ControlScan

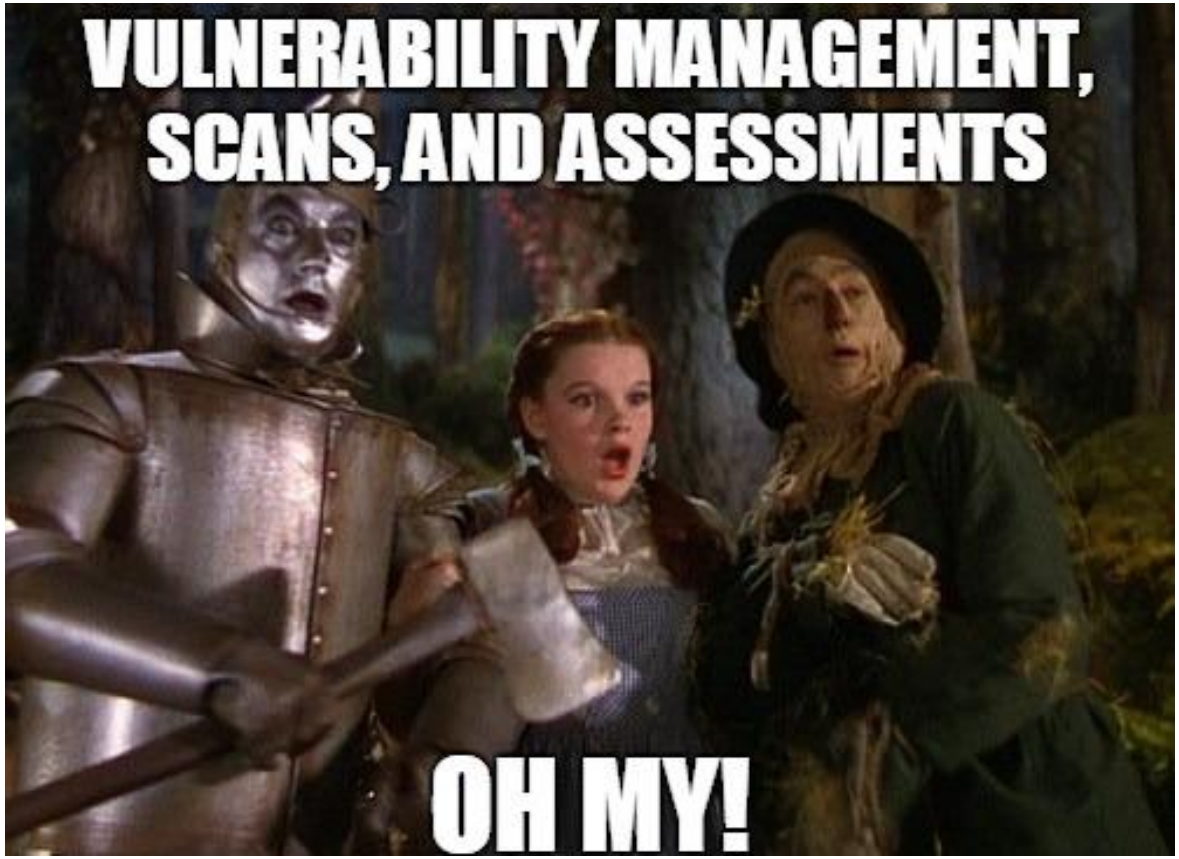
Vulnerability Management

2/2/2018 – ISACA West FL Chapter

Marc Punzirudu, Director Security Consulting Services
mpunzirudu@controlscan.com 352-584-6691

Agenda

- What is a vulnerability assessment?
- What is vulnerability management?
- What are the big differences?
- Why is vulnerability management important?
- Where does it all fall apart?

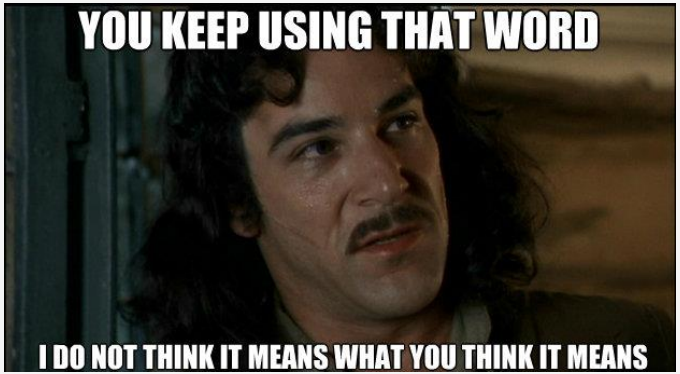


Vulnerability Assessment: What it is

- A point in time analysis
- Not easily measurable over time
- Not associated to a corporate risk plan
- Typically an automated process performed by a tool with minimal interaction.

