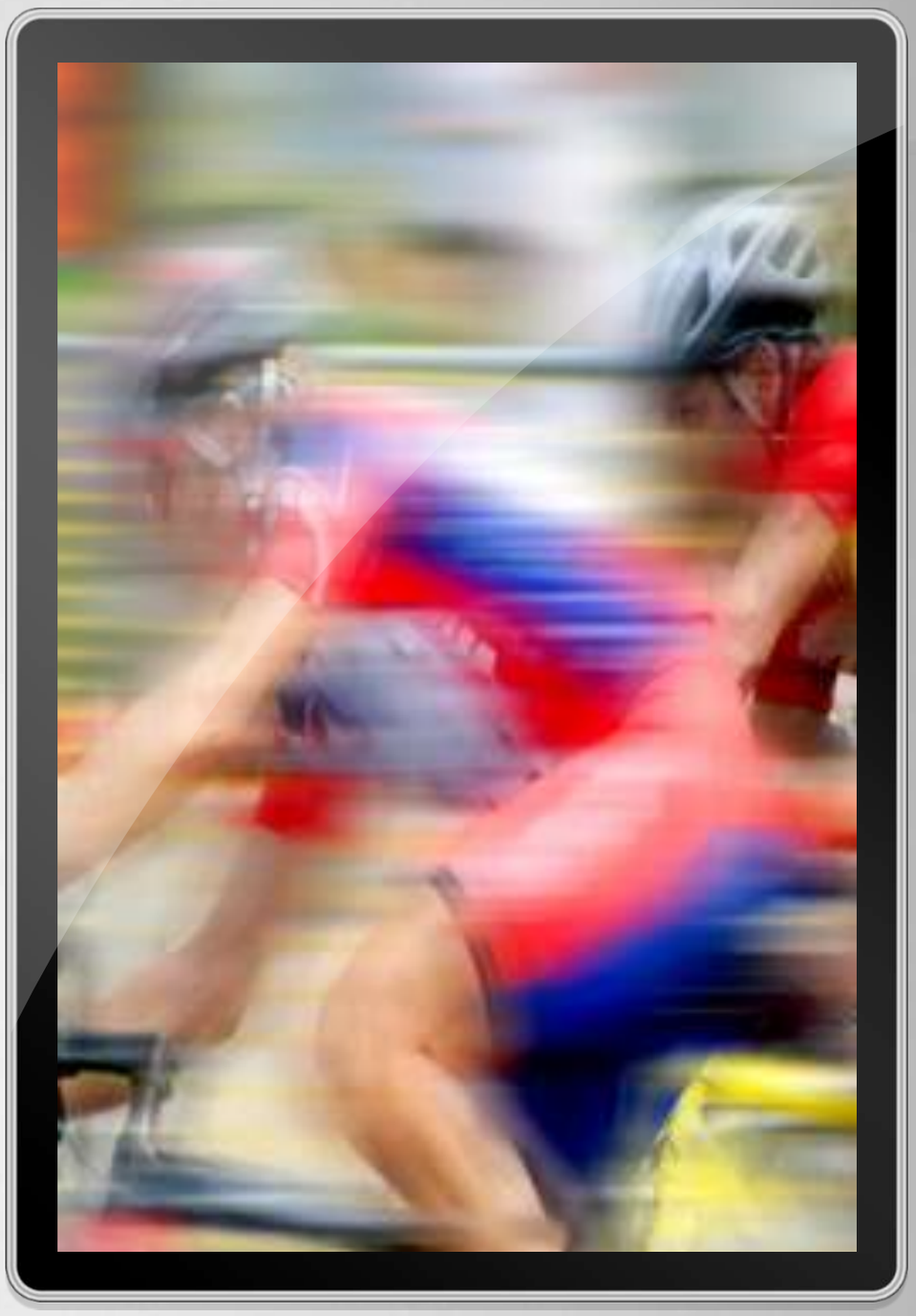
Encryption

Assessment

Threat Modeling

Securosis

- Your data center is always changing, and thus your risk is always changing.
- Iterative process
- Those changes impact the security posture, and thus the risk faced by an organization.
- Change is happening faster than ever.



