puppet

Puppet Enterprise with Windows

John O'Connor
Claire Cadman
Dave Johnston

23 September 2019

puppet

WIFI Sid: XENIA
Username: ccentre
Password: 99cityroad

23 September 2019

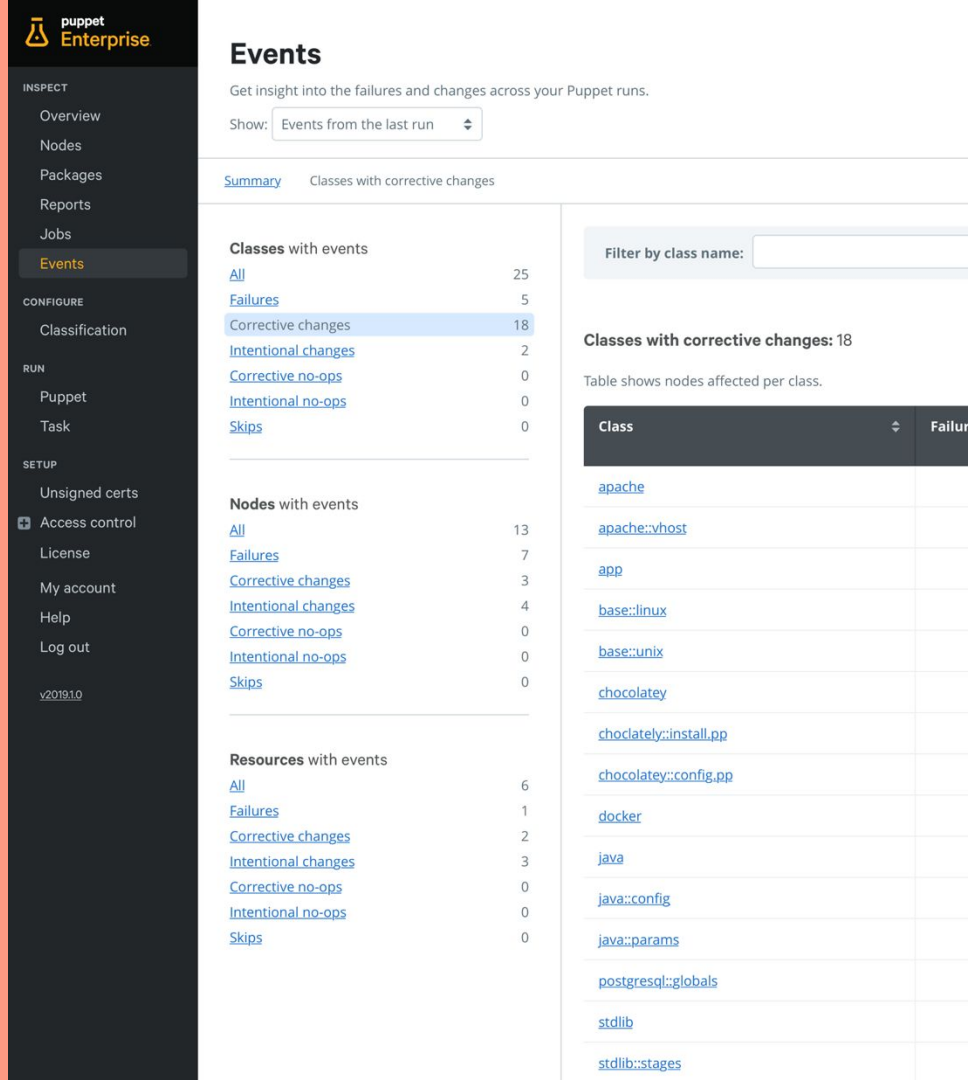
We do DevOps better because we need to

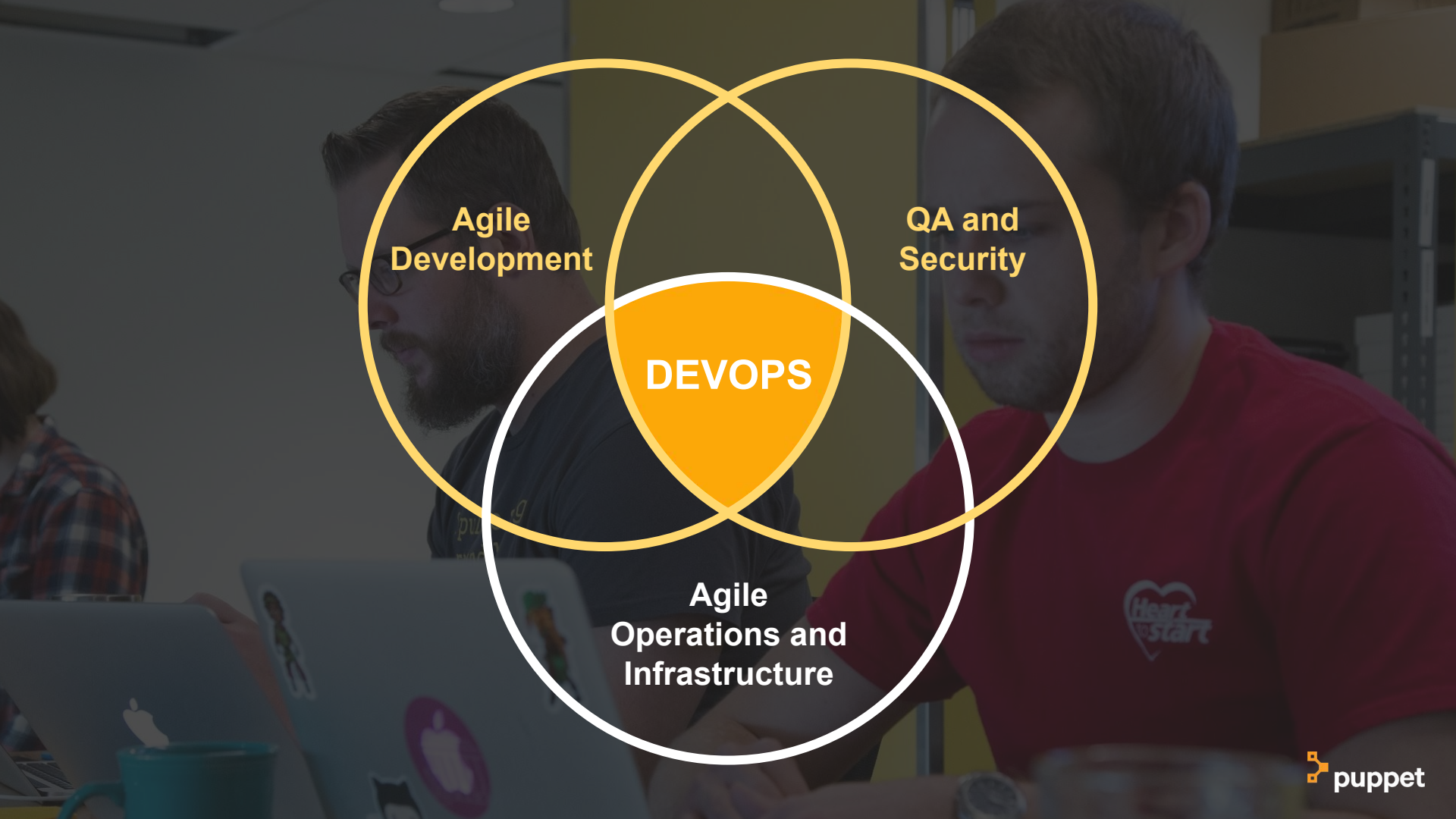
Deliver better software faster

puppet

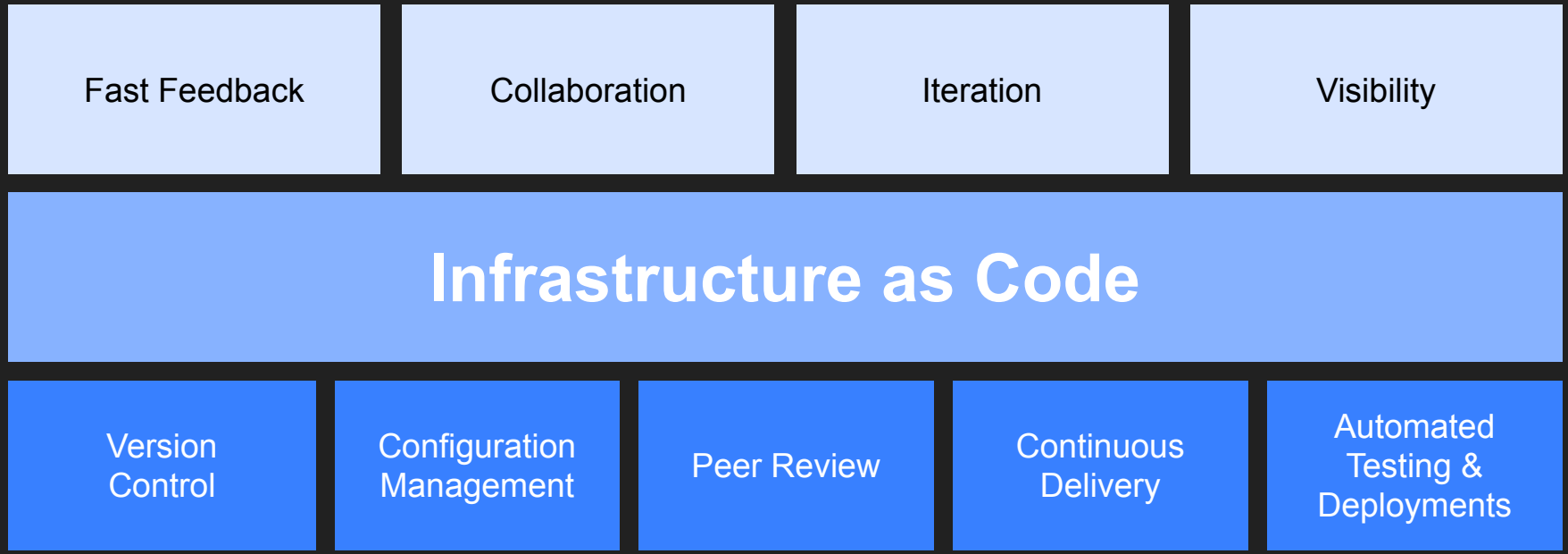
Accelerate infrastructure delivery

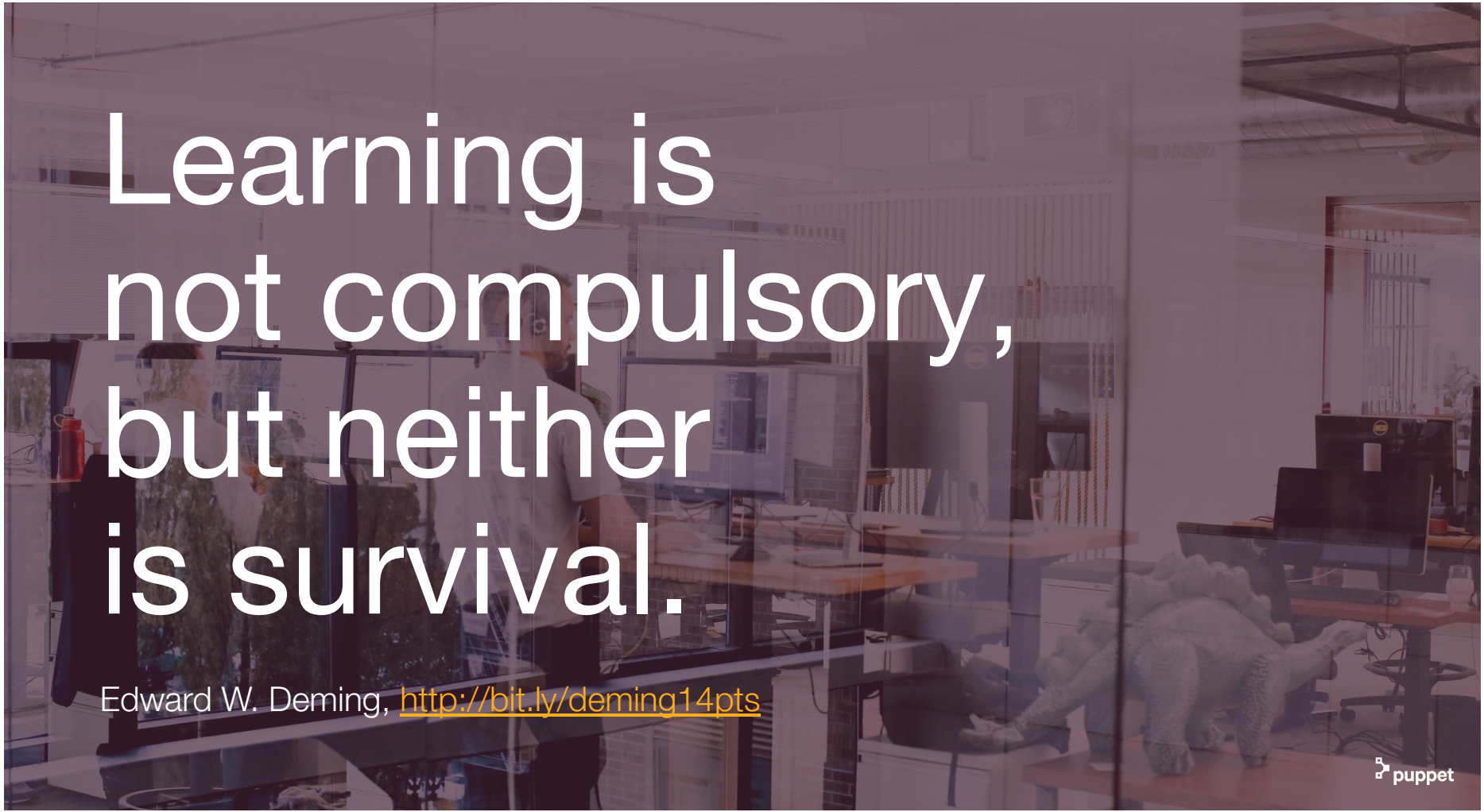
- Remediate security vulnerabilities
- Capabilities for every stage of your automation journey
- Continually monitor & enforce compliance
- Integrated CI/CD workflows for your infrastructure code




Agile
Development
QA and
Security
DEVOPS
Agile
Operations and
Infrastructure

puppet


Fast Feedback
Collaboration
Iteration
Visibility
Infrastructure as Code
Version Control
Configuration Management
Peer Review
Continuous Delivery
Automated Testing & Deployments


Learning is
not compulsory,
but neither
is survival.
Edward W. Deming, http://bit.ly/deming14pts
puppet

Pizza Anyone ????

Ordering a pizza - MENU

- Cheese & Tomato
- Mozzarella cheese (tomato, cheese)
- Vegetarian (tomato, onions, pepper, black olives)
- Pepperoni (tomato, cheese and spanish sausage)

Ordering a pizza - MENU & INSTRUCTIONS

Cheese & Tomato

- Tomato sauce
- Where is the tomato sauce?
- How do I open the can?
- How do I get the sauce out of the can?
- How much tomato sauce should I put on?……

Cheese

- How do I get from the tomato sauce to the cheese?
- Where is the cheese?
- How do I slice it? …….

EXECUTION

Put a thin layer of sauce on the dough.

Sprinkle some mozzarella cheese

Add a handful of onions

Add a handful of peppers

Add a few black olives

Procedural scripts for a pizza order

```
/******** Begin Procedure Script *********/

        BEGIN

        GOTO cupboard in the stockroom.
        GOTO third shelf from the bottom on left hand side facing the back.

        can = Take the can of tomato sauce

        open $can

        sauce = pour ½ $can onto the pizza dough

        END

/******** End Procedure Script *********/
```

Order a pizza with Puppet

Easy for a person to write and understandable for a computer

```
pizza { “John’s order”:
  sauce => tomato,
  cheese => mozzarella,
  vegetables => [ onions, peppers, black olives ],
  meat => pepperoni
}
```

Procedural (imperative) vs Declarative

Or Imperative .vs. XXXX (if you prefer)

Ordering from a computer

I need to tell the computer how to do what I want, step by step.

Ordering from a person

I just need to know what I want. The person knows how to do it.

