NCSHA

HFAs AT THE CENTER

AUSTIN 2018 ANNUAL CONFERENCE & SHOWPLACE

Cybersecurity: Protecting Your Clients and Organization

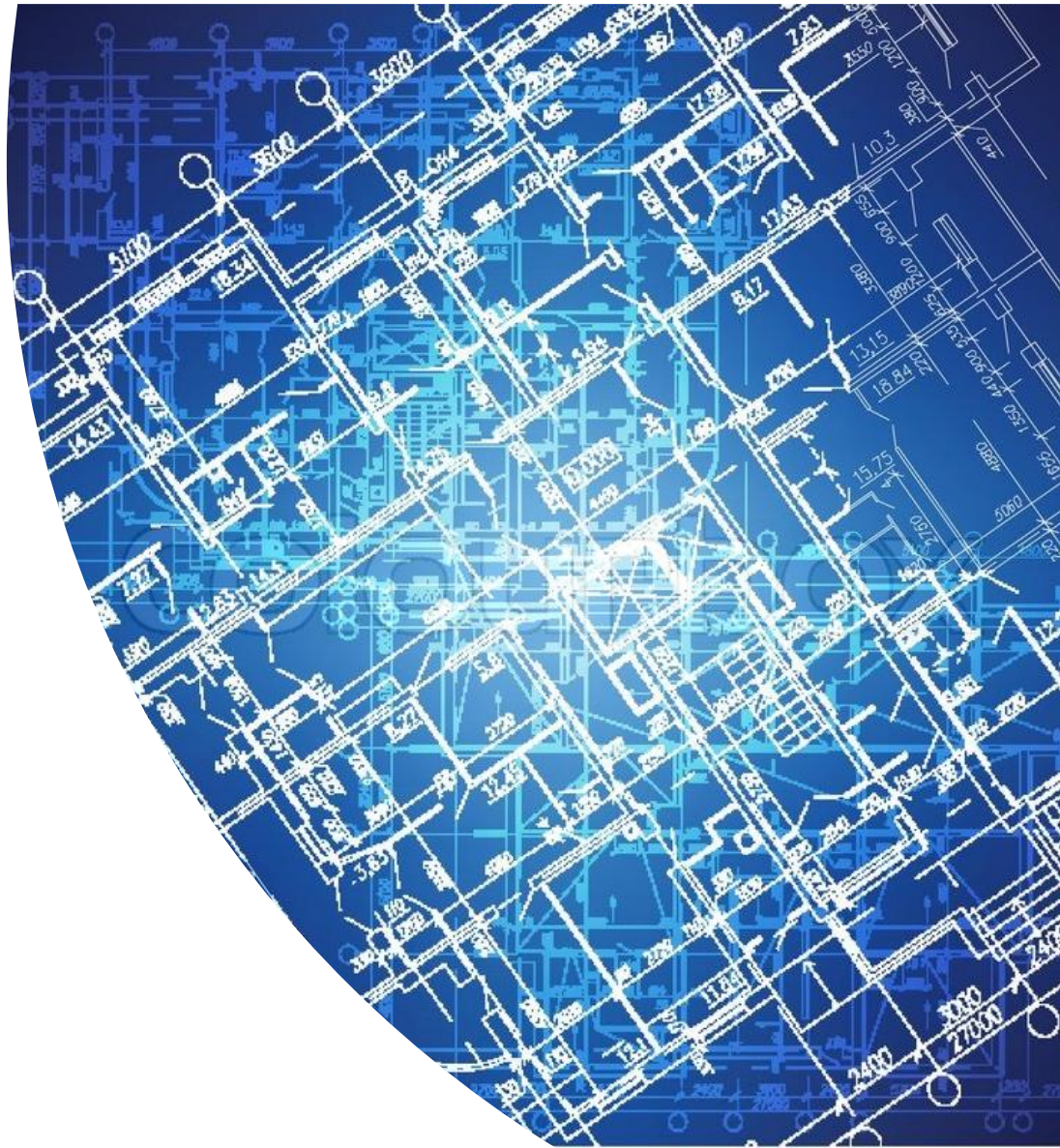
Brent Stackhouse | WP Engine

WP engine

Bio and Agenda

Brent Stackhouse
Director, Security, WP Engine –
CISSP, CISM, CRISC, GWAPT, CCSK

- 20 years+ in Information Security
  - 14 years in Austin
    - 6 years in financial services security
  - 6+ years in Seattle
    - Microsoft, Amazon, zulily



