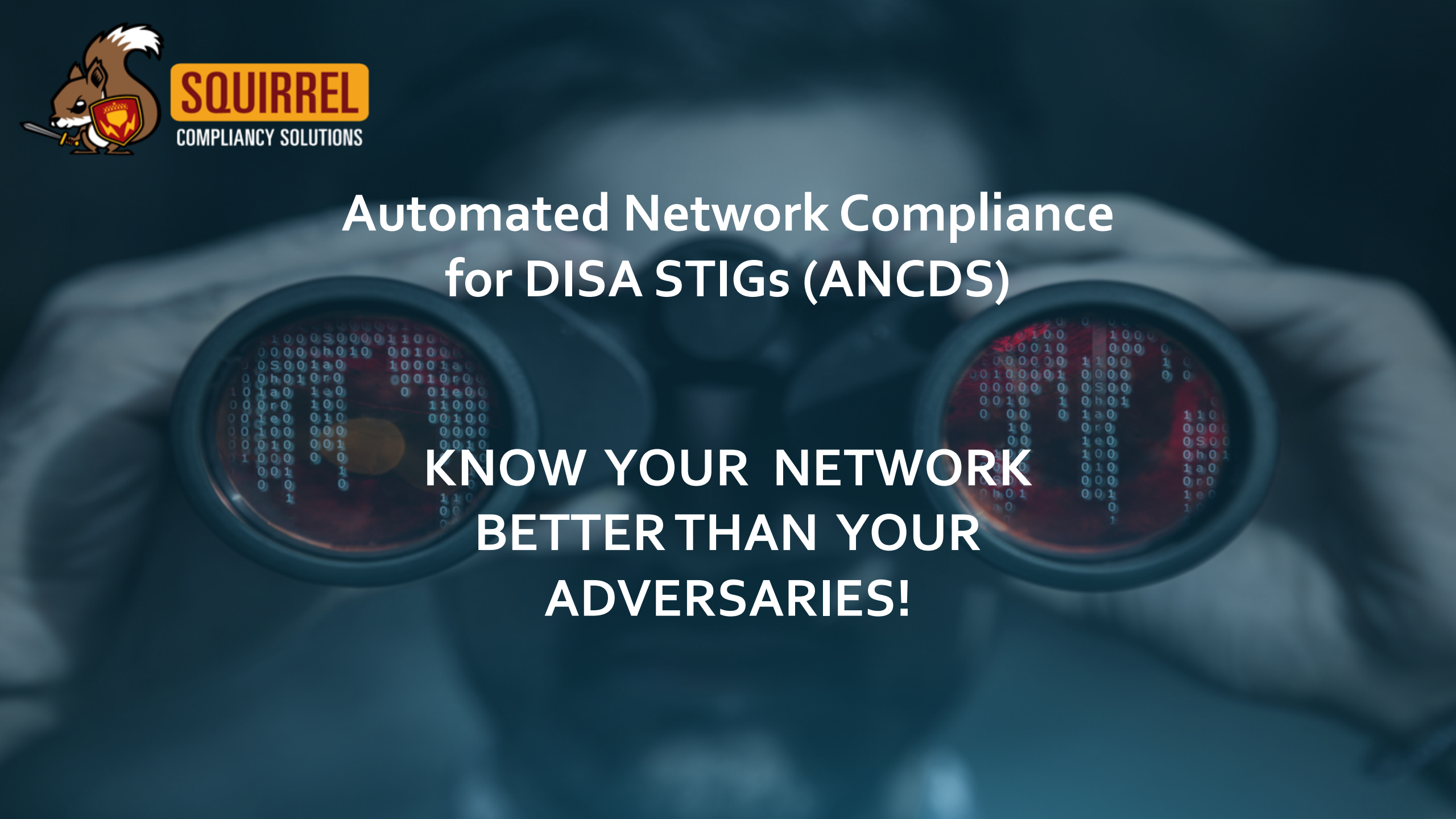

SQUIRREL
COMPLIANCY SOLUTIONS
Automated Network Compliance
for DISA STIGs (ANCDS)
KNOW YOUR NETWORK
BETTER THAN YOUR
ADVERSARIES!

