Security Automation

The Good, the Bad, and the Ugly

Presenter: Richard Gowen (a.k.a. @alt_bier)

I work as a Solution Architect for PepsiCo in the Global Cloud Foundation group specializing in network and security automation.

In my spare time I'm a hacker, maker, gamer, brewmaster, programmer and more... all the things.

One thing I'm known for is the indie electronic conference badges I create for the **#badgelife** movement which celebrates wearable electronic artwork.

Security Automation

“If You Work For a Living, Why Do You Kill Yourself Working?”
– Tuco, the Ugly

Automation can close skill and resource gaps, reduce human error, and perform tasks faster and more securely by applying and enforcing security standards.

Security Automation is its application on security tasks.

Security Automation Challenge

The challenge with automating security tasks is they tend to have more process and governance wrapped around them than other IT tasks.

For example, automating firewall rule creation for new services eliminates human error, provides rule consistency, and allows for triggering jobs on new service creation.

This provides many benefits including fast customer access to the new service.

However, there may be existing processes for new rule validations or approvals and other requirements that need to be met for governance.

Security Automation

The Good

Choosing GOOD automation use cases that will provide the biggest BANG!

The Bad

Processes can be BAD for automation KILLING its use case benefits.

Research, Integration and Process Modification can avoid these issues.

The Ugly

The UGLY truth about maintaining governance requirements.

Change control, job detail artifacts and other governance controls

The Good

“Every gun makes its own tune.” – Blondie, the Good

GOOD security automation candidates are security tasks that have a large human resource cost (i.e., staff time) or long delivery time, and have process / governance requirements that can be met with minimal effort.

This will allow for automation to provide the largest impact with the least amount of work.

Good Security Automation Use Cases

What will give us the biggest BANG for the buck?

The choice of a good security automation use case will differ from org to org so you must choose based on the specifics of your company:

- What tasks are staff taking the most time on?
- Where would automation provide a large impact?
- What are the processes wrapped around these tasks and can they be overcome or automated?
- What does governance require for these tasks, and can it be met by automation?

Security Automation Candidates

Identify Candidates For Use Cases

When building a security automation use case the primary benefits will usually be **resource cost (i.e., staff time) and delivery time reduction**.

Integration with other IT services to **provide a large impact** to the business is also an important benefit to consider.

So, research should be your first step to identify candidates.

Security Automation Candidates

Identify Candidates For Use Cases

Research to identify Good candidates:

- Which security tasks have the highest resource cost (i.e., what takes the most staff time)
- Which tasks take the longest to complete from request submission to delivery?
- Which tasks could be integrated into other IT automation workflows to provide a larger business impact?

The top 10 % are good candidates to become use cases.

Security Automation Use Cases

Flushing Out Candidates To Create Use Cases

Processes

Document how the candidate task is performed without automation

- Request Submission and Inputs
- Request Approvals
- Gathered Facts
- Implementation Steps

How will automation fit with these processes or will processes need to change to fit the automation?

Governance

Review the candidate task controls and artifact governance requirements.

- Change Control
- Artifacts
- Other Controls

How will automation meet these governance requirements?

Use Case: Security Rule Automation

Example: Implementing Security Rules using Templates

Problem: An existing IT automation workflow stands up a new external web service in minutes, but the firewall inbound rule takes a week to implement.

Use Case: Automate the implementation of an inbound security rule using a pre-approved template (that has a destination variable to be populated with the new external web service) which is triggered by the existing IT automation workflow.

Benefits: Resource cost reduction, Delivery time reduction, integration with existing IT automation job for large business impact.

Process: Pre-approval of the rule template

Governance: Rule details written to an audit log and appended to the Change Control record opened by the existing workflow

Presentation by Richard Gowen a.k.a. @alt_bier

Use Case: RBAC Automation

Example: Adding Role Based Access Control to AD Group

Problem: Users can't access newly created resources until an RBAC role is assigned to their AD group.
The service request takes a week to implement.