Vulnerability Assessment: What it is not

- A way to measure vulnerabilities over time
- How vulnerabilities are managed
- Something that provides assurances that an organization is security-aware



Vulnerability Management: What it is

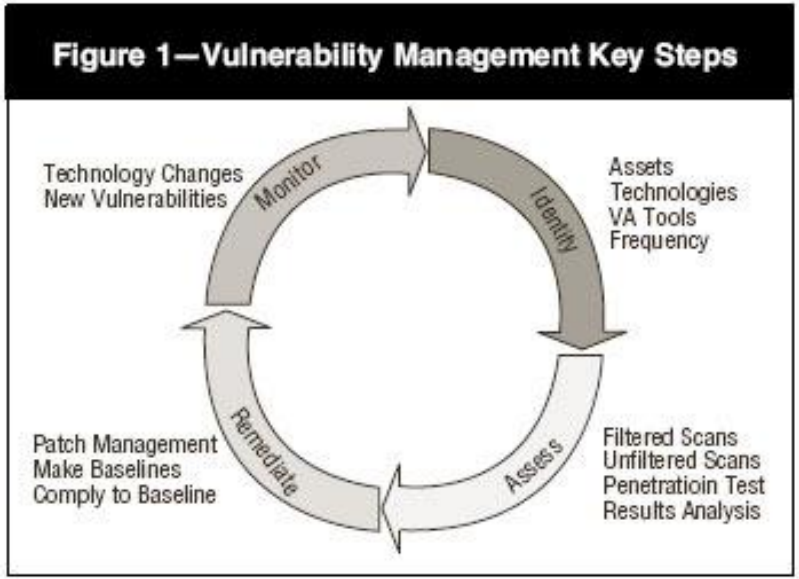
- An auditable process that is part of the organizations culture and is also business as usual.
- Vulnerability Management is the ability to assess, monitor, and secure an environment in accordance with an organizations risk plan.
- The goal of a proper vulnerability management program is to ensure that over time, the organization stays within the defined risk tolerance, and improves its security posture, taking into consideration evolving or recent threats.

Vulnerability Management: What it is Not

- Running scans
- Owned by a single individual
- Something performed as time permits
- A method of “being compliant” or a by-product of external compliance
- Assurance that you are secure and/or have mitigated organizational risk

Vulnerability Management: Why?

- The threat landscape is ever changing, and organizations must be agile in order to stay ahead of the curve.
- Vulnerability Management, when done properly, will provide a continuous overview of vulnerabilities, as well as the risk associated with them.
- A properly designed and functioning program, provides a bridge between stakeholders who define the risk appetite, and technical SME's who perform the tasks required to meet those goals.



Overview of a Vulnerability Management Program

- Identify assets
- Assess vulnerabilities
- Rank and remediate
- Monitor changes

