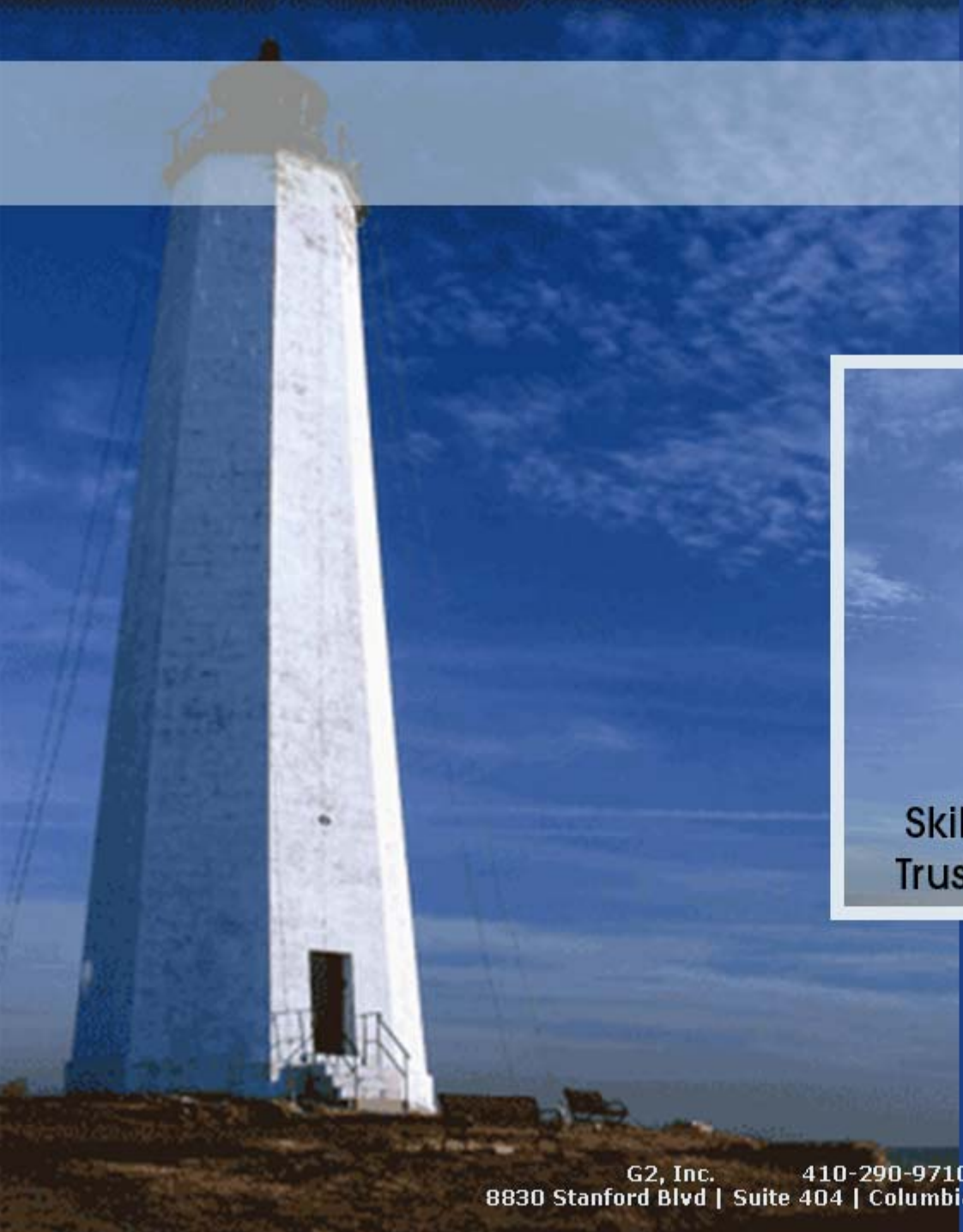


G2

Client Focused
Skilled Communicators
Trusted Security Advisors

G2, Inc. 410-290-9710
8830 Stanford Blvd | Suite 404 | Columbia, MD 21045

- Paul Green
  - President and Founder of G2, Inc
  - We are trusted security advisors to the Federal Government and Fortune 500.
  - We are not a product reseller.
  - We are recognized as having subject matter expertise in the implementation security compliance monitoring software.