Use Case: Automate the addition of an RBAC role to an AD Group.
A service request ticket triggers a workflow which sends approval requests and waits for a response. Approval triggers creation of a change control record followed by implementation and SR update.

Benefits: Resource cost reduction and delivery time reduction.

Process: Service ticket input, approval gathered before implementing

Governance: Change details and approval details written to an audit log and appended to SR & Change Record

The Bad

"You're smart enough to know that talking won't save you."
– Angel Eyes, the Bad

Working automation into existing Processes can be BAD for *certain* use cases, preventing full benefit realization or (in extreme cases) making it worse than the manual process.

A compromise must be reached with existing processes for automation to provide its full benefit.

Identify Processes Bad for Automation

Research is Key for Automation Integration

Research how the security automation use case is performed manually.

How will automation fit with these processes?

Do you see potential problems?

- Can automation access and work with all the systems used (e.g., API, routing, access control, etc.)?
- Are there manual steps that can't be automated?
- Are multiple groups involved in implementation?
- How are approvals gathered and recorded?

Detailed Process Research

Research **Everything** Related to the Use Case

Request Submission and Inputs

- How are requests submitted, what systems are used, and how is status updated?
- Are request data inputs validated and what systems are referenced?

Request Approvals

- How are requests approved and how are those approvals recorded?
- Are multiple levels of approval needed from one or more groups?

Detailed Process Research

Research **Everything** Related to the Use Case

Gathered Facts

- What other data needs to be gathered and what systems are referenced?

Implementation Steps

- How is the change implemented and what systems are used?
- Does the change require task work from more than one group and if so, can these tasks be done concurrently or what order and handoffs are used?
- What pre/post change communication is required and what systems are used?

Automation Process Integration

Integrating the use case into the existing processes

Process Replication

For many process tasks we can have automation replicate what is being done manually.

From calling an API to create/update a service ticket or change record to saving detailed artifacts into file shares or repositories, we can use automation to replicate tasks without changing the existing process.

Process Modification

For some process tasks we need to modify the process to accommodate our automation use case.

Manual tasks such as updating legacy systems that do not have APIs, voice calls to trigger actions, updating artifacts in a shared spreadsheet and more will require process change to allow for automation.

Automation Success Criteria

Getting Everyone On Board With Automation

While research may be the key to allowing for automation integration, people working together are the key to its success.

Everyone needs to be on board to fully realize the automation benefit.

Having **decision makers** and **leaders** on board will help make required process changes less painful and provide a safety net for **developers** allowing them to fail and try again as needed (Agile) to make it work.

Having **employees** on board and properly training them on how to use automation and its new processes will reduce pushback from people worried about being replaced by automation.

Process Modification: Manual Approval

Example: Manual Approval Process Modification

Problem: Existing process has a task to gather approval from a manager via service request task or email.

Process Change: For the automation use case this process must change to eliminate email as a valid approval method and implement an SLA on the service request approval task.

As a transition step the service owner can complete the service request approval task from the emails they receive.

Automation Integration: The service request system has an API that automation can query for the approval and trigger on its completion.

The SLA on the service request approval task is what allows for the delivery time reduction benefit to be fully realized.

Presentation by Richard Gowen a.k.a. @alt_bier

The Ugly

"When you have to shoot, shoot. Don't talk."
– Tuco, the Ugly

The UGLY Truth about maintaining governance requirements is that they are not flexible to modification like other processes.

Governance dictates the controls to be adhered to and artifacts to be captured for various security tasks and the automation infrastructure that drives the use cases.

Automation must adapt to the requirements, not the other way around. However, we can get creative in how do it.