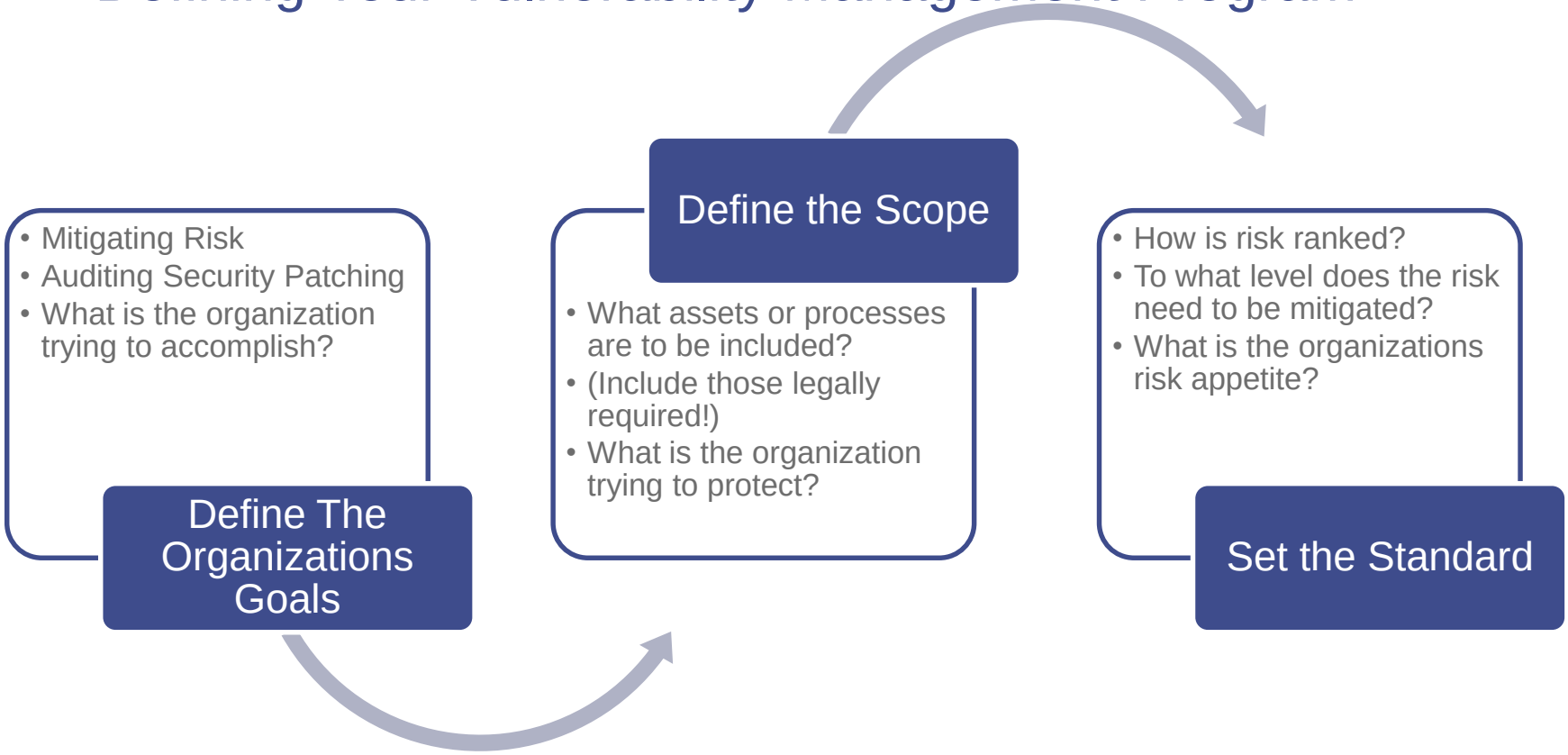
Key Points of a Vulnerability Management Program

- Assigned Responsibilities
- Integrated into all organizational processes
  - Change Management
  - Inventory/Asset Management
  - Configuration Management
- Well defined goals based on the organizations risk plan and appetite
- May incorporate the use of tools such as vulnerability scanners
- Defined process and method to find, risk rank, prioritize, remediate, and document vulnerabilities.

