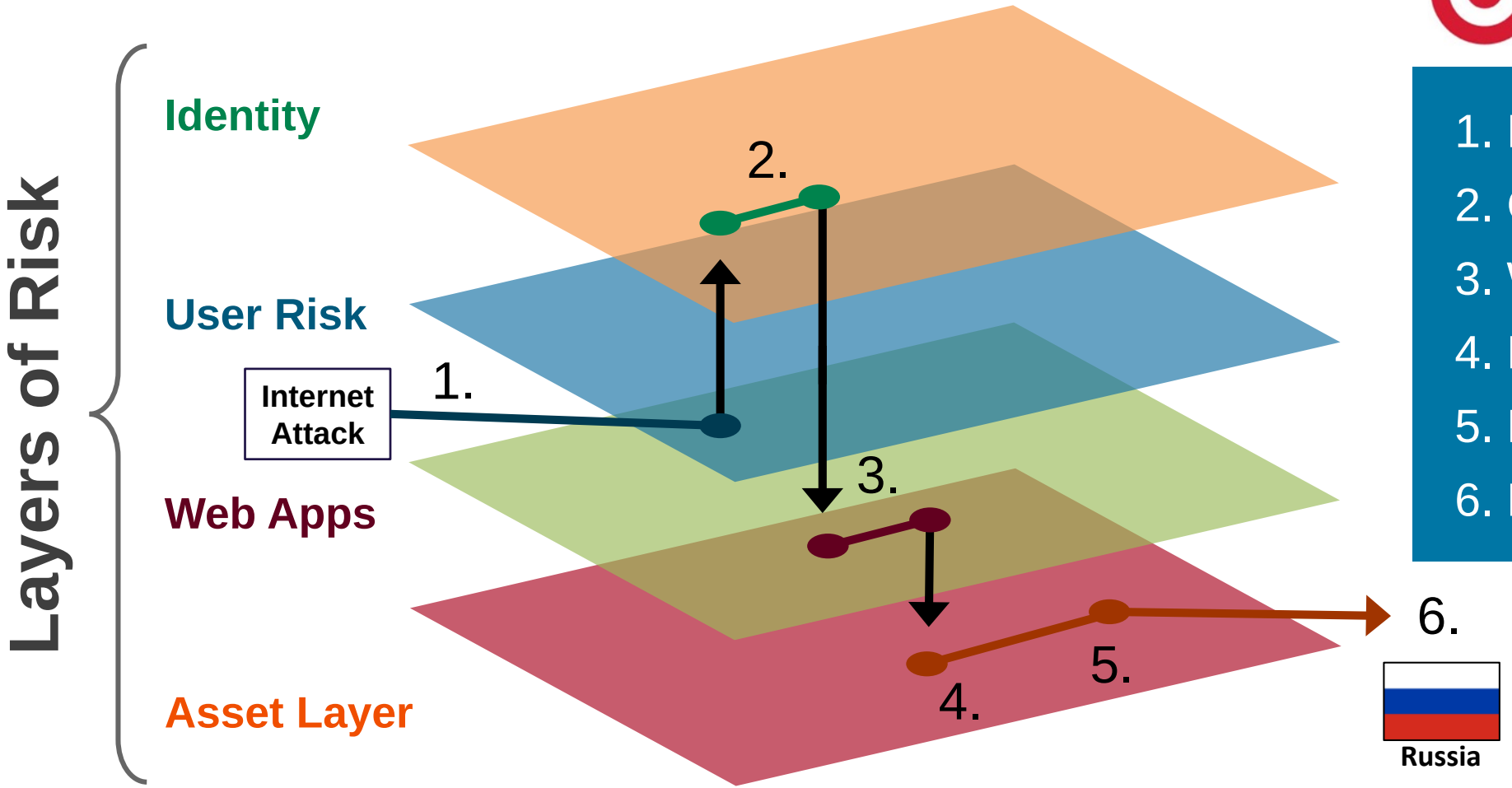
Comprehensive Attack Intelligence

Katherine James, SVP – Global Sales

6/23/16

Anatomy of a Cyber Attack



TARGET

1. Partner Phished
2. Credentials Stolen
3. Web app used
4. Network accessed
5. PoS system reached
6. Malware extracts

CORE SECURITY

By the Numbers

700K+

Vulnerabilities

93K – Highs

241K – Mediums

353K - Lows

Some Math….

93K+

High Threat Vulnerabilities

250

Working Days

=

372

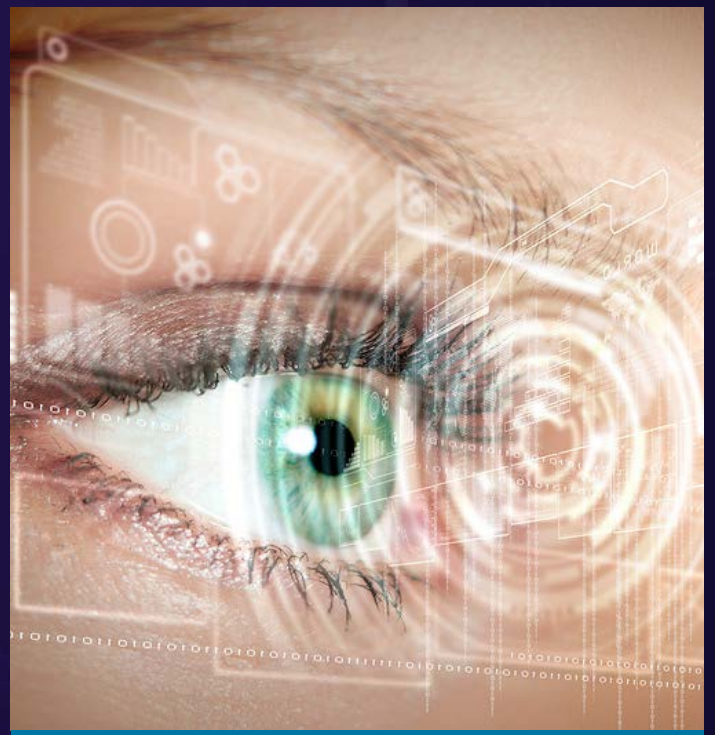
Vulnerabilities needed to be fixed EACH DAY

CORE SECURITY

What About Identity Risk?