Agenda

- Foundational Assumptions
- Strategies & Tactics
- Parting Thoughts

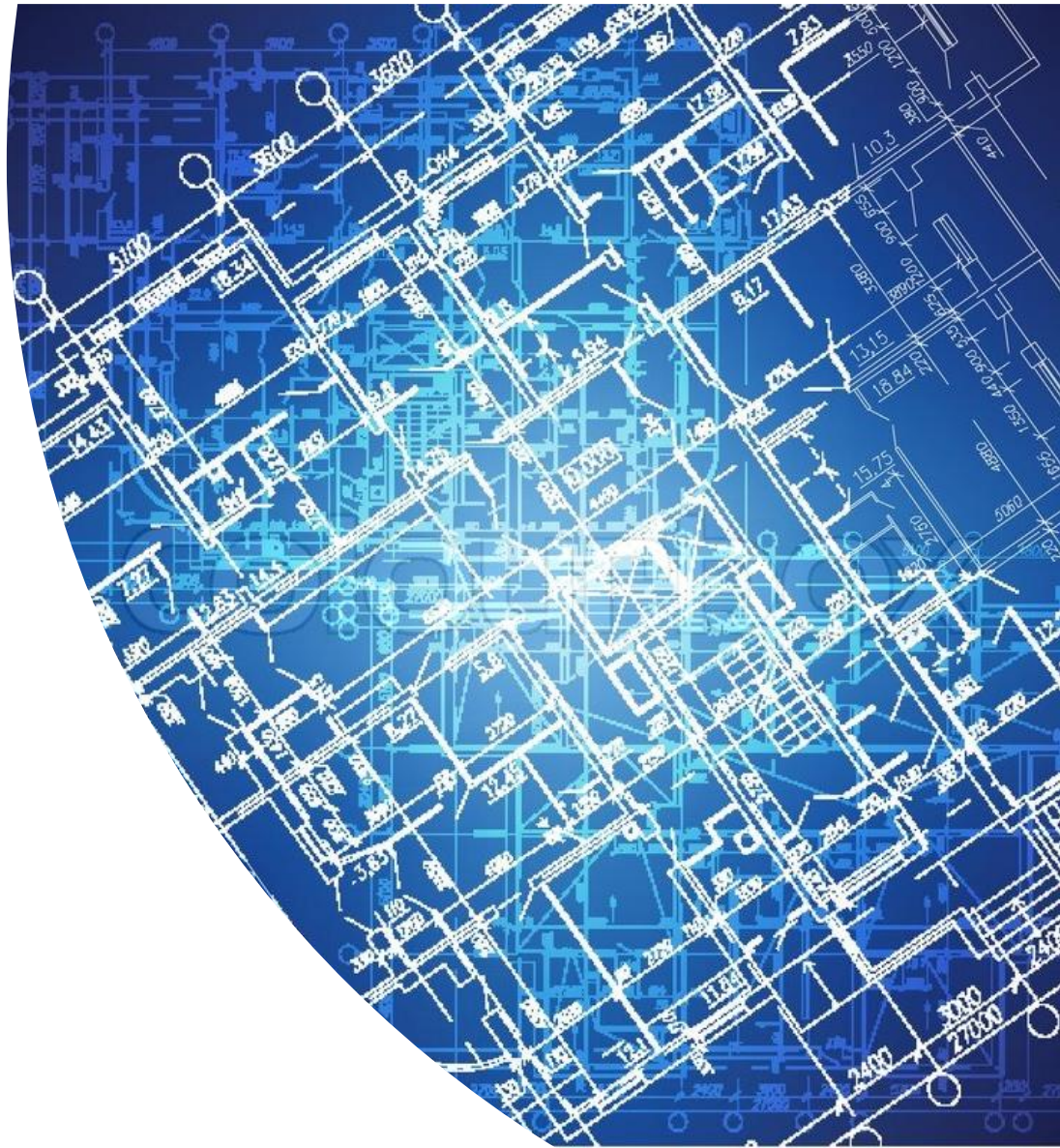
Foundational Assumptions

Foundational Assumptions

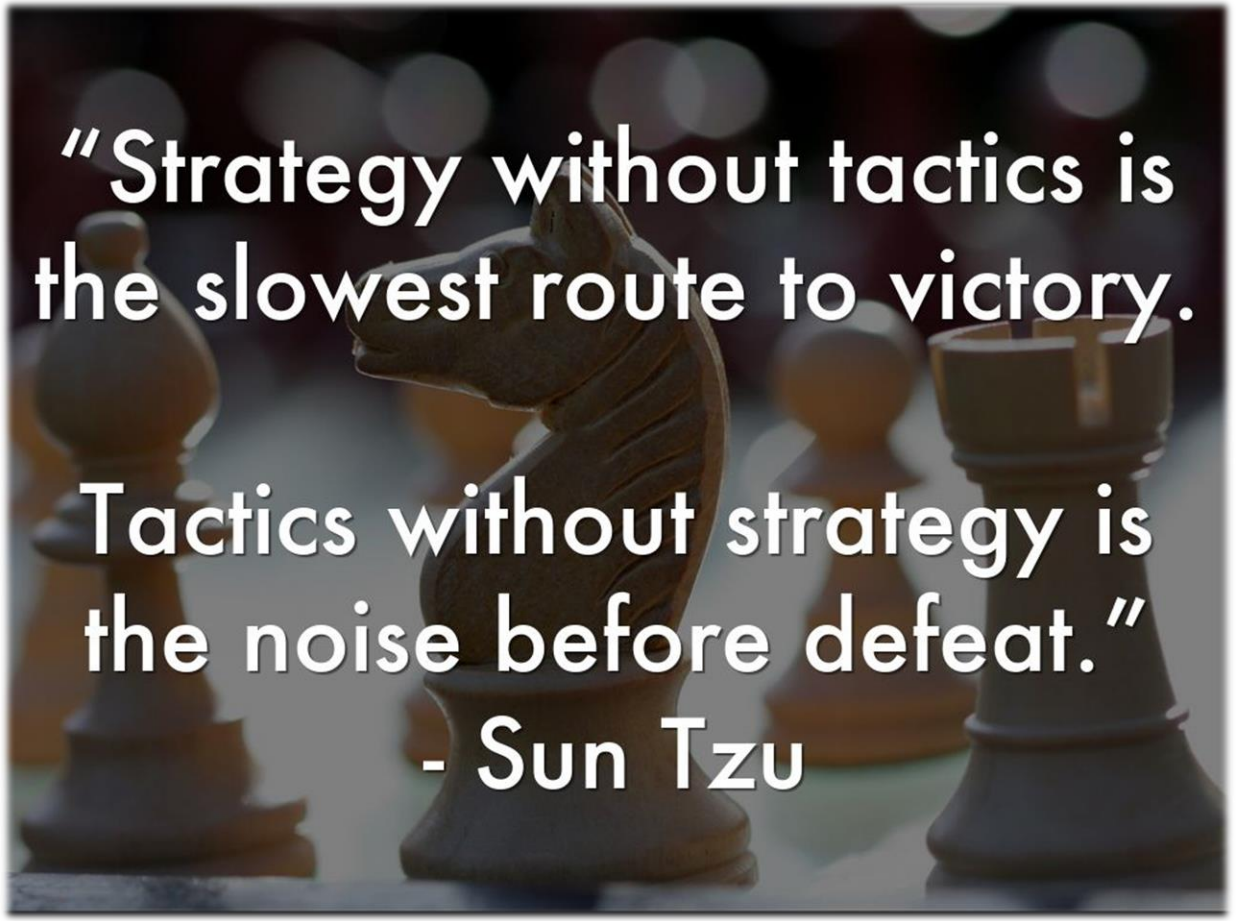
- **If**: Information Security is a risk management discipline with a strong technology component…
- **Then**: Your top security folks need to be (primarily) risk management professionals, not technologists.