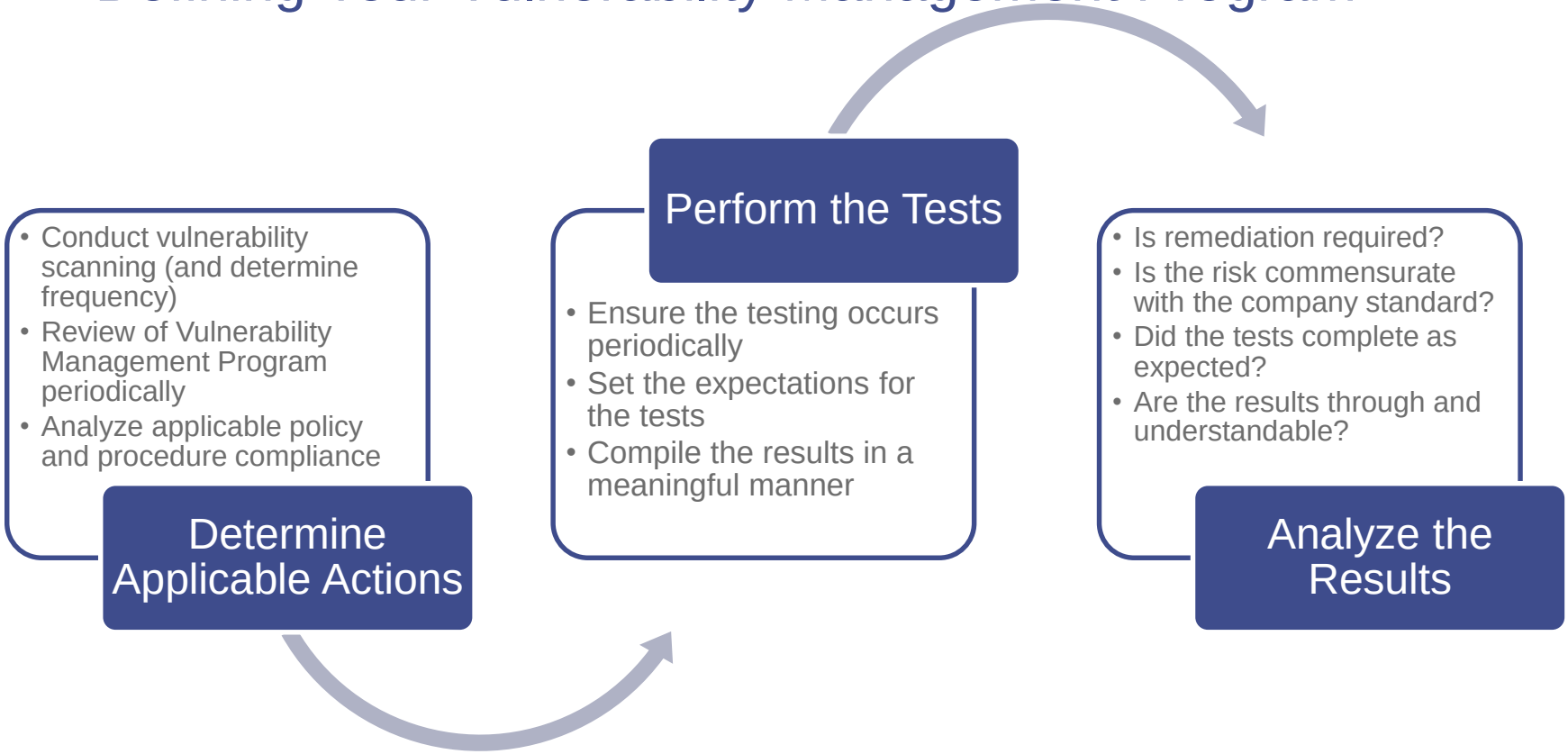
Vulnerability Management Program: Key Points

- As with all formal programs:
  - It is Repeatable
  - It is Measurable
  - It has Defined Metrics of Success
    - or Failure