The Ugly Truth About Governance

Requirements aren’t flexible; how you get there is

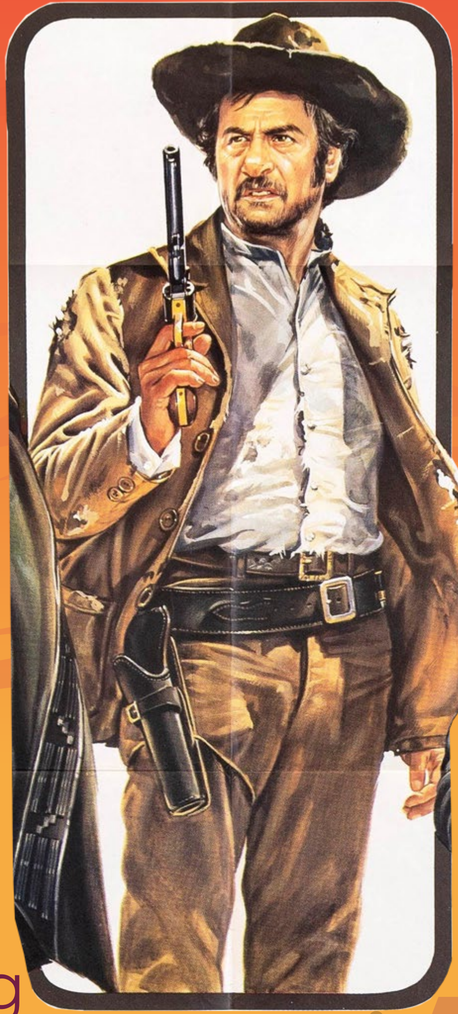
Governance requirements aren’t flexible, they accept only compliance. How we comply is where we get creative.

Unless you run into a sadist, most policies clearly define what is required <u>without</u> requiring exact steps to get there.

`“Change approvals must be recorded in the CR.”`
This does not specify how we get the approvals.
If a system has built-in approval jobs that most use, we can bypass them as long as we meet the requirement.

This ties to the earlier example on templates where attaching a pre-approval to the CR would meet the requirement.

This is what I mean by “get creative”. Your first step on this creative journey will once again begin with research.



Presentation by Richard Gowen a.k.a. @alt_bier

Detailed Governance Research

Research **Everything** Related to the Use Case

Change Control

How are change records submitted, what systems are used, and how is status updated?

Change Approvals

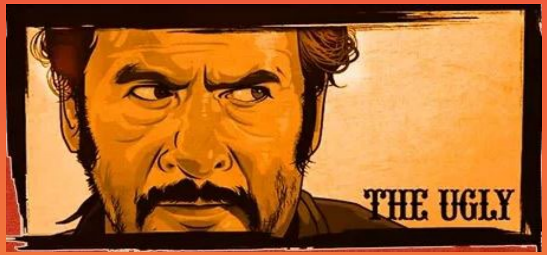
How are change requests approved and how are those approvals recorded?

Change Risk Assessments

How are risk assessments performed / recorded, what systems are used?

Change Backout Procedures

How are backout procedures defined / recorded, what systems are used?



Detailed Governance Research

Research **Everything** Related to the Use Case

Artifact Format and Storage

Artifacts are vital pieces of information that need to be kept for reference in various formats and locations?

Approval Artifacts

Details required for approval artifacts (evidence), how is this formatted and recorded, what systems are used?

Change Detail Artifacts

Details required for change artifacts, how is this formatted and recorded, what systems are used?

Other Required Artifacts

Other artifacts required: details/format/record on what systems?

Detailed Governance Research

Research **Everything** Related to the Use Case

Other Controls

What other controls are required for either the use case or the automation infrastructure?

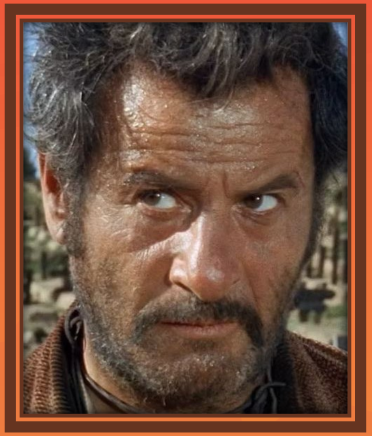
Controls related to Secrets
Controls for secrets: storage, access, use, etc.?

