Foundations of Automation

Clay Haynes

Who Am I?

- Senior Network Security Engineer at Twitter
- Juniper Ambassador
- Dual JNCIE in Enterprise Route/Switch and Security

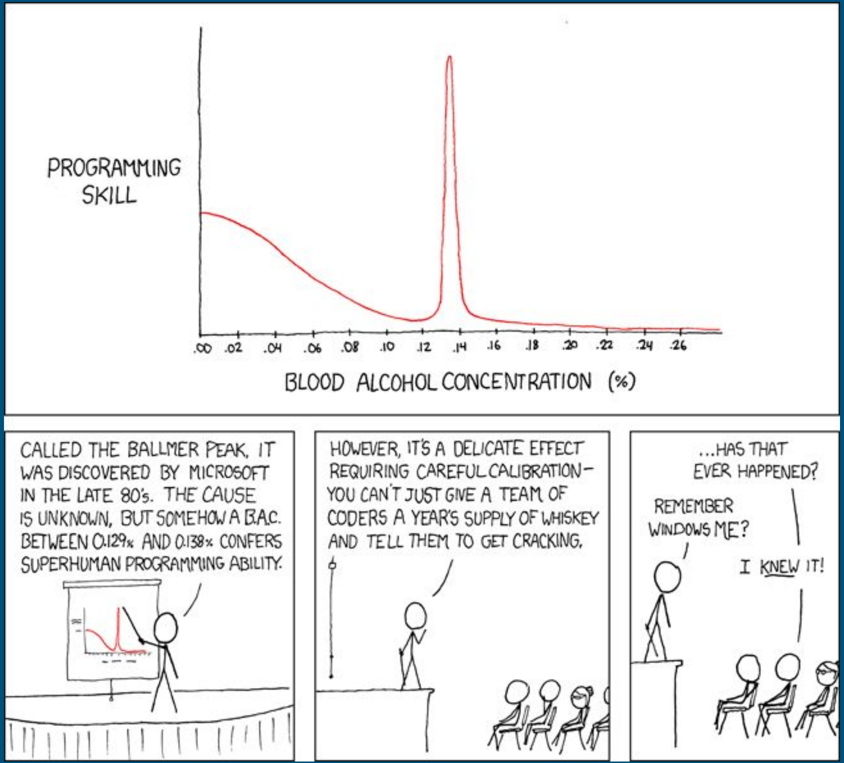
Topics

- Why automation projects fail
- What we can do about them

Why Automation Projects Fail

- The needs of the Organization are poorly defined
- Lack of information of the infrastructure
- Lack of standards and templates
- Scope creep

Why Automation Projects Fail


PROGRAMMING SKILL
.00 .02 .04 .06 .08 .10 .12 .14 .16 .18 .20 .22 .24 .26
BLOOD ALCOHOL CONCENTRATION (%)
CALLED THE BALLMER PEAK, IT WAS DISCOVERED BY MICROSOFT IN THE LATE 80's. THE CAUSE IS UNKNOWN, BUT SOMEHOW A B.A.C. BETWEEN 0.129% AND 0.138% CONFERS SUPERHUMAN PROGRAMMING ABILITY.
HOWEVER, IT'S A DELICATE EFFECT REQUIRING CAREFUL CALIBRATION – YOU CAN'T JUST GIVE A TEAM OF CODERS A YEAR'S SUPPLY OF WHISKEY AND TELL THEM TO GET CRACKING.
...HAS THAT EVER HAPPENED?
REMEMBER WINDOWS ME?
I KNEW IT!

Source: XKCD

Organization Needs

- Different groups are asking the different questions:
  - CISO - How do I show value to the org while maintaining best security practices?
  - Manager - How do I make sure my resources are utilized efficiently?
  - Engineer - How do I stop having to run the same task weekly/daily/hourly?
- In essence, ‘What problem are you trying to solve’?