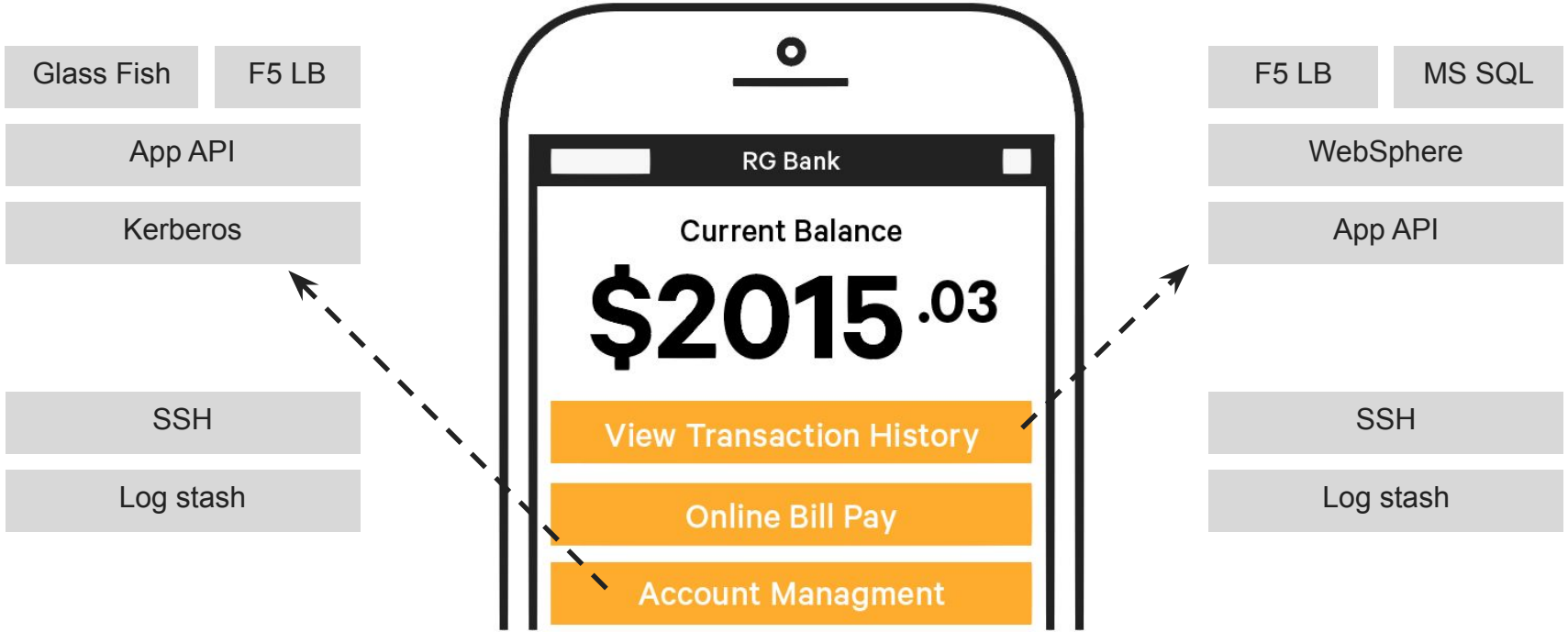
A Business Scenario

Why are we doing all this?

Why does Puppet matter in the modern world?

The APP example

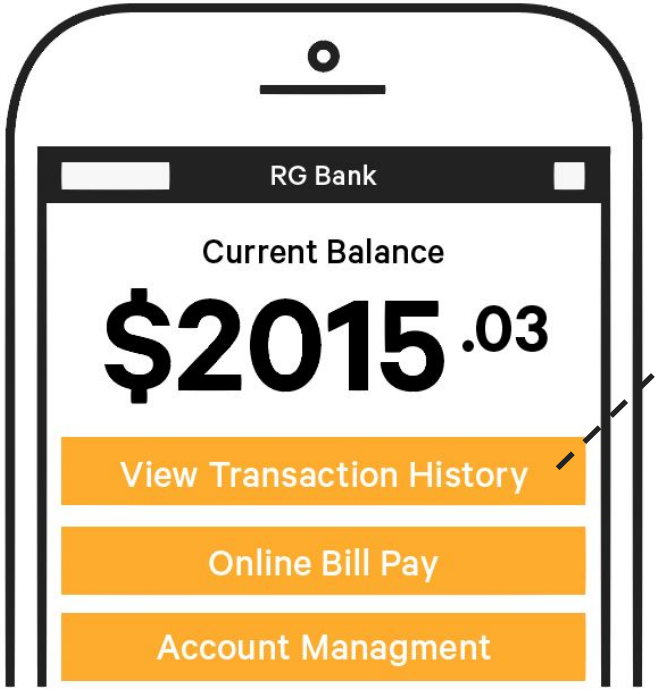
App relies on multiple services that span infrastructure



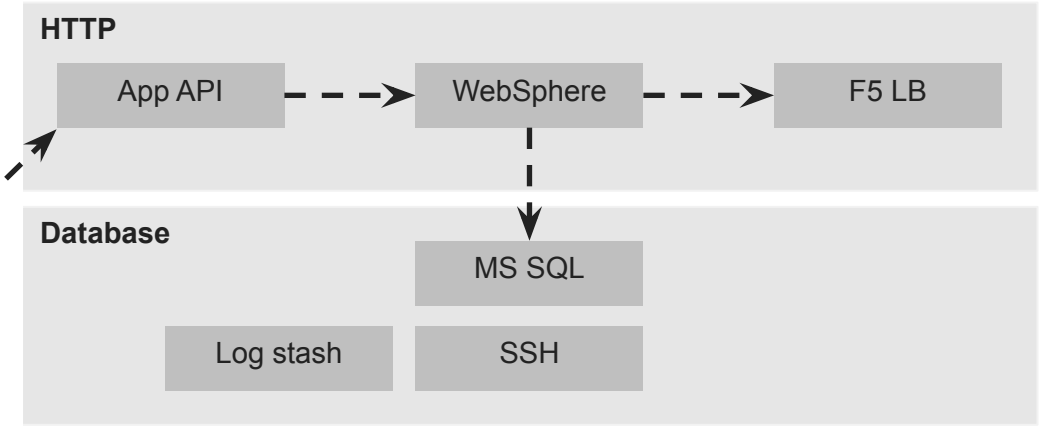
puppet

The APP example

Use Puppet language to model your application



Model Services, Dependencies, Relationships and Instances

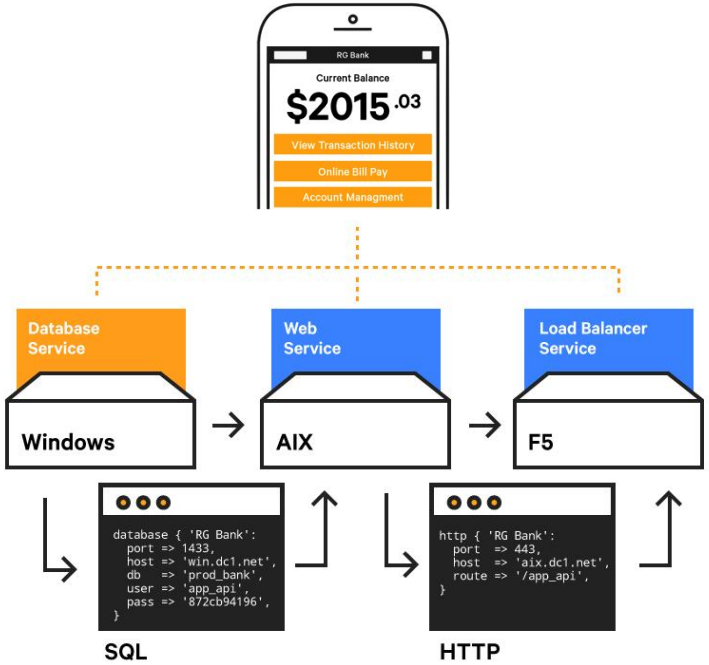


Across all environments: Dev, Staging, Production

puppet

Example application

Puppet Enterprise determines order and deploys your application.



puppet

Benefits of using Puppet over scripts

Scripts only provision, they don't manage "Day 2" and beyond.

- Puppet manages the infrastructure that it provisions. Because it knows the desired state of the infrastructure it provisions, it knows automatically if something has changed AND has the ability to enforce that configuration.

Scripts are specific to an operating system or network device.

- Puppets modules (over 5000 available to all Puppet users at forge.puppet.com) deploy the desired state to any server with any operating system.

Scripts are typically dependent on one person.