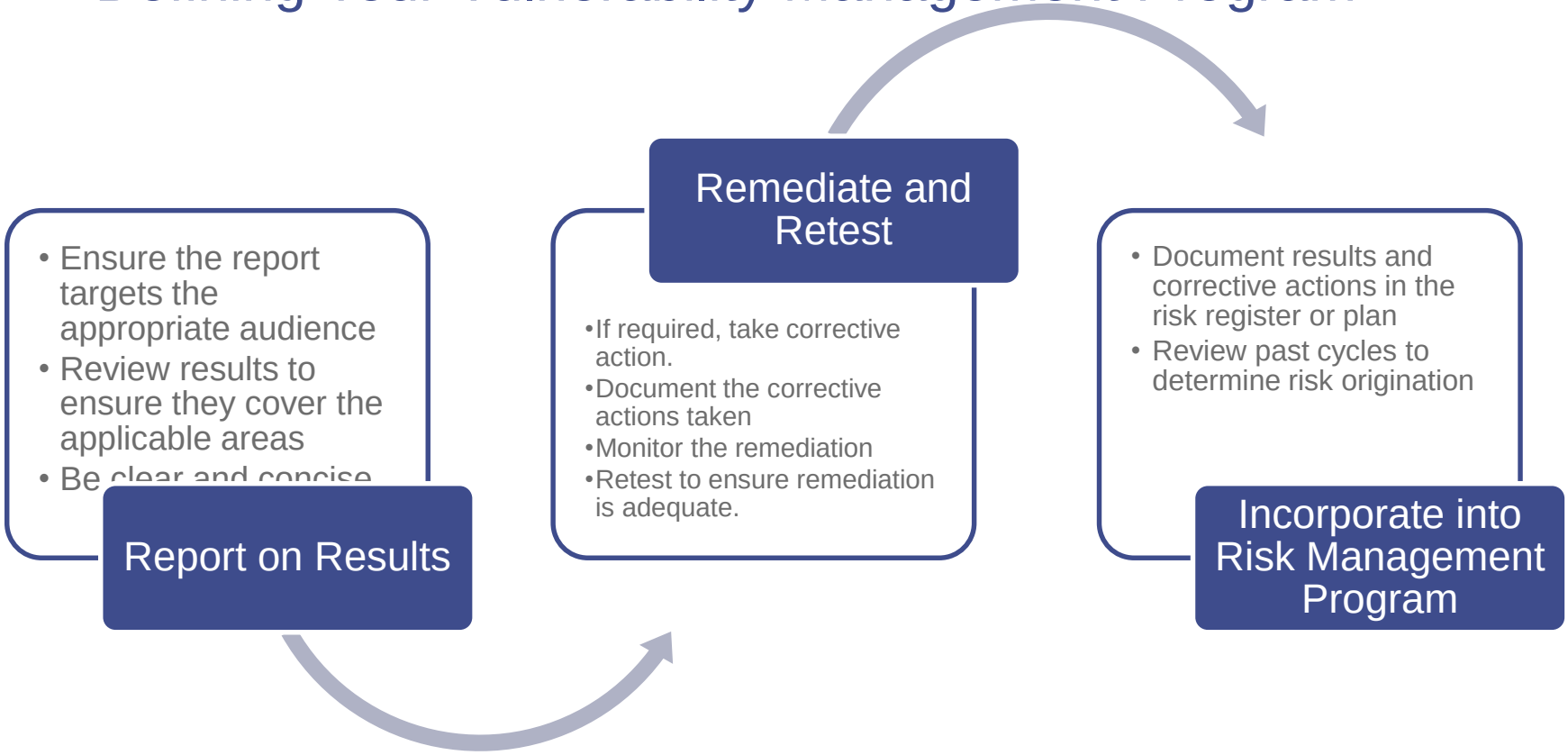
Defining Your Vulnerability Management Program



Defining Your Vulnerability Management Program



Defining Your Vulnerability Management Program



Big Questions: Vulnerability Management Programs

- What can you do with the resources that you have?
  - Is it enough?
  - Is the organizations expectations larger than its budget?
- How often should vulnerability analysis be performed?
- Is there executive buy-in?
- Do you have a process to rank risk as an organization? How long can your organization be vulnerable and to what extent?
- Do you have a method to adjust the vulnerability management program based on the current security landscape and evolving threats?

Major Issues: Reporting the Findings

Bad Data	Application of the Data
False Positives Improperly configured tools Scope is not correct	No process to incorporate the data into anything meaningful Audience doesn't have any context or understanding of the results

Major Issues: Reporting the Findings

Irrelevant or Inconsistent Data

- Incorrect Scope
- Vulnerability Analysis not conducted frequent enough
- Vulnerability Analysis not being done consistently

Major Issues: Patching

- Patches aren’t deployed
  - Break-fix deployment
  - New assets
  - Out of support
  - Downtime/Availability
  - Broken Processes
    - The patch person left
    - No assigned responsibility or ownership

Major Issues: Patching

- Who owns what systems or assets?
- Who is accountable for patching them?
- There could be asset, OS, and application owners all on the same system. Documenting this responsibility is key.
- Are there too many vulnerabilities to manage due to lack of patching?

Too Much Data!