Controls related to Code
Controls for code: storage, branch protection, progression, etc.?

Controls related to Testing
Controls for testing: required tests, systems used, etc.?

Controls related to Scanning
Controls for scanning: vulnerability, virus, systems used, etc., ?

Automation and Change Control



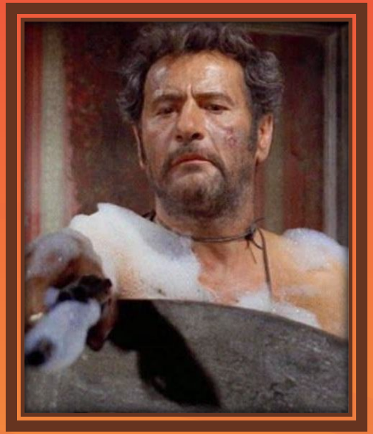
Compliance with Change Control Requirements

Most companies have change control governance policies.

Processes like change coordinator meetings and tools like IT Service Management (ITSM) systems are built around those policies to ensure compliance.

There are several ways that automation can comply with these policies

- ✓ Process Avoidance: Remove change control from your workflow having automation be run as a task in a change window other processes implemented
  - ✓ Possible impact to delivery time reduction if change control process is slow
- ✓ Process Replication: Use the ITSM API to perform all aspects of change control
  - ✓ Possible impact to delivery time reduction if change approvals are slow
- ✓ Process Modification: Deal with approvals or other tasks via some *new creative* process and feed the results into ITSM API (or whatever change tool is used)



Automation Artifacts

Vital Reference Information Format and Storage

Artifacts are vital pieces of information that need to be kept for reference in various formats and stored in various systems/locations

There are many different artifacts each with unique formats that will need to be stored in several different systems as governance controls dictate.

A few examples would include approvals, test/implementation/backout plans and results, risk assessments, service data, change data, inventory data, IP data, etc.

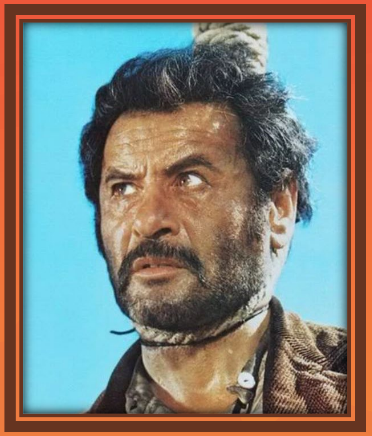
Your research should have identified what artifacts are required for your use case.

For each of these you will need to assess how to gather the artifact data, format it, and store it where it is required.

In some cases, this may require process modification to accomplish.

Get those Network teams to stop using spreadsheets!

Other Controls for Automation



… and in the darkness bind them.

Governance is more than just change control and record keeping.

There will be <u>many controls</u> that automation will be required to adhere to.

Some of these controls will be tied to the use cases you are automating.

- For example, new service vulnerability scans and intrusion tests, or CMDB updates, etc.

Some of these controls will be tied to the automation infrastructure itself.

- For example, storage and usage of secrets (e.g., API tokens, credentials), code repository access and branch protection, testing requirements, etc.

Governance policies and controls are too numerous and varied to detail here. <u>However, you must comply with them all.</u>

So, use your research and if necessary, your creativity to meet each of these.

The last thing you want your employment epitaph to read is “Non-Compliant”.

Artifacts for Service Changes

Example: Service Changes Must Be Added to the CMDB

Control: Policy states that any service changes must be added to the configuration management database. Our use case will be making a service change.