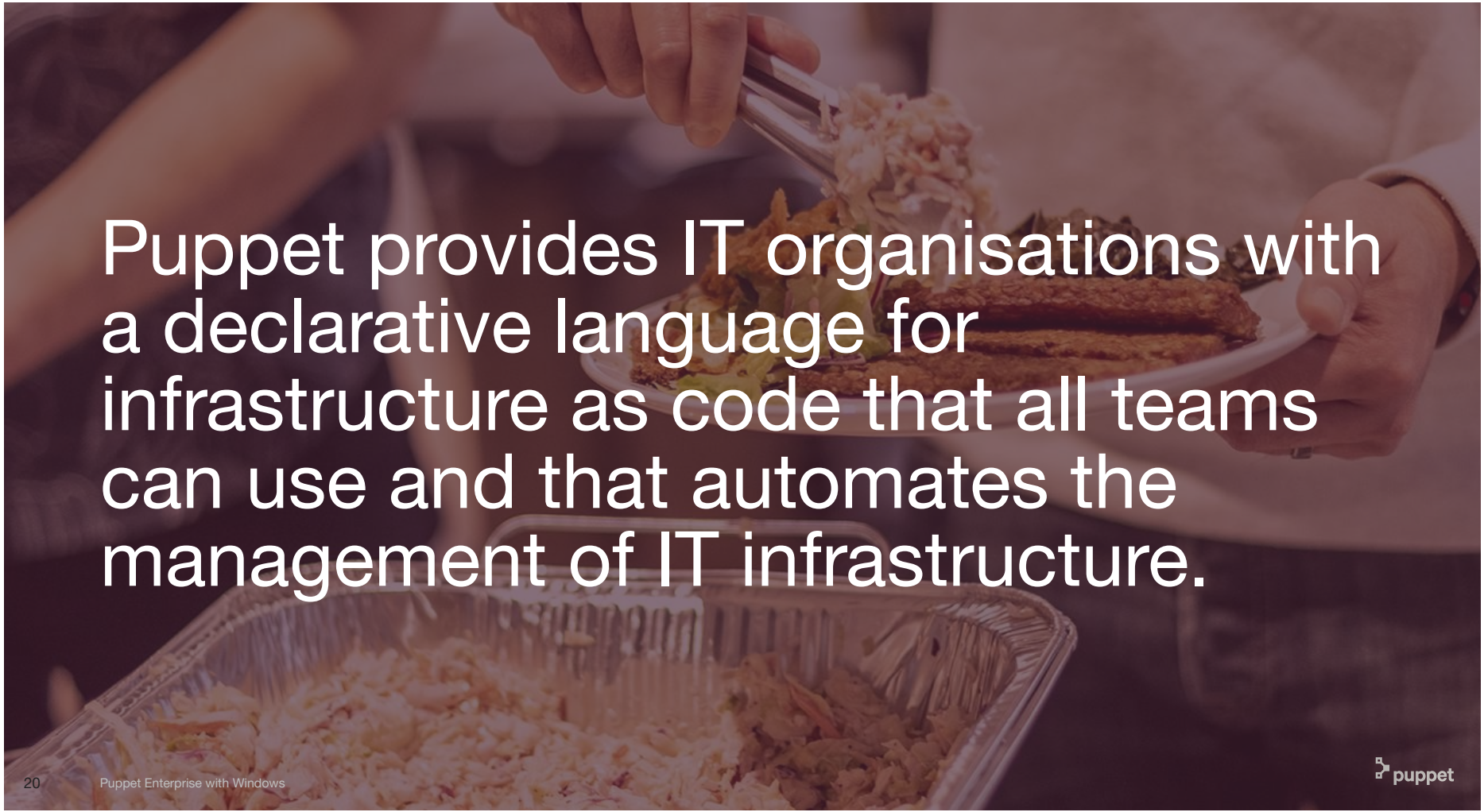
- Puppet employs a common language that any developer or administrator can easily adopt. The problem of individuals and siloed teams managing OS dependent scripts is eliminated.

Scripts aren't managed as software.

- Puppet is software. It employs the disciplines of software development like check-in and check out using any standard code repository so it can be leveraged by any team member.

Summary of Benefits

- Automates provisioning, configuration and ongoing management
- Eliminates time spent configuring, deploying, troubleshooting and managing infrastructure
- Allows teams to quickly and confidently use repeatable processes to deploy applications
- Make infrastructure-wide changes
- Enforces consistency for all systems, devices and applications
- Automatically remediates unauthorized changes
- Minimizes and often eliminates both configuration drift and downtime


Puppet provides IT organisations with a declarative language for infrastructure as code that all teams can use and that automates the management of IT infrastructure.

puppet

Puppet basics learning

Puppet Language, Roles and Profiles, Modules and the Forge

The basics of Puppet language - Resources

Resource Type listing

```
[root@training ~]# puppet describe --list
These are the types known to puppet:
anchor          -  A simple resource type intended to be used a ...
augeas          -  Apply a change or an array of changes to the ...
computer        - Computer object management using DirectorySer ...
cron            -  Installs and manages cron jobs
exec            - Executes external commands
file            - Manages files, including their content, owner ...
file_line       -  Ensures that a given line is contained withi ...
firewall        -  This type provides the capability to manage  ...
firewallchain   -  This type provides the capability to manage  ...
group           - Manage groups
host            - Installs and manages host entries
ini_setting     - .. no documentation ..
ini_subsetting  - .. no documentation ..
interface       - This represents a router or switch interface
java_ks         - Manages entries in a java keystore
k5login         - Manage the `.k5login` file for a user
macauthorization - Manage the Mac OS X authorization database
mount           - Manages mounted filesystems, including puttin ...
...
```

Common resource types

```
package { 'ssh':
  ensure => present,
  name   => 'openssh-clients',
}
```

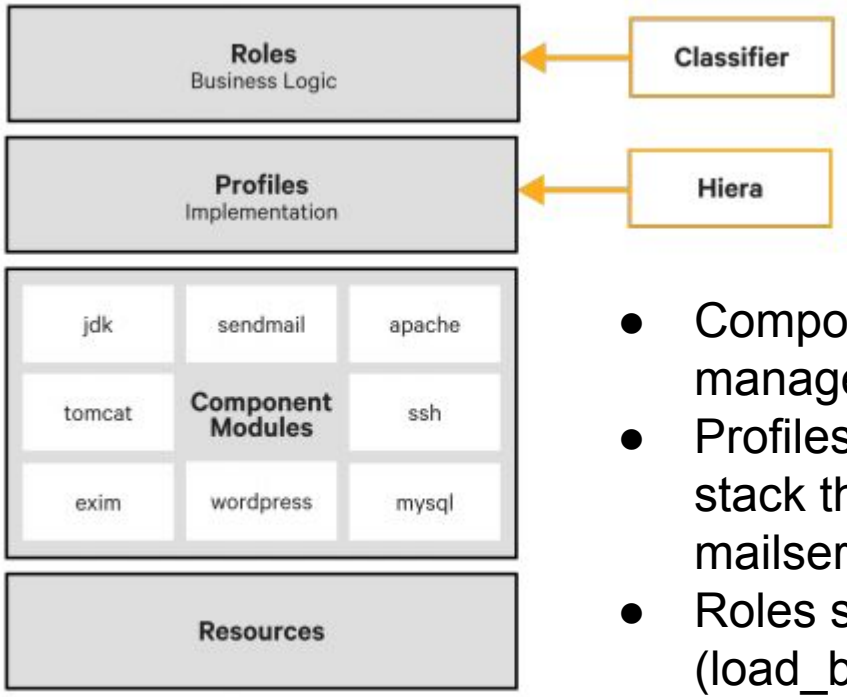
```
file { 'sudoers':
  ensure => file,
  path   => '/etc/sudoers',
  source => 'puppet:///modules/sudo/sudoers',
}
```

The basics of Puppet language - Classes

```
# A class with no parameters
class base::linux {
  file { '/etc/passwd':
    owner => 'root',
    group => 'root',
    mode  => '0644',
  }
  file { '/etc/shadow':
    owner => 'root',
    group => 'root',
    mode  => '0440',
  }
}
```

```
# A class with parameters
class apache (String $version = 'latest') {
  package {'httpd':
    ensure => $version, # Using the class parameter from above
    before => File['/etc/httpd.conf'],
  }
  file {'/etc/httpd.conf':
    ensure  => file,
    owner   => 'httpd',
    content => template('apache/httpd.conf.erb'), # Template from a module
  }
  service {'httpd':
    ensure    => running,
    enable    => true,
    subscribe => File['/etc/httpd.conf'],
  }
}
```

Roles and profiles



- Components should be named after what they manage (apache, ssh, mysql);
- Profiles should be named after the technology stack they implement (database , bastion , mailserver
- Roles should be named by business roles (load_balancer , web_cluster , application , archive)

puppet

Modules and the Forge

Modules are self-contained bundles of code and data. You can write your own modules or you can download pre-built modules from the Puppet Forge. - https://forge.puppetlabs.com/

The demo's today focuses on modules for windows including:

- puppet-windows_env
- puppetlabs-dsc_lite
- puppetlabs-iis
- puppetlabs-powershell
- puppetlabs-registry
- puppetlabs-stdlib
- puppetlabs-wsus_client