Background

- Defense Information Systems Agency (DISA) releases Security Technical Implementation Guides (STIGs) to increase the security posture of Department of Defense (DoD) environments
- Cyber Security Readiness Inspections (CCRI) are performed to determine compliance with the DISA STIGs and without notice / surprise inspections
- Communication Security (COMSEC) is critical to mission success and the protection of our secrets

Challenges of Operating a Secure Environment

How is compliance assessed today?

- Time consuming process, performed once a year
- Each device is reviewed individually
- Manually, which leads to errors and oversights
- Requires deep technical knowledge in many technologies
- No severity priority assigned for remediation with manual compliance

Compliance competes with mission needs of an already overtasked staff—therefore, compliance never gets done…

Value Proposition – Typical Scenario for ANCDS

Level of Effort quickly becomes overwhelming due to the required personnel hours.

Number of Devices	Hours **per** Manual Audit	Cost **per** Manual Automated Audit*
200	800	$104,000
1,500	6,000	$780,000
3,000	12,000	$1,560,000
5,000	20,000	$2,600,000
10,000	40,000	$5,200,000

*Effort estimate based on 4 hours per device per audit at $130 per hour

The Squirrel Solution

Improve your security posture quickly and efficiently

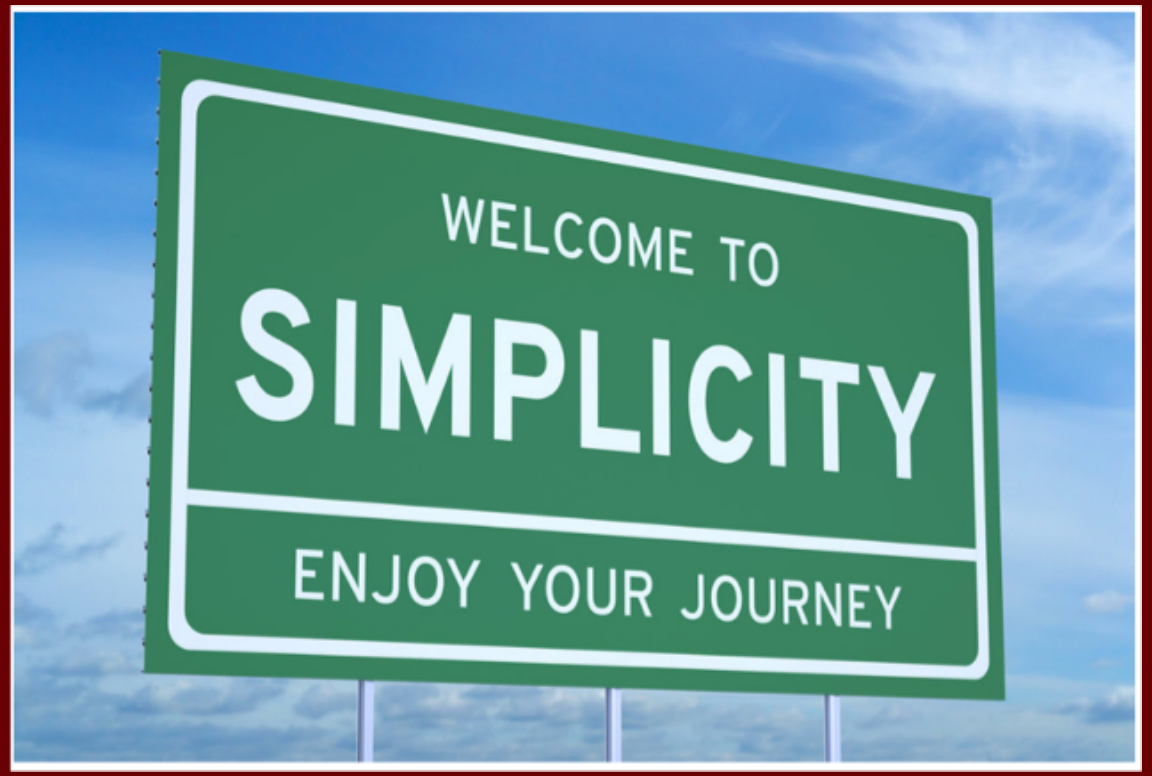
Capitalize On Your Existing Investment

We provide the automation policies to **leverage** your existing Network Configuration Change Manager (NCCM) software investment.