Problem: The automation use case will be making a change to a service that is in the CMDB. This CMDB does not have a web front end or an API. It does have SQL middleware that allows for queries and updates which get validated before being accepted.

Compliance: Our automation will need to make an SQL QUERY for the related service record, gather the change data, format this change data as an SQL UPDATE, and post that update to the CMDB middleware. Then it will confirm the validation response.

Controls for Privileged Access

Example: Privileged Access Secrets must be Rotated Daily

Control: Policy states that secrets for privileged accounts must be changed daily and automation needs to use a privileged account for its use case.

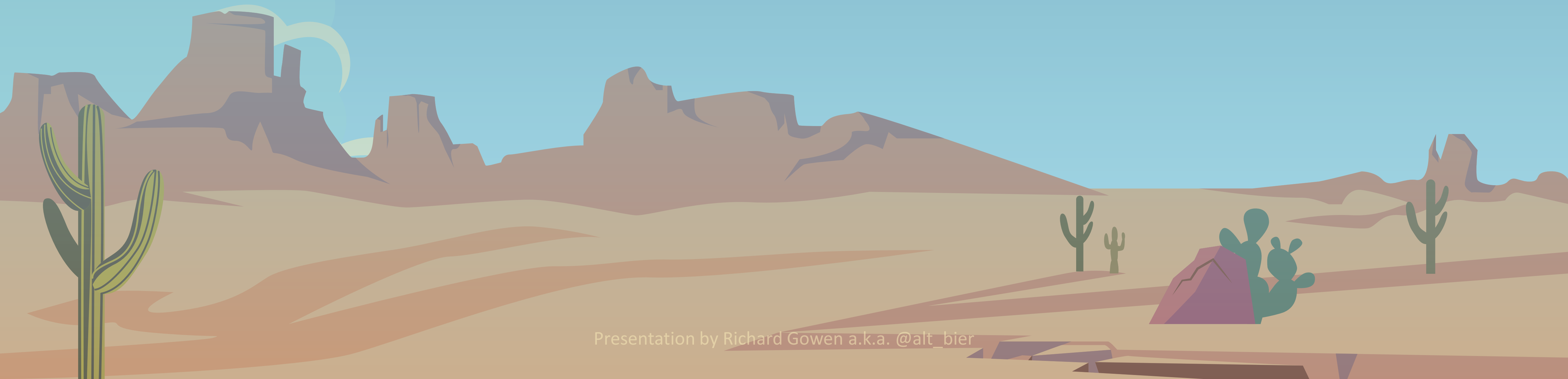
Problem: The automation use case which needs a privileged account will not be able to store its secret locally or in code as the secret would be changing too often for this to be feasible.

Compliance: Use of a privileged account management tool such as CyberArk or SecureAuth (or a dozen others) would allow for the automation infrastructure to make an API query to this tool to gather the current value of the secret on-demand. As the tool rotates the secret to new values the automation will always have the latest value when it runs.