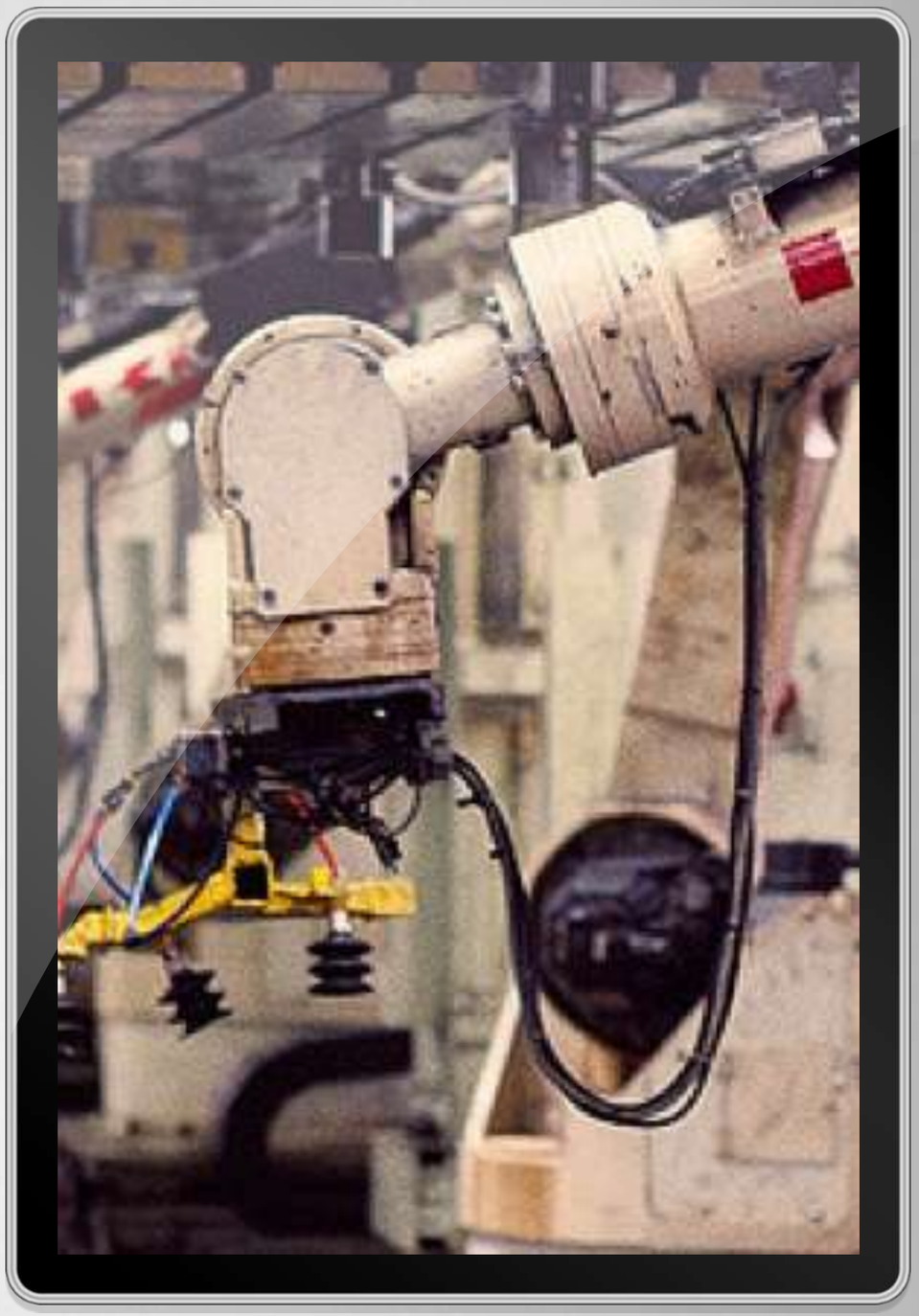
Constant Change

Securosis

Operations, Security and Compliance need to be aligned

Securosis

- You will need to continuously monitor and audit.
- You cannot keep pace with changes w/o help.
- You're not a security researcher.



Automate!

Securosis

- Do what’s cheap and easy first
- Show value of:
  - Assessment
  - Discovery
  - Monitoring
- Once you get executive buy-in, things get easier.
- That means budget and help

Start with quick wins!

Securosis

Read our stuff

- Blog
  - http://securosis.com/blog
- Research
  - http://nexus.securosis.com/
  - http://securosis.com/research
- We publish (almost) everything for free
- Contribute. Make it better.

Securosis

Adrian Lane

Securosis LLC

alane@securosis.com

http://securosis.com/blog

Twitter: @AdrianLane

Securosis