Puppet VSCode Extension

Get started writing Puppet manifests

Claire Cadman

VSCode extension website:
https://puppet-vscode.github.io/

Office hours:
https://puppet.com/community/office-hours

Hands on Puppet

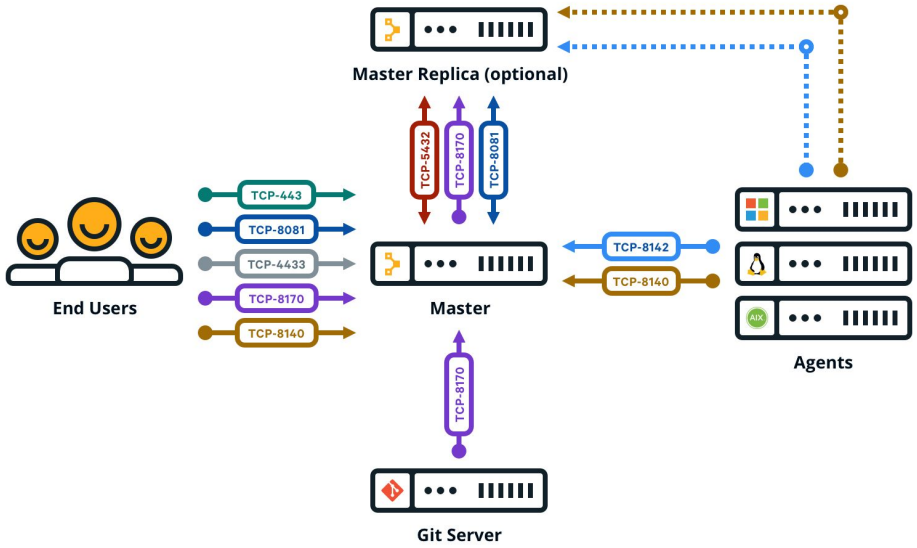
Use Puppet to configure and manage a group of pre-provisioned Windows servers on Azure

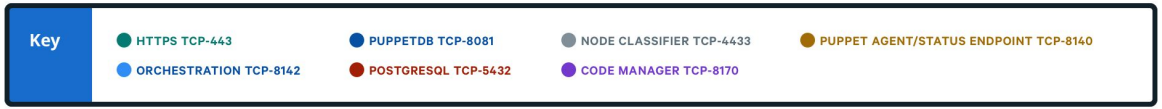
John O’Connor

WinOps “Demo” Configuration

- Add some registry entries using puppet-registry
- Create two Demo Users
- Install various packages
- Change Power Setting to Balanced
- DSC Examples:
  - Add some DSC Registry Entries
  - Use DSC to add a file to the desktop
  - Use DSC to add a user

Puppet Master/Agent Architecture





puppet

Demonstration Nodes

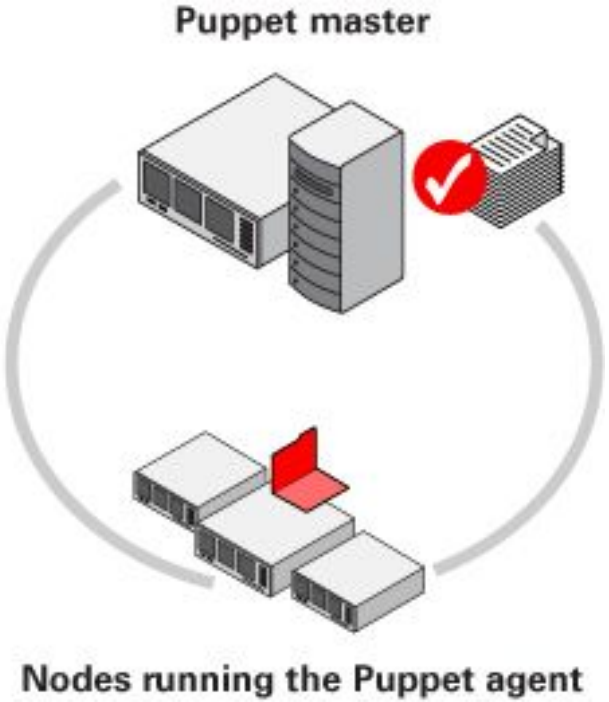
- Windows Server 2019 on Azure setup with Bolt/Azure_ARM
- Have pre-installed Puppet Agent and:
  - Visual Studio Code
  - Google Chrome
  - Git
- Will use Puppet Agent to further Configure the node and demonstration Puppet Corrective actions
- Package Inspection
- Enabling WSUS

Puppet Agent

- Is installed and runs on all client nodes (and on the master).
- Normally runs every 30 minutes but can be configured to:
  - Run at different intervals
  - Run Manually
  - Run in NoOP mode
- Can also be run on Demand from the Puppet Enterprise Console or through a Remote Management Process

Puppet Master/Agent Interaction

1. Node that is running the Puppet agent collects data about itself using facts
2. Agent sends facts to Puppet master
3. Master compiles a catalog based on data for how the node should be configured
4. Master sends catalog back to agent
5. Agent configures itself and reports back to master



puppet

“Puppet Agent -t” First Run

```
PS C:\Users\puppet> puppet agent -t
Info: Downloaded certificate for ca from
puppet.305dypwoztkuhgv5no5fu5a5xa.zx.internal.cloudapp.net
Info: Downloaded certificate revocation list for ca from
puppet.305dypwoztkuhgv5no5fu5a5xa.zx.internal.cloudapp.net
Info: Creating a new SSL key for winlarge-04
Info: csr_attributes file loading from C:/ProgramData/PuppetLabs/puppet/etc/csr_attributes.yaml
Info: Creating a new SSL certificate request for winlarge-04
Info: Certificate Request fingerprint (SHA256):
4B:F6:70:09:4A:F1:AE:F7:EE:CA:7E:EB:5B:0F:11:43:76:6C:D1:A4:DA:7F:85:DF:A6:9F:DC:3C:79:CE:9B:22
Info: Downloaded certificate for winlarge-04 from
puppet.305dypwoztkuhgv5no5fu5a5xa.zx.internal.cloudapp.net
Info: Using configured environment 'production'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Notice: /File[C:/ProgramData/PuppetLabs/puppet/cache/lib/facter]/ensure: created
Notice: /File[C:/ProgramData/PuppetLabs/puppet/cache/lib/facter/aio_agent_build.rb]/ensure:
```

“Puppet Agent -t” - Run - No Changes

```
PS C:\Users\puppet> puppet agent -t
Info: Using configured environment 'production'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Retrieving locales
Info: Loading facts
Info: Caching catalog for winlarge-04
Info: Applying configuration version '1568974493'
Notice: Applied catalog in 29.26 seconds
PS C:\Users\puppet>
```

“Puppet Agent -t” First Run

```
PS C:\Users\puppet> puppet agent -t
Info: Using configured environment 'production'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Retrieving locales
Info: Loading facts
Info: Caching catalog for winlarge-04
Info: Applying configuration version '1568974493'
Notice: /Stage[main]/Profile::Users::Demousers/User[winopsdemo_1]/ensure: created
Notice: /Stage[main]/Profile::Users::Demousers/User[winopsdemo_2]/ensure: created
Notice: /Stage[main]/Profile::Power::Power/Exec[set power scheme]/returns: executed successfully
Notice: /Stage[main]/Profile::Util::Util/Package[notepadplusplus]/ensure: created
Notice: /Stage[main]/Profile::Util::Util/Package[treesizefree]/ensure: created
Notice: Applied catalog in 29.26 seconds
PS C:\Users\puppet>
```

Puppet Remediate

Find and Fix Vulnerabilities

Dave Johnston

What are we doing today?

- What is Puppet Remediate (vulnerability management)
- Where can you get it
- Demo: Remediating a Windows CVE

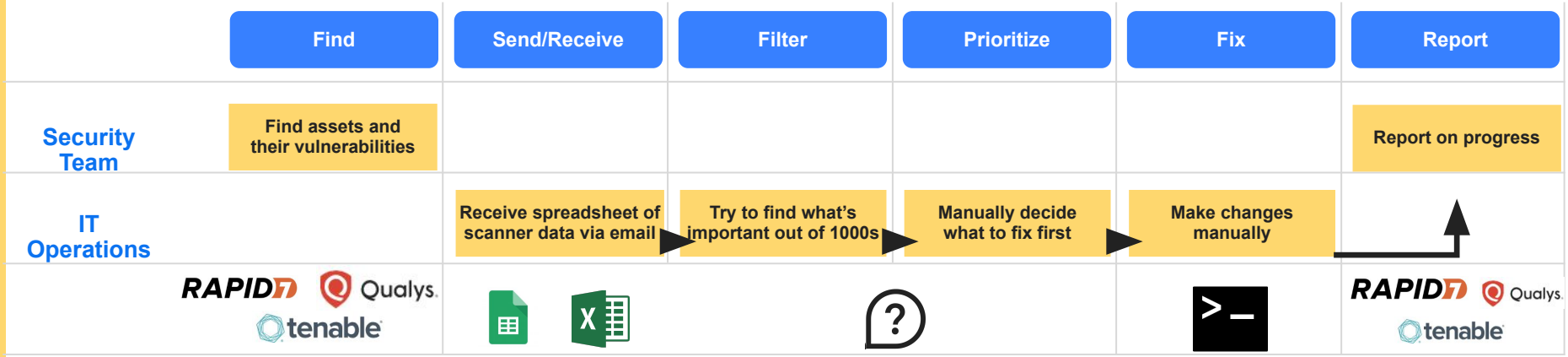
Vulnerability management - What is it?

Vulnerability management is the practice of identifying, classifying, prioritizing, remediating, and mitigating, software **vulnerabilities**.