Foundational Assumptions

- **If**: Your infrastructure is already (able to be) compromised...
- **Then**: You should *plan accordingly* and have multiple layers of defense.
- **Larger Point** – Your executive team should be aware of, and comfortable with, the idea that determined attackers can always find a way in – and that hopefully, you've planned for it.

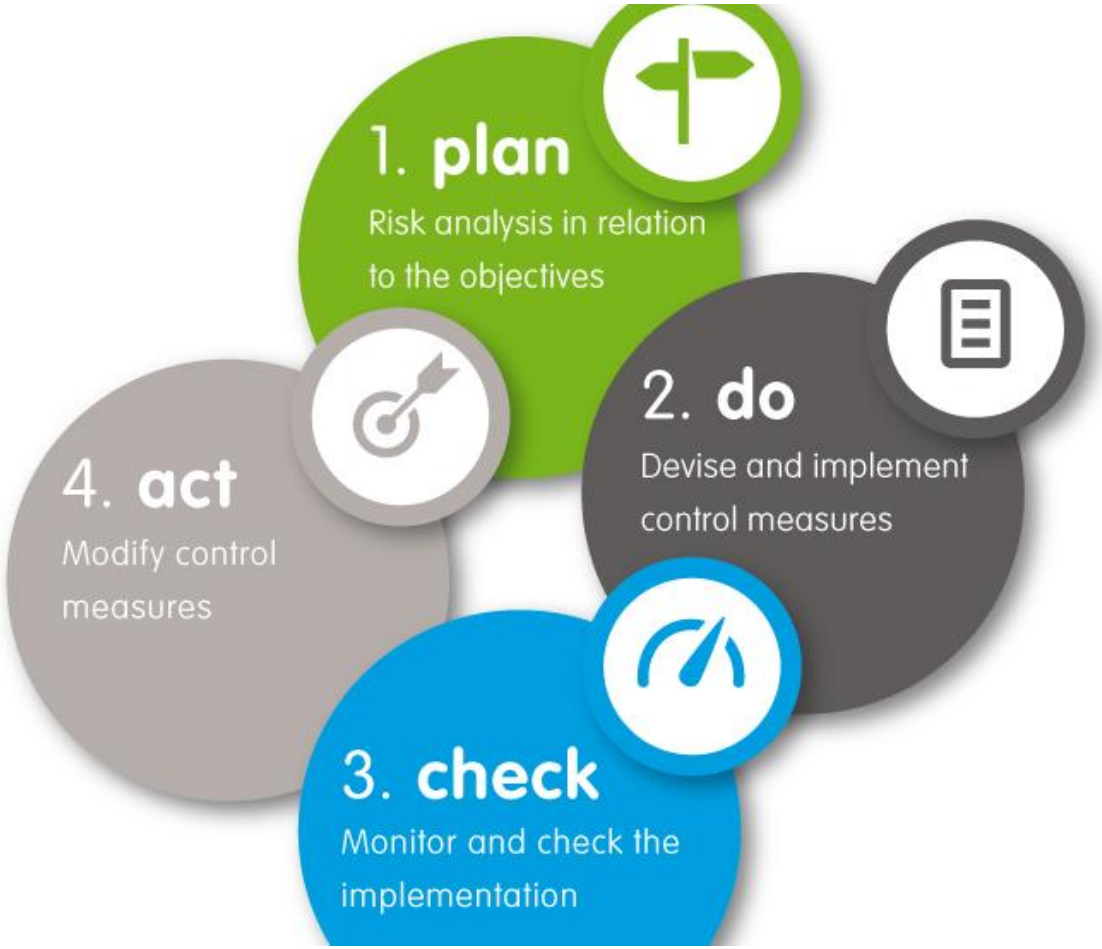


Strategies and Tactics



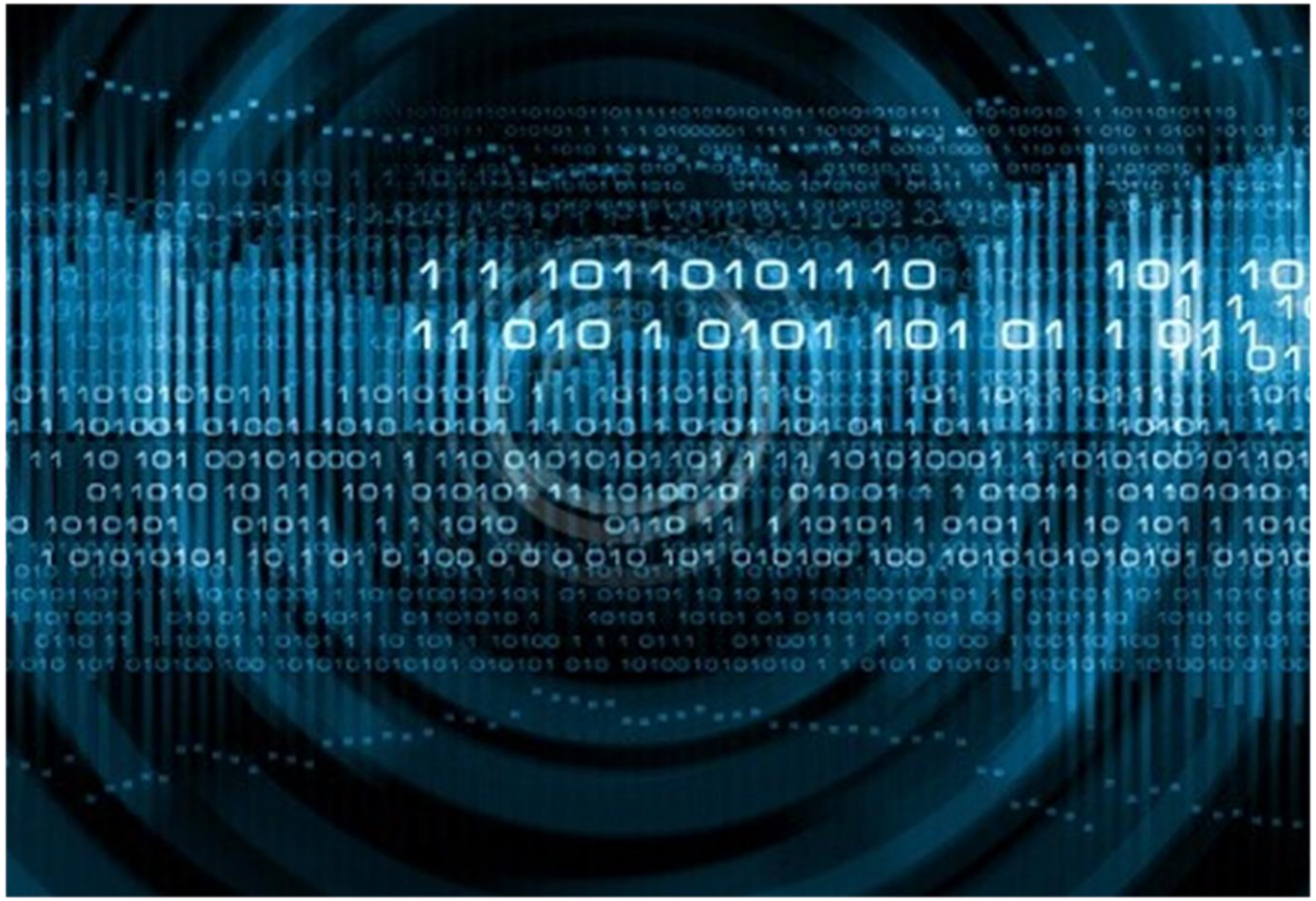
Strategic Priorities

- **Leverage an ISMS such as ISO 27001**
  - Benefits
    - Better assurance that security efforts are in sync with the business
    - Ensures risk is a core component of the overall program
    - Provides a lifecycle approach that leads to continuous improvement
- **Risk Assessment**
  - What it's not…
  - Answers the question, "Can we be breached?"
  - Business-driven while maintaining a highly-technical focus
  - Qualitative is fine, quantitative can be better
    - Keep in mind, if something's on fire, you don't need to risk assess it…