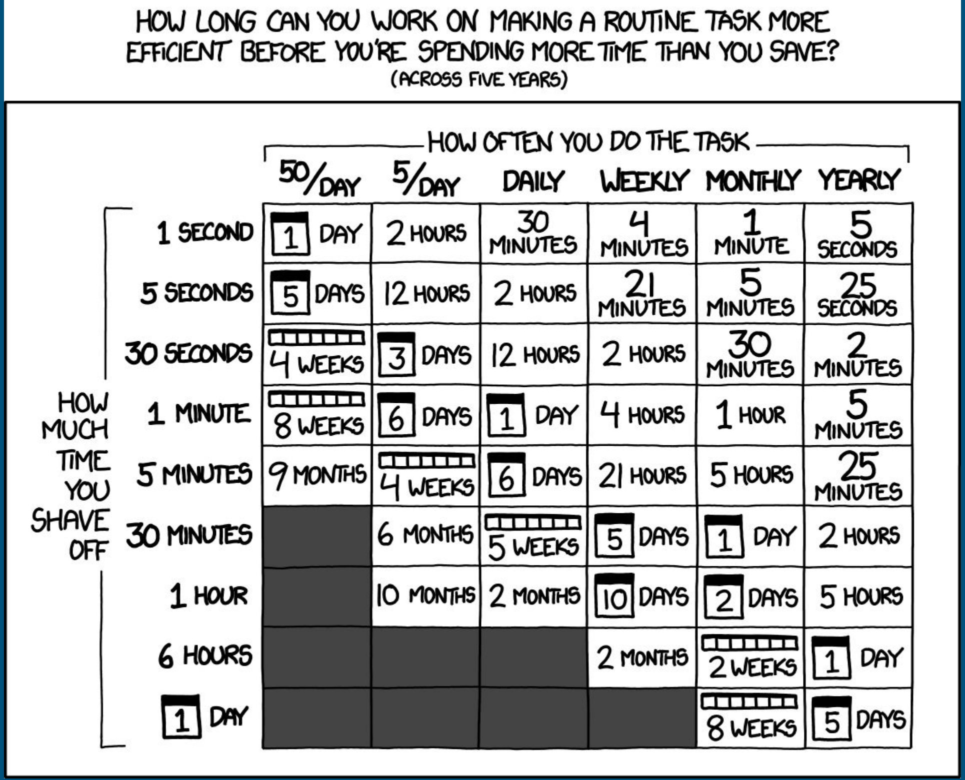
Organization Needs

- Different questions can still be part of the same goal
- Automating simple daily tasks can have significant impact:
  - A daily task which takes 30 minutes save a week's worth of effort annually
  - A monthly task which takes a full day can save ~2 week's worth of effort annually
- These small optimizations add up quickly, but can drain resources unintentionally
  - Automating a 5 second task performed daily only saves 24 minutes annually

Organization Needs

- Engineers:
  - Understand and communicate the tasks that take a significant amount of time
  - Automate tasks, not full jobs or functions
  - Use existing tools!
- Managers:
  - Help your team to prioritize their tasks
  - Offer assistance in getting the right resources to automate tasks
  - Communicate up to the value of these tasks
  - Help developers and engineers avoid the ‘Not Invented Here’ syndrome
- Executives:
  - Trust, but verify
  - Provide resources (training, infrastructure, time, buy-in) to support automation

Organization Needs



HOW LONG CAN YOU WORK ON MAKING A ROUTINE TASK MORE EFFICIENT BEFORE YOU'RE SPENDING MORE TIME THAN YOU SAVE?
(ACROSS FIVE YEARS)

	HOW OFTEN YOU DO THE TASK					
HOW MUCH TIME YOU SHAVE OFF	50/DAY	5/DAY	DAILY	WEEKLY	MONTHLY	YEARLY
1 SECOND	1 DAY	2 HOURS	30 MINUTES	4 MINUTES	1 MINUTE	5 SECONDS
5 SECONDS	5 DAYS	12 HOURS	2 HOURS	21 MINUTES	5 MINUTES	25 SECONDS
30 SECONDS	4 WEEKS	3 DAYS	12 HOURS	2 HOURS	30 MINUTES	2 MINUTES
1 MINUTE	8 WEEKS	6 DAYS	1 DAY	4 HOURS	1 HOUR	5 MINUTES
5 MINUTES	9 MONTHS	4 WEEKS	6 DAYS	21 HOURS	5 HOURS	25 MINUTES
30 MINUTES	■	6 MONTHS	5 WEEKS	5 DAYS	1 DAY	2 HOURS
1 HOUR	■	10 MONTHS	2 MONTHS	10 DAYS	2 DAYS	5 HOURS
6 HOURS	■	■	■	2 MONTHS	2 WEEKS	1 DAY
1 DAY	■	■	■	■	8 WEEKS	5 DAYS