Is vulnerability management and patching the same thing?
They are related but they are not the same thing.
Patching helps preventing vulnerabilities but is not enough!

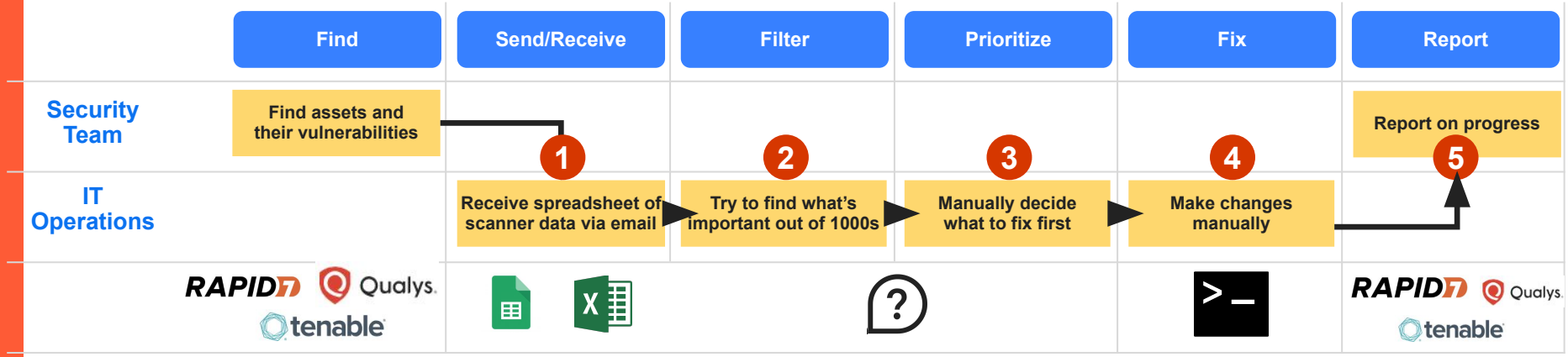
How do I identify vulnerabilities left in the system?
I can use vulnerability scanners, like:
Qualys, Rapid7 and Tenable.

Vulnerability management process



puppet

Typical problems with managing vulnerabilities



1. IT Ops wastes time confirming whether data is current.
2. Don't know what's important to fix out of thousands.
3. Takes days/weeks to prioritize critical vulnerabilities.
4. Takes too long. No standard approach to fixing.
5. Completely manual. No reliable way to show what's fixed.

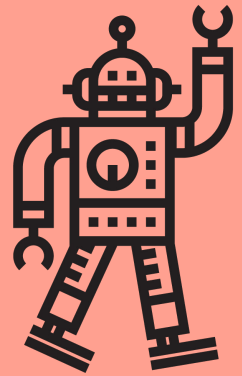
Implications

Data breaches/loss of share & brand value

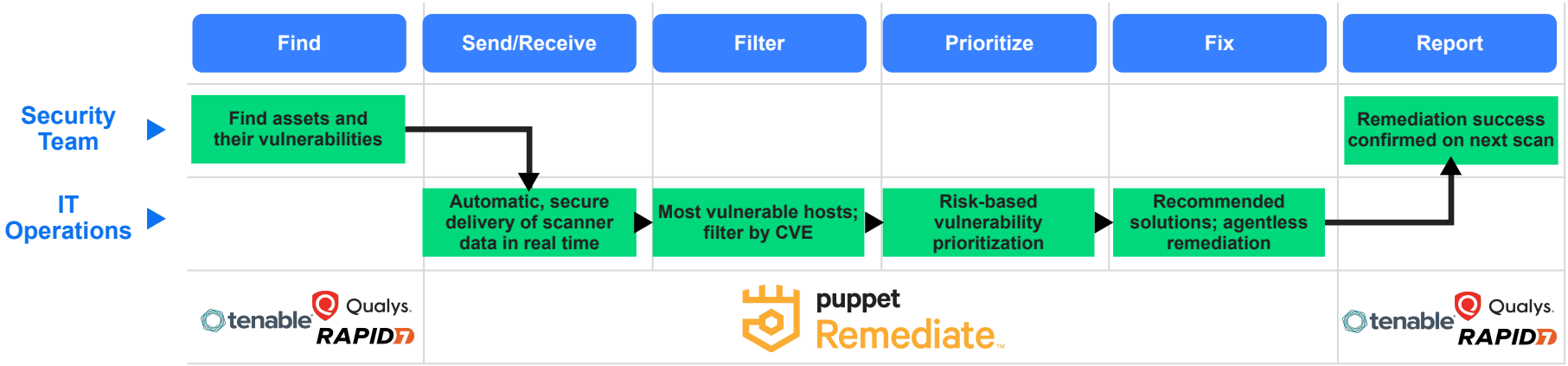
Losing people due to lack of DevSecOps

Inability to fix vulnerabilities fast enough

Puppet Remediate helps organizations mitigate their security risks.



Puppet Remediate + scanner integrations accelerate the vulnerability remediation workflow



Customers such as a global retailer and a U.S. Federal agency expect to:

- Reduce the time to fix vulnerabilities from weeks or days down to less than a day.
- Reduce the number vulnerabilities in their systems.
- Get through audits faster and with less effort.

puppet

Remediate Windows Hosts

Installation

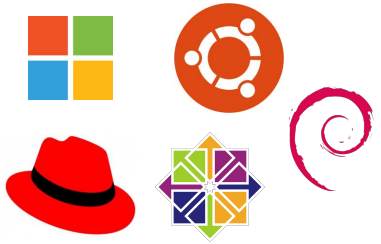
Register for free trial license here:
https://puppet.com/products/puppet-remediate

Download the compose file:
https://storage.googleapis.com/remediate/stable/latest/docker-compose.yml

```
choco install docker-desktop
docker swarm init
docker-compose run remediate start --license-file
./license.json
```