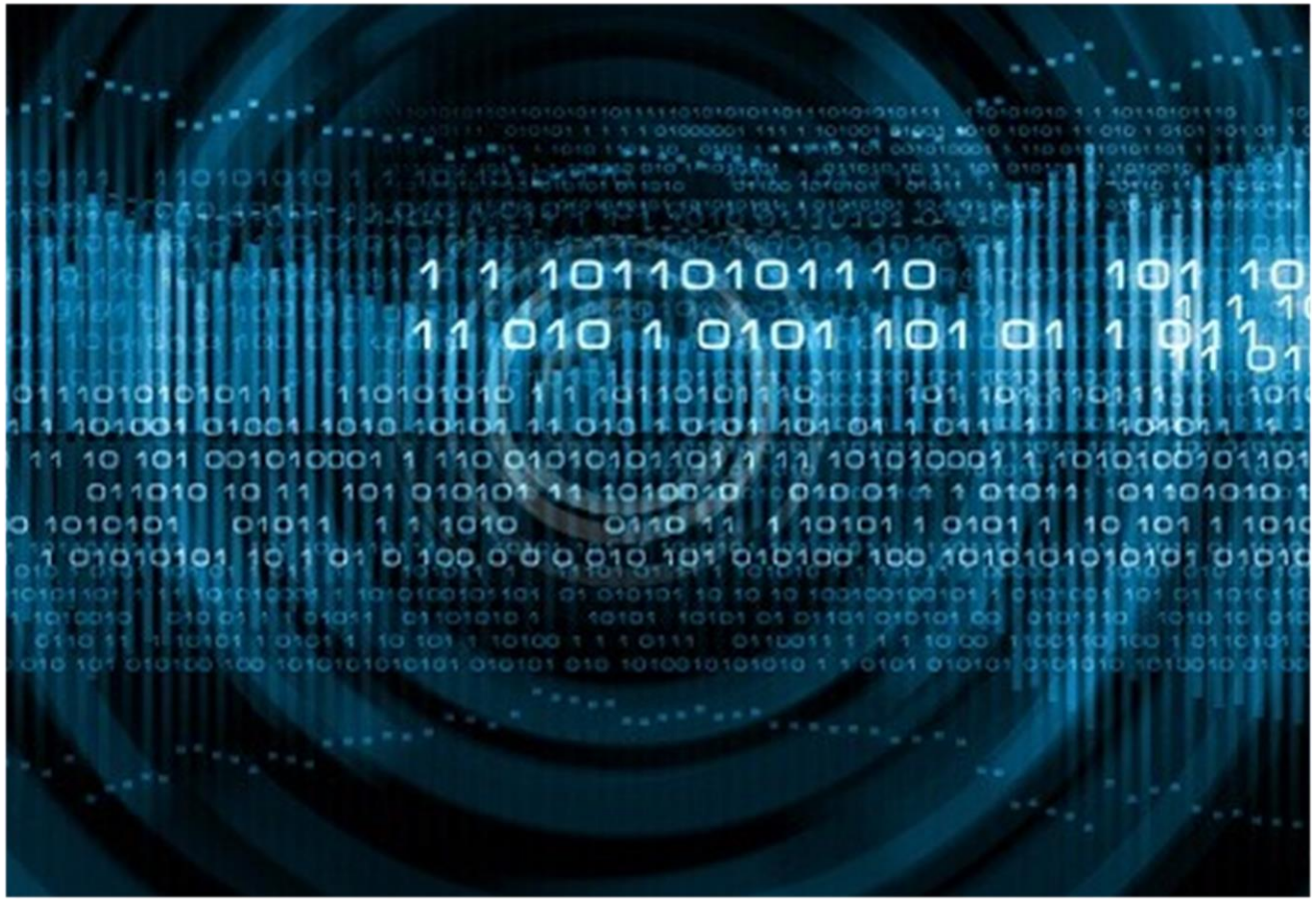
Tactical Priorities – Detection is Key!