Our Clients

U.S. Department of Health and Human Services
Food and Drug Administration

One of My Greatest Accomplishments

Zoe Marie

8lbs, 11oz.

9 days old.

Still True in 2006

“Through 2005, 90 percent of cyber attacks will continue to exploit known security flaws for which a patch is available or a preventive measure known.”

Gartner Group, May 6, 2002

Let’s Address Two Questions.

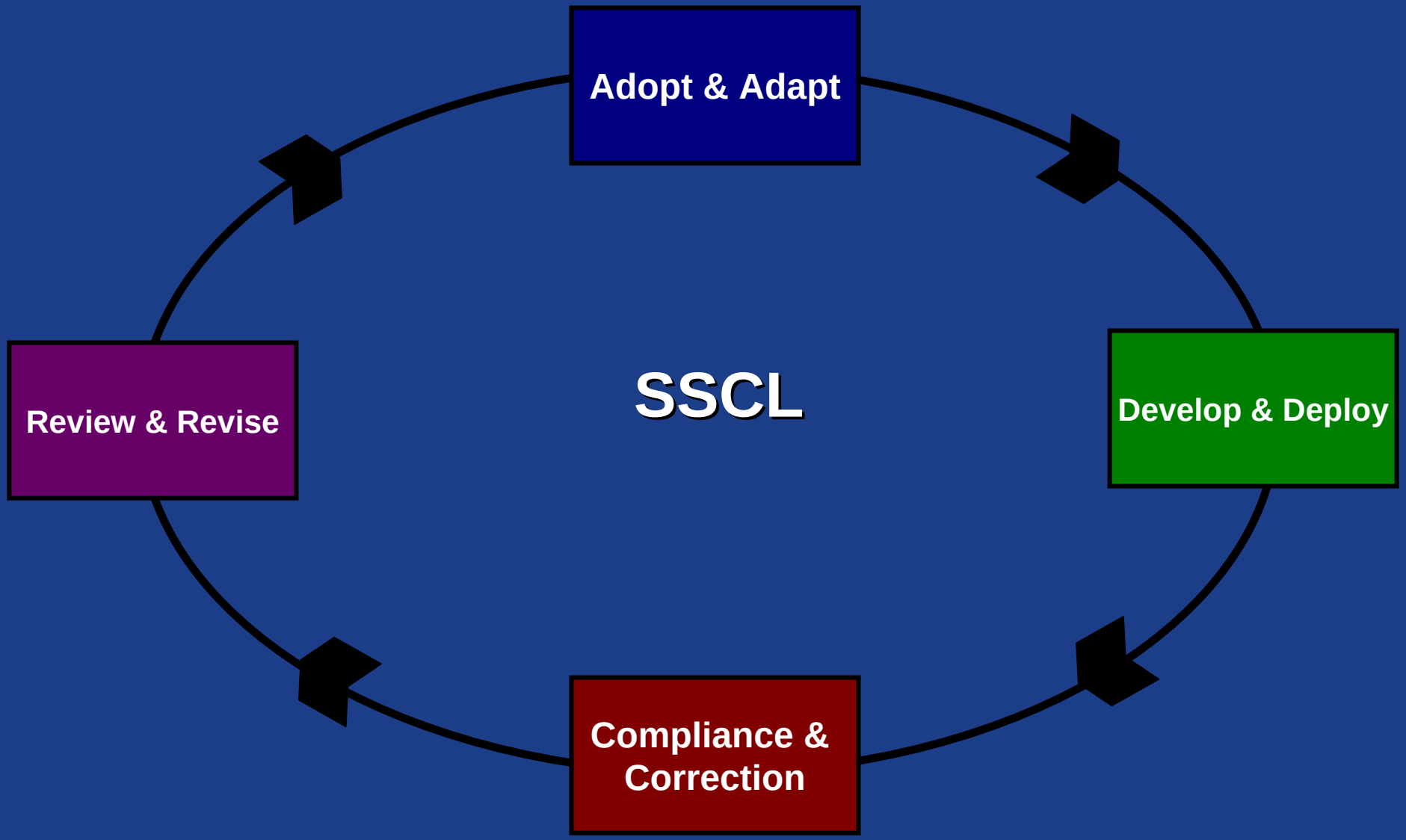
1. How can security automation improve the system security configuration lifecycle?

2. How could this change the services that we now offer?

What Are My SSCL Goals?