Login to Remediate:
https://<hostname/ip>:8443

Supported Platforms

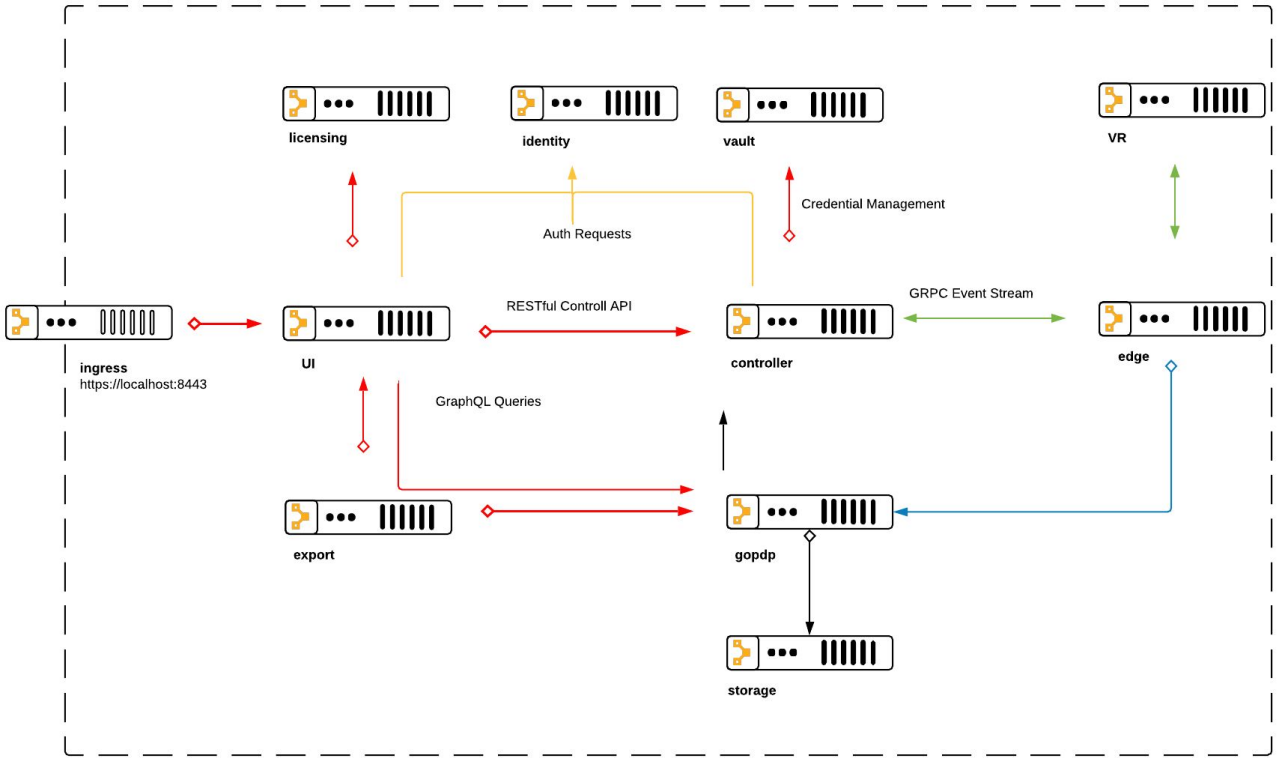


Prerequisites

Docker

puppet

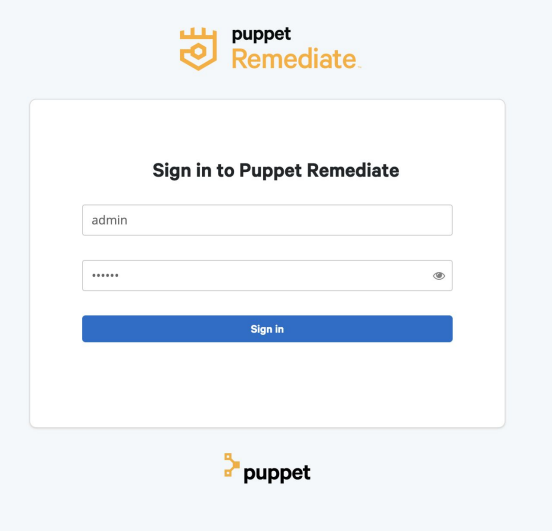
Architecture

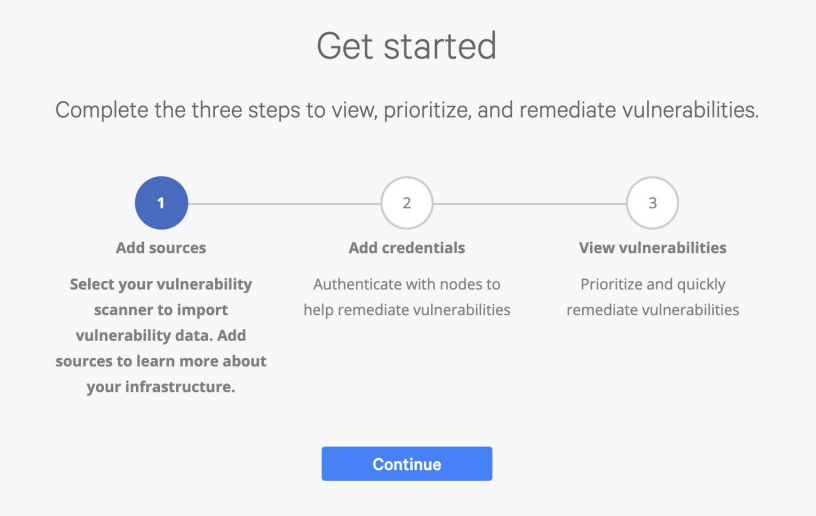


Login and first time flow

https://remediate.winops2019.automationdemos.com:8443

Login: user01
Password: remediate





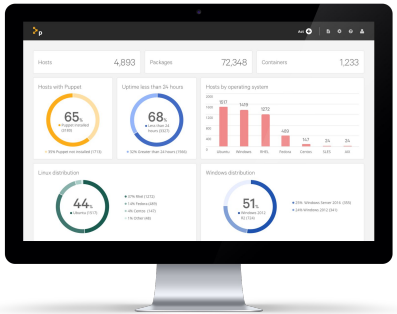
puppet

Discovery

2)
Query Providers for Host and Vulnerability data

3) Return Host and Vulnerability Info

1) Add
Account Details
WinRM/SSH Credentials

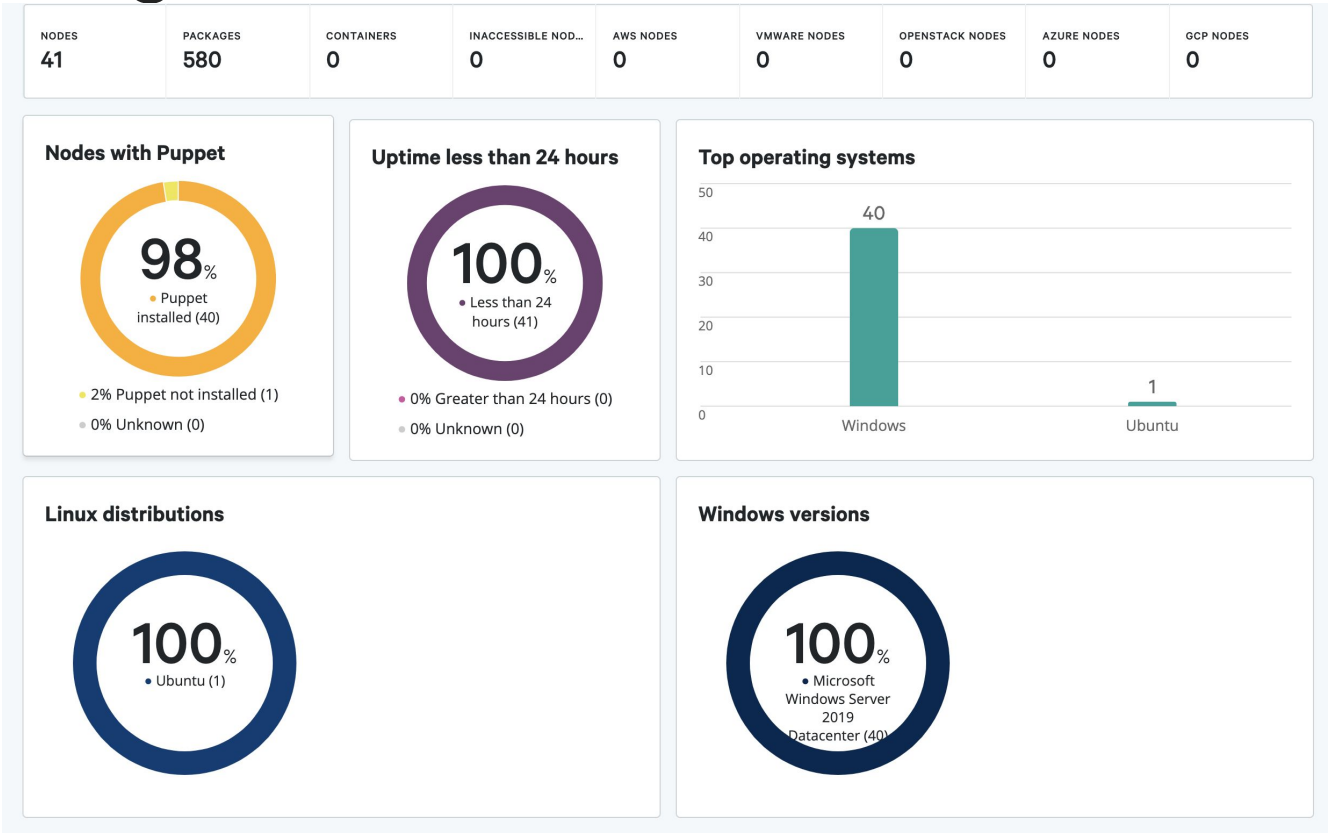


4) Query Hosts for Package, User, Service Info

5) Return package, user and service info

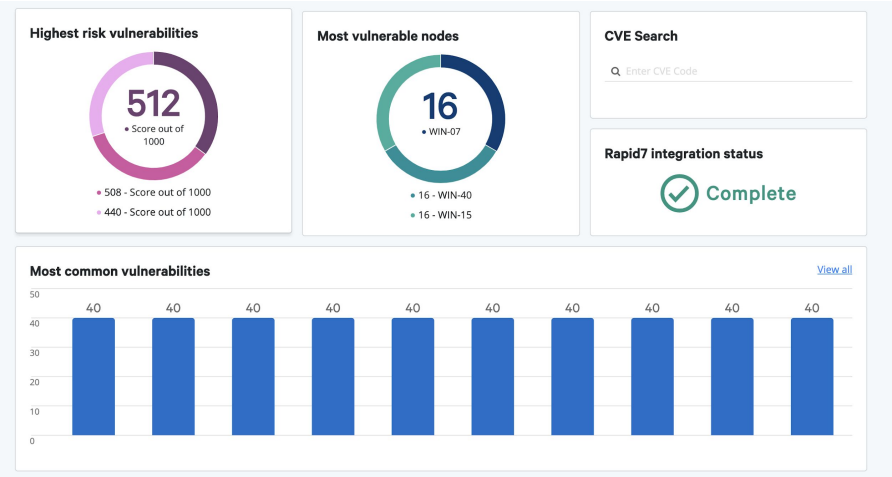
puppet

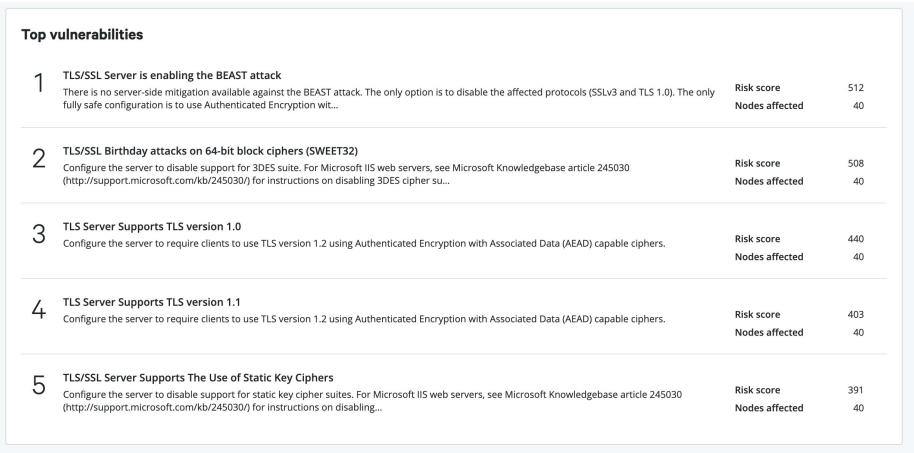