Stolen Credentials

Passwords



Multi-factor Authentication

The Problem: “We Are Overwhelmed by Data”

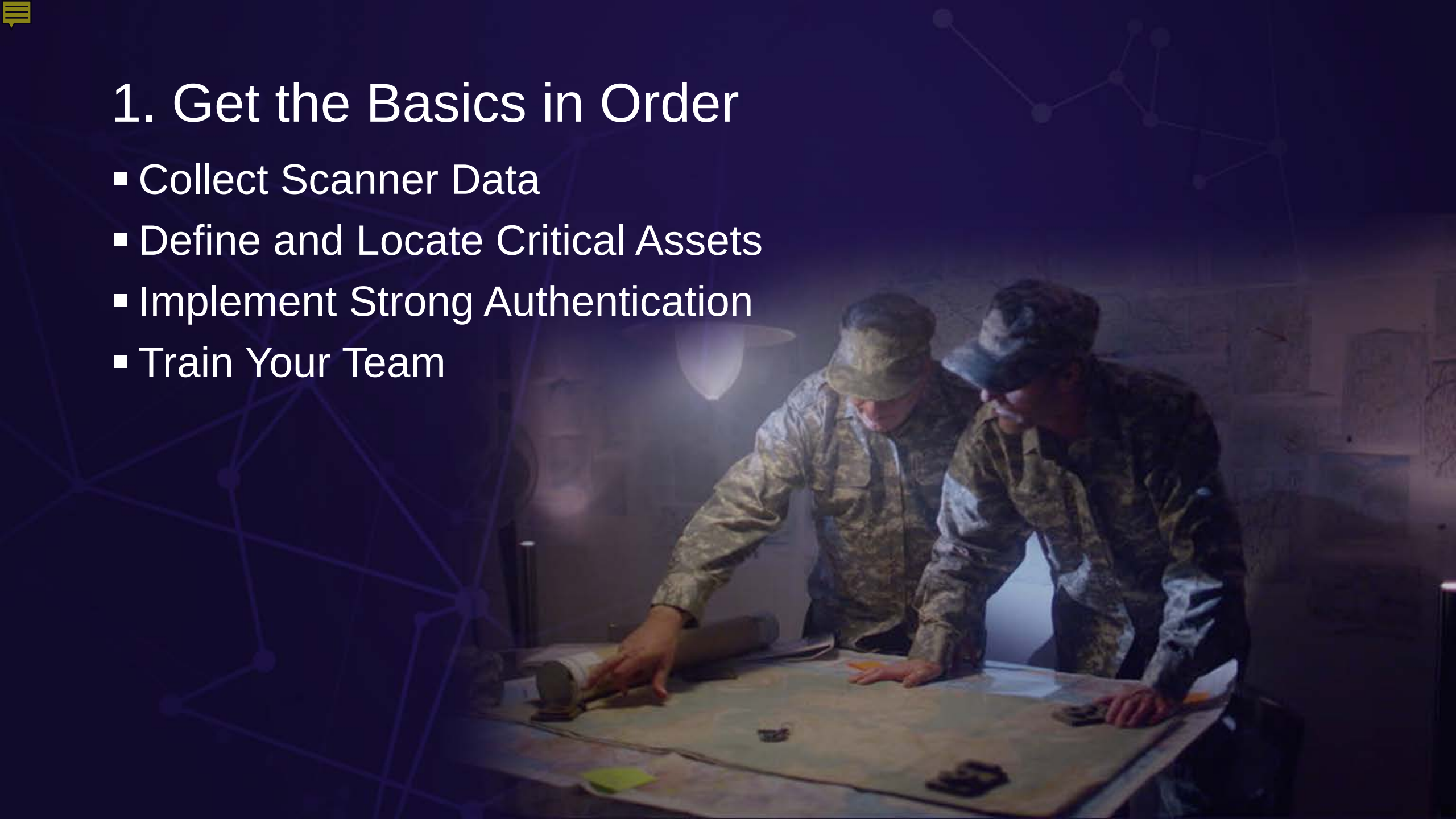
- Too much data leaves organizations paralyzed
- Attackers take advantage of that limitation
- You can’t manage what you can’t see

CORE SECURITY

Create a Comprehensive Attack Strategy

1. Get the Basics in Order

- Collect Scanner Data
- Define and Locate Critical Assets
- Implement Strong Authentication
- Train Your Team



2. Assess, Analyze, Remediate

- Assess Critical Assets
- Analyze Risk
  - Prioritize for vulnerability and access risks
- Remediate

3. Vulnerability + Access Risk Management

- Continuous and Comprehensive Monitoring
- Align your threat vectors with business goals
- Make sure all threat vectors are scanned and prioritized
- Automated solutions
  - Pen-testing
  - Role based provisioning
  - Micro-certifications

Takeaways

Technical Takeaway

- Increase Efficiencies
- Reduce IT Costs

Business Takeaway

- Reduce Threat Surface
- Reduce IT Costs
- Increase Efficiencies
- Improve Compliance

Questions?

Katherine James, SVP Global Sales
kjames@coresecurity.com