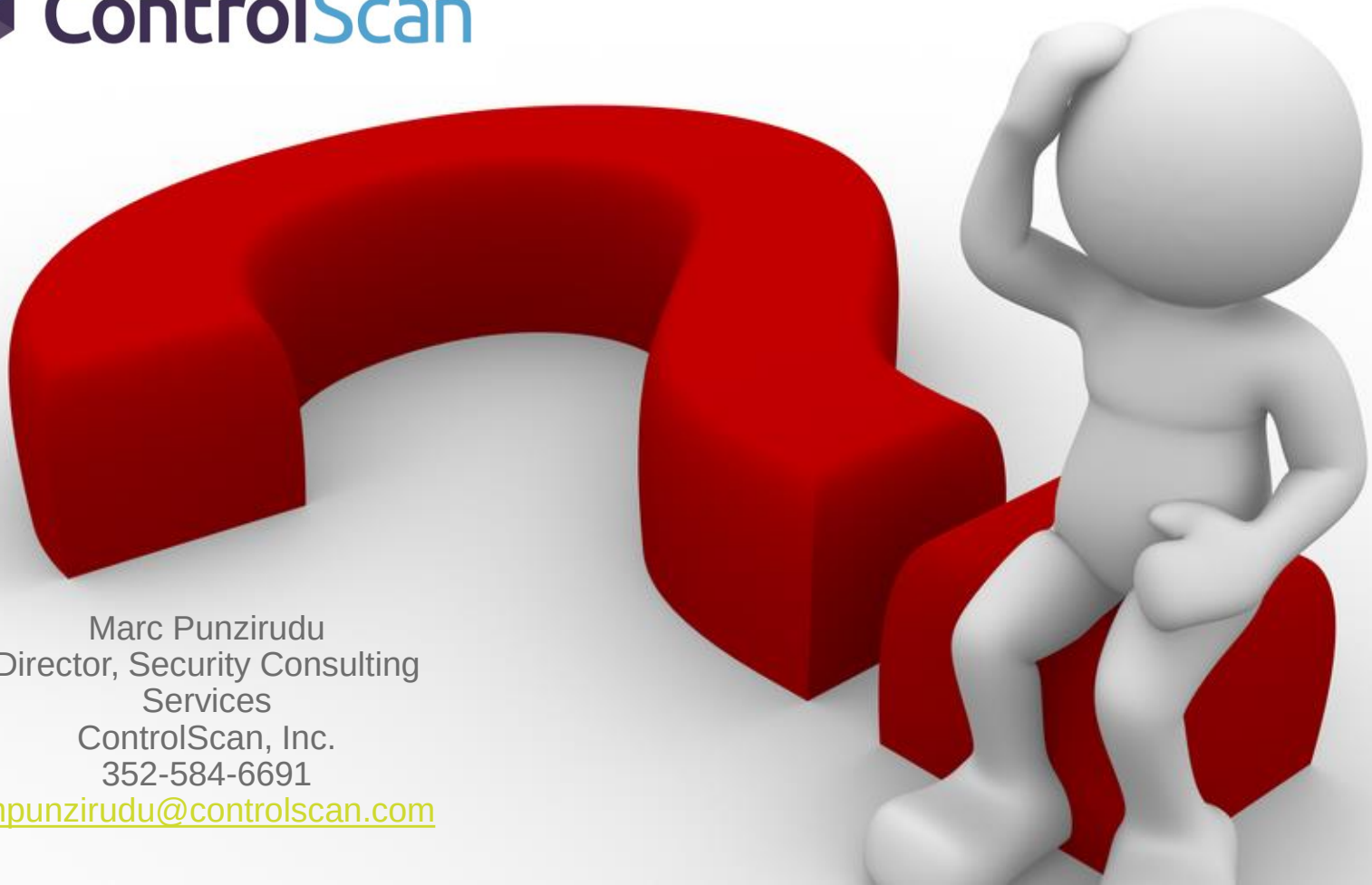
Major Issues: Secure Configuration

- Reasons things aren't hardened
  - New systems/assets
  - No standard for hardening, or documented process
  - Changes to the industry or security requirements
  - No one monitoring and/or directly responsible
  - Irregular configuration audits

Major Issues: Secure Configuration

- Who owns what systems or assets?
- Who is accountable for configuring them?
  - OS? Hardware? Application? Database?
- Are there too many vulnerabilities to manage effectively due to lack of secure configuration standards?
- Is there configuration creep or are their misconfigurations?

ControlScan



Marc Punzirudu
Director, Security Consulting Services
ControlScan, Inc.
352-584-6691
mpunzirudu@controlscan.com