Exploring the Dashboard



puppet

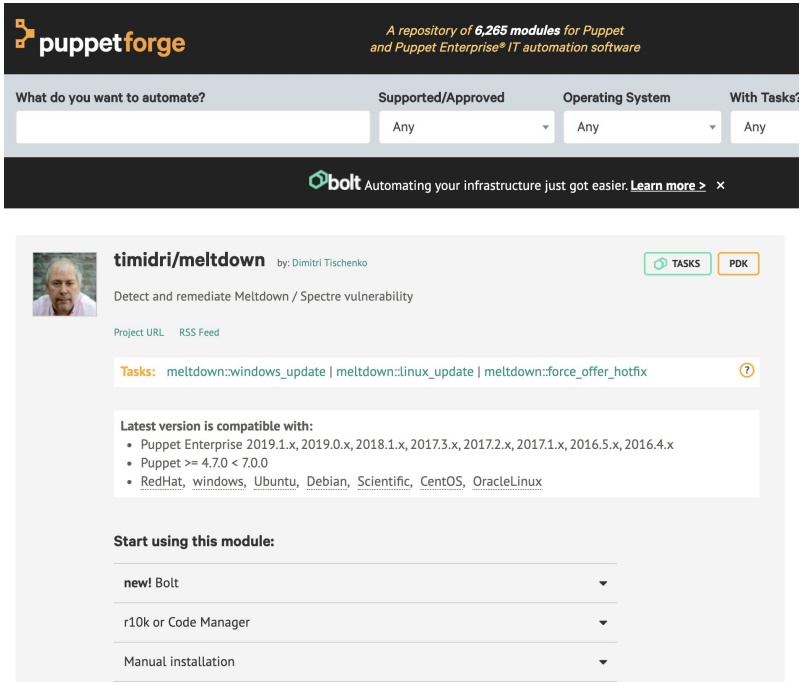
Finding Vulnerabilities

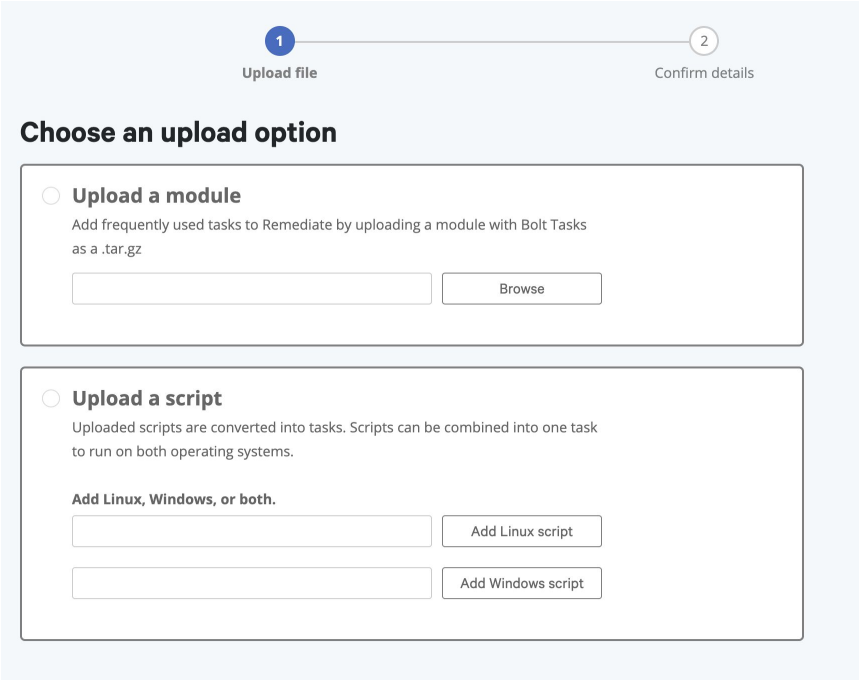




puppet

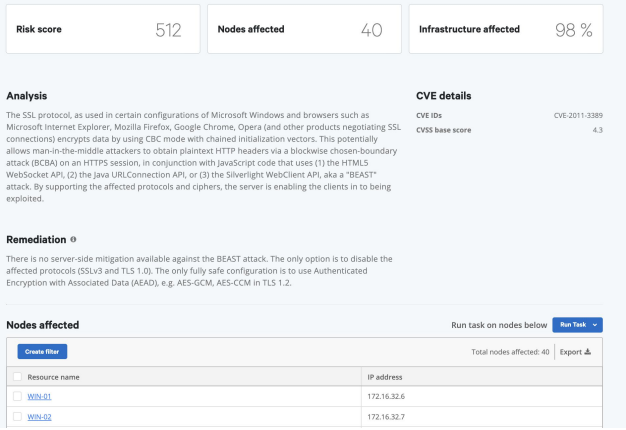
Working with Tasks

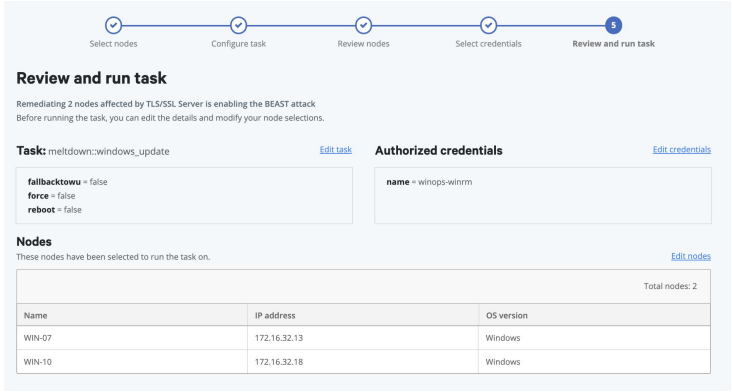


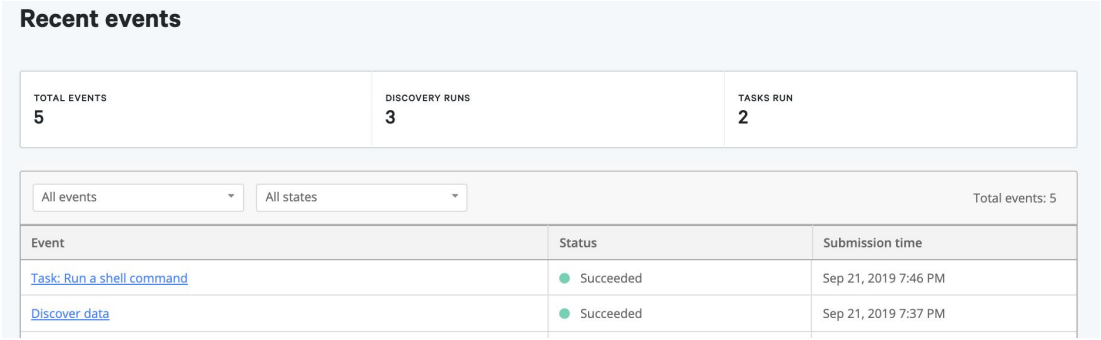


puppet

Fixing the Vulnerability







puppet

Roadmap

- RBAC - fine grained controls
- Full Audit Logging
- Improved dashboards
- Tracking Fixes

Find out more about Remediate

puppetcommunity.slack.com @DaveJ

puppet

Q&A

Stay Connected

github.com/jcoconnor/winops2019

John O'Connor
Senior Software Engineer
john.oconnor@puppet.com

Claire Cadman
Technical Writer
claire.cadman@puppet.com

Dave Johnston,
Senior Software Engineer
dave.johnston@puppet.com

puppet