Summary

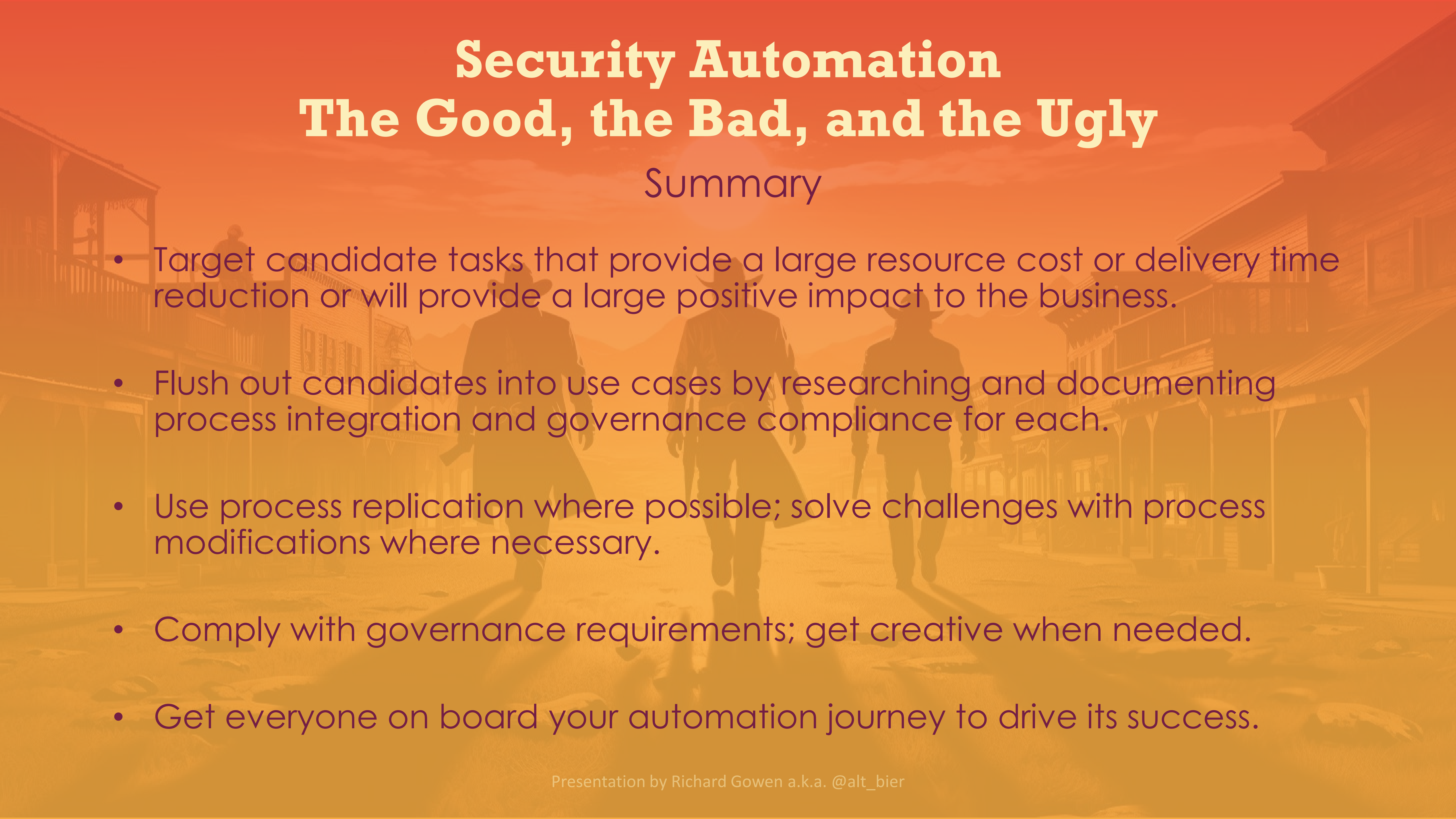
"In this world there's two kinds of people, my friend:
Those with loaded guns and those who dig."
– Blondie, the Good

This presentation has given you the ammunition needed to load your Security Automation guns so you can stop digging for all your security tasks.



Security Automation
The Good, the Bad, and the Ugly

Summary



- Target candidate tasks that provide a large resource cost or delivery time reduction or will provide a large positive impact to the business.
- Flush out candidates into use cases by researching and documenting process integration and governance compliance for each.
- Use process replication where possible; solve challenges with process modifications where necessary.
- Comply with governance requirements; get creative when needed.
- Get everyone on board your automation journey to drive its success.

Thank You

Are there Questions?

Presenter:	Richard Gowen
Twitter/X:	@alt_bier
Mastodon:	defcon.social/@alt_bier
Projects:	altbier.us
Github:	github.com/gowenrw

Presentation Available Here:

https://bsidesdfw2023.altbier.us/

Template based on “Spaghetti Western Style” from poweredtemplate.com