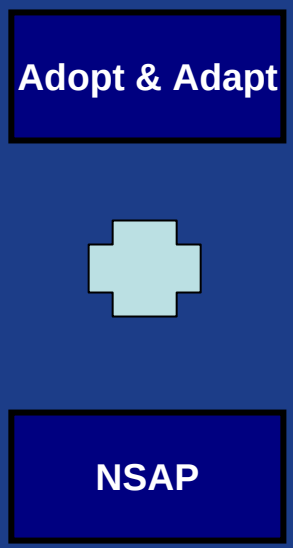
- To facilitate easy-to-manage, consistent server compliance monitoring
- Evolve server security strategy from ***reactive*** to ***proactive***
- Reduce attack surface and minimize operational risk
- Near-real-time, verifiable server compliance documentation
- These products will automate and change the way we validate and test our high-level requirements

The System Security Configuration Lifecycle



- Review existing industry and government configuration checklists and standards (CIS, NIST, NSA, Vendors, etc.)
  - Checklists are often prose documents or spreadsheets and are not machine readable
    - Difficult to manage these files,
    - AND, nearly impossible to compare “side-to-side”

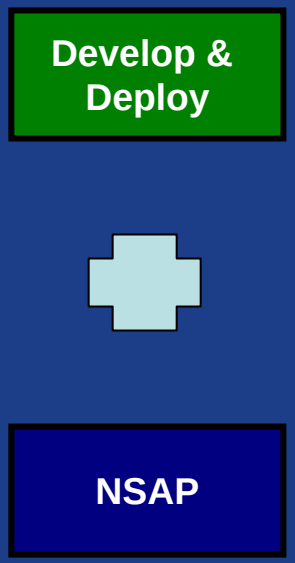
- Customize standard/checklist based on compatibility and risk assessment
  - These are often conglomerations of various checklists creating N number of “custom” baselines
    - When we account for operational issues we end up with NN variations.
    - In the end, how does your “custom” implementation compare to the original standards?



- Educate our clients that a machine readable format for checklists allows us to spend less time on document management and more time focused on other activities in the lifecycle.
- We now have a framework that provides traceability between our customized checklists and high level requirements. (e.g. 800.53, 8500)

Develop & Deploy

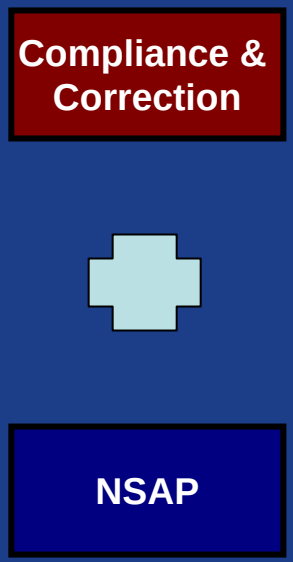
- Customize standard/checklist based on compatibility and risk assessment
- Develop configuration scripts (address all standard OS’s and builds) based on standards/checklists from A&A
- Incorporate standards/checklists into automated auditing toolset



- We can now convert the current organization's custom checklists into standardized XML format. (XCCDF/OVAL)
- A larger number of man hours can now be saved by using tools that accept the machine readable XCCDF format by directly importing the policies into the security tools
- We want to create build scripts that interpret standardized XML inputs and configure build scripts
- Learn how to express "customer specific checks" that are may not be included in CCE

Compliance & Correction

- Analyze output from each of the scanning tools, in certain cases this includes manual cross referencing of findings
- Report and communicate results
  - In many cases this process is still paper-based, are the results produce 1000's of pages of information.
- Remediate (initial cycles will produce large amounts of remediation)



- We can develop scripts to compare the standardized XML output from each of the scanning tools.
- A machine readable format can support a seamless integration with XCCDF compatible tools.
- Using CCE, we now also have a common reference that allows us to map the configuration results between different security tools.
- Now we begin the decision process of determining and implementing the appropriate remediation path.
- This can include the analysis of compensating controls.

Our Wish List

Review & Revise

- We'd love to know if a CVE applies based on a the value of a CCE. (CVE pertains to only SSH, we want to report how many systems currently run SSH in a moment.)
- Facilitate temporary changes in systems configuration levels with respect to attack based scenarios and then return to the normal operation baseline once a patch has been identified.
- Love to see the connection between other high level requirements such as COBIT control objectives and XCCDF/OVAL.