Our solution is designed to be deployed quickly.

Simplify Your Audit Process

Our service allows you to audit your environment **daily** (or more frequently, if desired) to improve the situational awareness of your security posture.



Improve Staff Efficiency

By automating time-consuming audits, we allow your staff to **focus** better on the mission and operating the network infrastructure.

How do we do it?

- Automate the auditing of network devices using policies based on the latest DISA STIGs for network infrastructure devices
- NCCM software agnostic*
- Automate remediation** of **user selected** DISA STIG violations to further decrease Level of Effort***
- Update policies as the DISA STIGs are revised (2-3 times a year)
- Continual updates of additional DISA STIG policies released during the subscription
- Audit your environment 365 days a year with minimal effort

* Capabilities vary between NCCM software
** Only vulnerabilities not impacting network availability
** Time saved varies based on network size

How does this benefit your organization?

- Know your security posture every morning / at will
- Allows you to determine your operational risks using the DISA STIG vulnerability ranking classification system
- Quickly move our solution across network classifications as needed ensures communication security for any environment
- Automates a repetitive, tedious, and labor-intensive process saving you and your technicians thousands of hours
- Maintain capability between staff rotations!

Know your security posture and address risks before they become issues

The Squirrel Compliancy Solution Service

- Annual subscription
- Regular updated policies
- Policy Maintenance
- Support for multiple Network Configuration Change Manager (NCCM) software vendors
- Tiered pricing to meet your organization's needs
- Remote Support Offering

Overview

Cyber Defense Enforcement

- Continuous monitoring of your compliance status
- Know your security posture awareness at any moment
- Know your network better than your adversaries

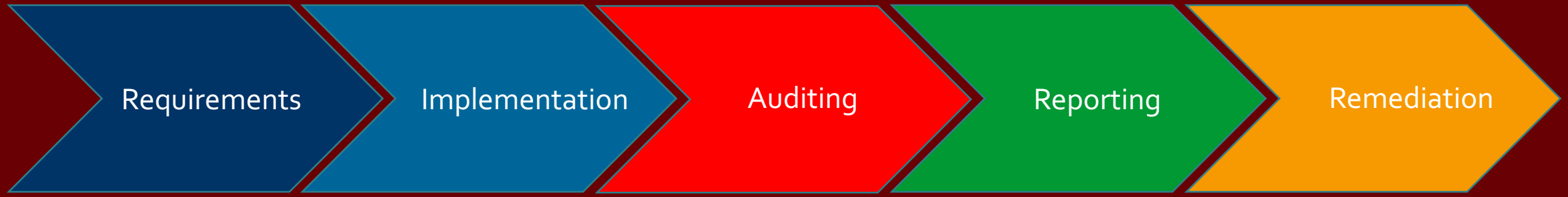
Operational Benefits

- Reduced Level of Effort to maintain your environment saving thousands of man hours per audit
- Staff is able to focus on mission needs and the deployment of new capabilities

Thank You!

Backup Slides

ANCDS Process Flow



- **Number and type of devices**
- **Security considerations**
- **NCCM platform***

- **Provide policies w/ installation guides**
- **Finalize requirements**
- **Customize rule-set (as needed)**

- **Audit devices using Squirrel DISA STIG policies**

- **Review Audit Findings**

- **Automate user-selected vulnerabilities****
- **Manually correct remaining vulnerabilities**

* Not all NCCM software packages support corrective actions
** Only vulnerabilities not impacting network availability