- **Monitoring - Easy to do incorrectly.**
  - Collecting a lot of data isn't the same as collecting the *right* data
  - A patchwork approach is destined to fail
  - Don't expect a single platform to (easily or cheaply) accomplish the two primary use cases of monitoring



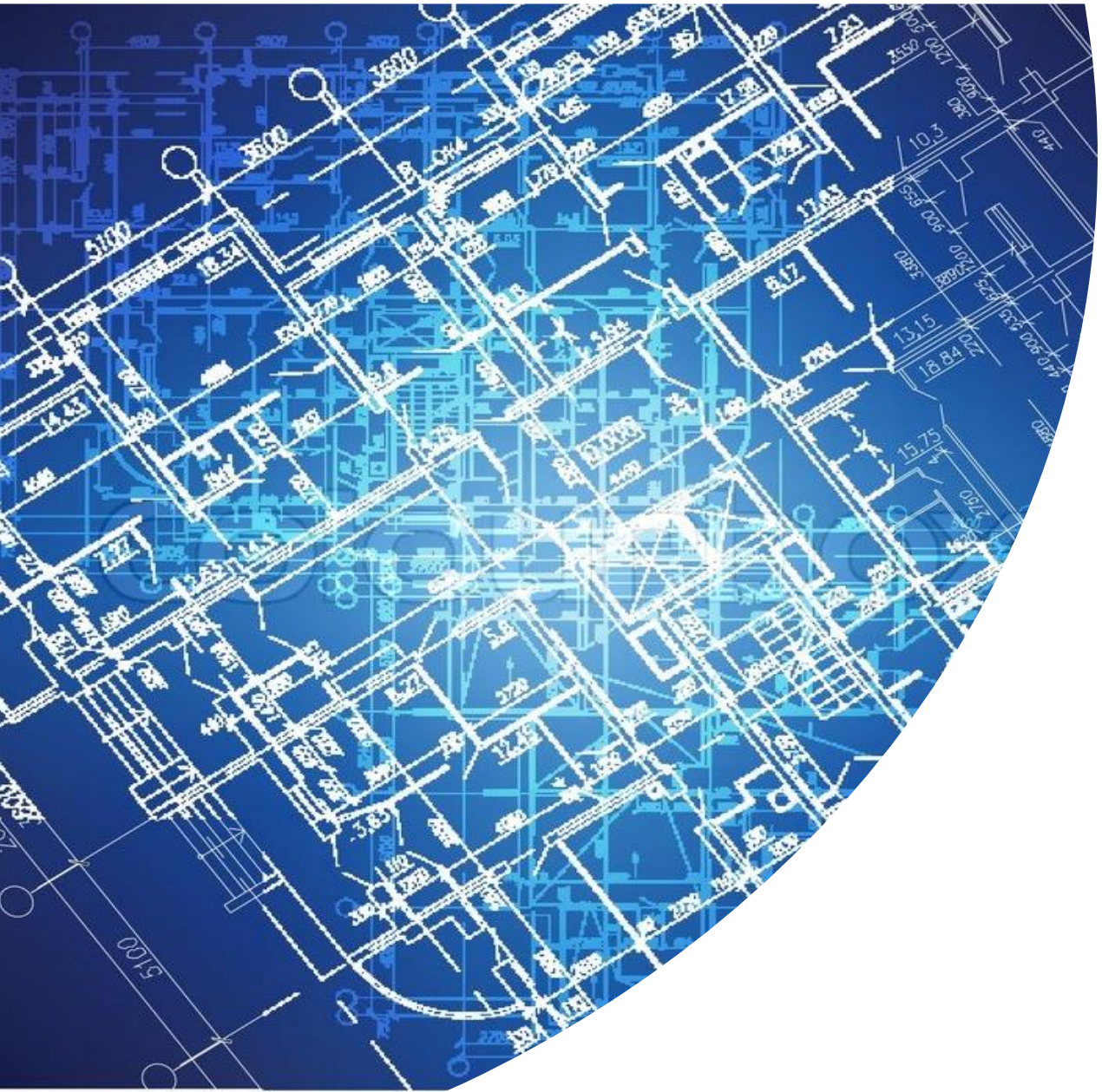
Tactical Priorities - Monitoring (cont.)

- **How to do it right (at scale)**
  - Perform a threat modeling exercise first
  - Perform a gap analysis
  - Collect data centrally
  - Create detections and alerts carefully



Parting Thoughts

- Risk trumps Technology
- Strategy trumps Tactics
- Monitoring is Mandatory



Thank you!