Source: XKCD

Infrastructure Information

- This is the largest common cause of automation failures
- Each service, device, application is unique
- Poor or nonexistent documentation on what goes into each service
- Infrastructure is organized by group, not function

Infrastructure Information

- Consider organizing infrastructure by roles and group:
    - DB.HR - Database for HR
    - DB.WEB - Database for Website
    - FS.CORP - File Server for Corp
    - FE.WEB - Front End for Website
- Identify and document basic information in a central database
    - IP Addresses
        - Main IP
        - IPMI/OOB
    - Server location (Datacenter, Rack, Rack Unit, Cluster/Availability Group)
    - Hostname/FQDN
    - Make and Model
    - Service Owner

Infrastructure Information

- Central Database - The Source of Truth™
- For a Source of Truth to be usable it must contain the following attributes:
  - Easy to input information
    - A Web UI for non-technical users
    - CLI for power users
    - A script, using an answer file/CSV
  - Easy to query
    - A Web-based Report for informational uses (How many servers are the DB.HR Role?)
    - A CLI-based tool that can be scripted
    - Individual elements, such as IP addresses, can be pulled for a specific role

Infrastructure Information

- When implementing security policies, consider the following:
  - Minimize the usage of subnets inside security policies
  - Use roles as a basis for policy enforcement
  - Add servers to roles
  - Use roles when applying policies, not individual servers
- When using roles, it is much easier to add a server to a role than it is to re-order an entire firewall policy
- Automating policies based on roles is easier than accounting for one-offs in code

Standards and Templates

- Similar to the lack of information issue, lack of standards hurt automation efforts
- One-off services can make automation a risky proposition
- Lack of a standard naming convention in servers and security policies
  - Net1.company.com can be referenced differently than NET1.company.com
- Services deployed manually often have differing software versions/patches

Standards and Templates

- Each role defined should be very similar in form and function, if not identical
- Tools such as Puppet, Chef, JAMF, and SCCM are critical here
    - Enforce a standard configuration and software package
    - Update configurations/software across the fleet/workforce
    - Highlight inconsistencies across servers
- Treat applications more like cattle instead of pets
    - “Pet” applications must be constantly maintained
    - “Cattle” applications allows for faster tear-down and rebuilding of servers
    - This also makes moving applications to a cloud service much easier!
- Create simple ‘blessed’ or blanket rules:
    - All host with the Web server role allow HTTP/HTTPS inbound
    - Corp users can always connect to any host in the Citrix Role

Scope Creep

- Quite often, many initial projects are too ambitious
- Jack of all trades, master of none
- Increasing the number of features throughout the project
- When too many things are wanted at the start, nothing ever gets completed
- Engineers will often try to automate a full job function versus a single task

Scope Creep

- Focus on a single task at a time
- Consider starting with monitoring automation
  - Pulling all link states on devices
  - Checking to see if routes/network topology has changed
  - Adding a feature your NMS lacks
- Use existing tools whenever possible

Scope Creep

- Move horizontally across a large project
  - For a network device or firewall, automate adding a single infrastructure service first:
    - DNS/NTP/SNMP servers used for name resolution/time synchronization/monitoring
    - Creating/Deleting servers in a firewall configuration
    - Adding/removing servers from a role/function
    - Combine all three tasks together - new networking provisioning tool
  - For a service or application
    - Automate the shutdown and removal of a server from a service
    - Automate ‘kicking’ (re-installing) a server from scratch based on role
    - Combine both tasks together - new server provisioning tool
  - Combine the provisioning tools together - new deployment times are greatly reduced!

In Summary

- Focus on ‘What problem are we trying to solve?’
- Start on individual tasks and build up from there
- Have a usable/searchable repository of information - The Source of Truth™
- Develop, implement, and enforce standards and template

Thank you!

Juniper Networks

Information Security Summit

You!