

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center

The logo consists of the word "BETTER." in a bold, white, sans-serif font. The letters are partially obscured by a complex network of thin, curved lines in shades of blue, green, and yellow, which radiate from the bottom right corner of the slide.

SESSION ID: ASD-F02

DevSecOps for the Rest of Us!

Sara Perrott

Sr. Information Security Technology Engineer
BECU
Twitter: @PerrottSara

#RSAC

More Time in the Day

Don't you wish you had more time?

- Time for project work?
- Time for training?
- Time for lunch?
- Time for vacation?



This Photo by Unknown Author is licensed under [CC BY-NC-ND](#)

Cloning Technology

Wouldn't it be great if there were more of you?

- Too much manual work
- Poor work/life balance
- Stress
- Burnout

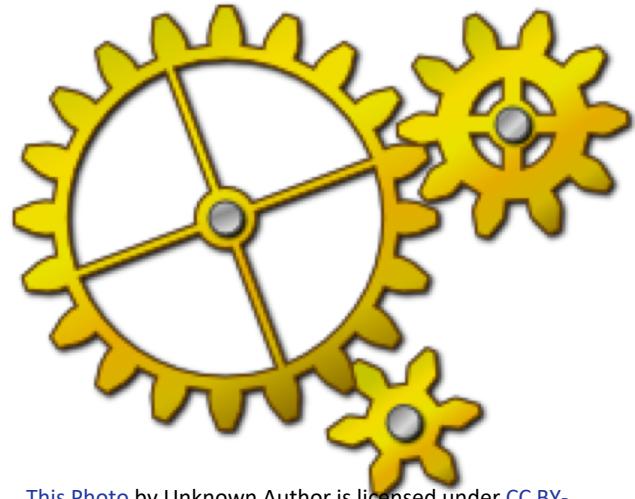


[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

Automation

Imagine if you will...

- A ticket is created in your ticketing system for a new server
- That ticket kicks off a workflow, and the server is automatically built with the specifications from the ticket
- Instead of the server build taking a few hours, it is done within 15-30 minutes



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

What is DevOps and DevSecOps?

- DevOps
 - Continuous Integration
 - Continuous Delivery
- DevSecOps
 - Moving Security to the Left
- What does this have to do with me?



[This Photo](#) by Unknown Author is licensed under [CC BY](#)

DevOps/DevSecOps is not just for Developers!



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

Tools in Your Arsenal-PowerShell

- Universal language
- Expandable with modules
- Product Specific modules:
PowerShell Gallery
- Tell it how it should be built



Module

psCheckPoint

By: tkoopman | 679 downloads | Last Updated: 8/22/2018 | Latest Version: 1.0.1

Commands for accessing Check Point Web-API Calls

Tags [firewall](#) [checkpoint](#)

Module

pfSense

By: masters274 | 219 downloads | Last Updated: 12/7/2017 | Latest Version: 0.8

pfSense management functions built for pfSense version 2.x

Tags [pfSense](#) [firewall](#) [security](#) [vpn](#)

Module

Checkpoint

By: masters274 | 92 downloads | Last Updated: 8/8/2018 | Latest Version: 1.2

Command line management, and automation of Checkpoint Firewall systems

Tags [checkpoint](#) [firewall](#) [security](#) [vpn](#) [network](#)

Tools in Your Arsenal-PowerShell Issues

Remote PowerShell

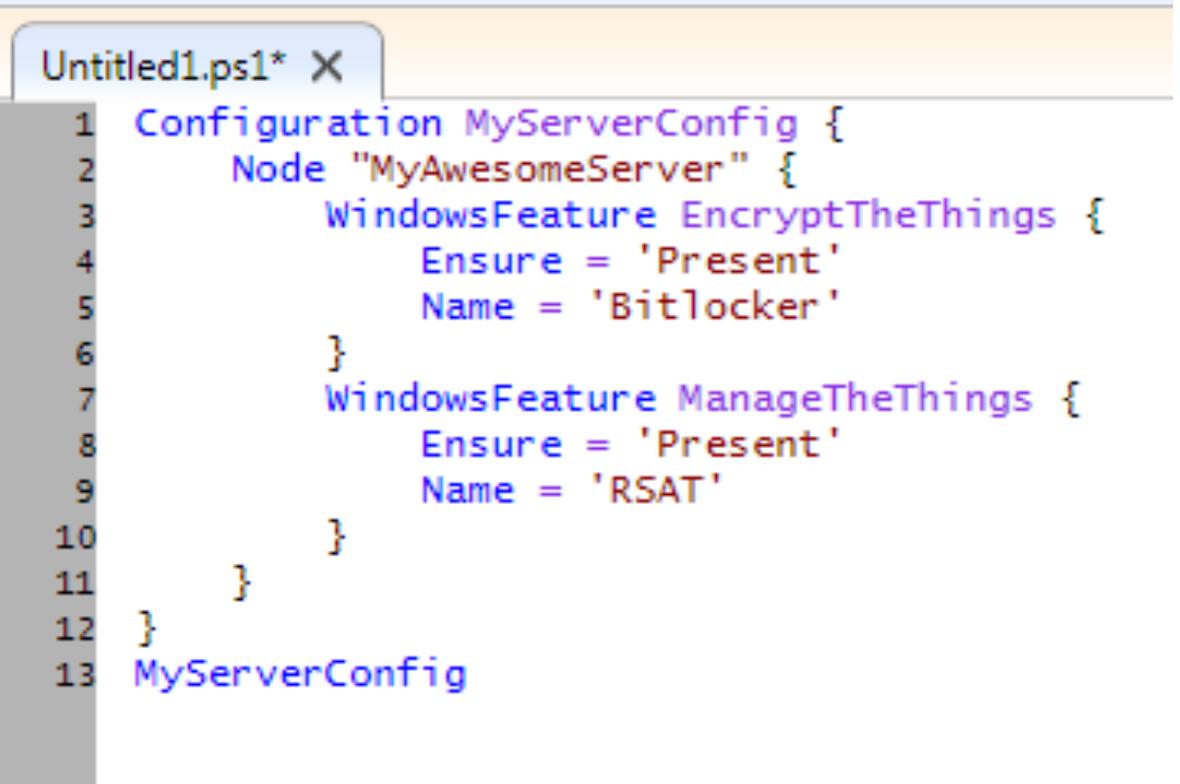
- Firewall ports:
 - WinRM
 - TCP 5985 (HTTP)
 - TCP 5986 (HTTPS)
- Execution Policy
 - RemoteSigned



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

Tools in Your Arsenal-PowerShell DSC

- Saved as ps1
- Tell it what it is
 - not how it is



The screenshot shows a code editor window titled "Untitled1.ps1*". The script content is as follows:

```
1 Configuration MyServerConfig {
2     Node "MyAwesomeServer" {
3         WindowsFeature EncryptTheThings {
4             Ensure = 'Present'
5             Name = 'Bitlocker'
6         }
7         WindowsFeature ManageTheThings {
8             Ensure = 'Present'
9             Name = 'RSAT'
10        }
11    }
12 }
13 MyServerConfig
```

Tools in Your Arsenal-PowerShell DSC Issues

- Behavior: Push or Pull
- Know the correct names
 - Roles
 - Features
 - Services



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

When to use...

PowerShell

- Instructions (How)



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

PowerShell DSC

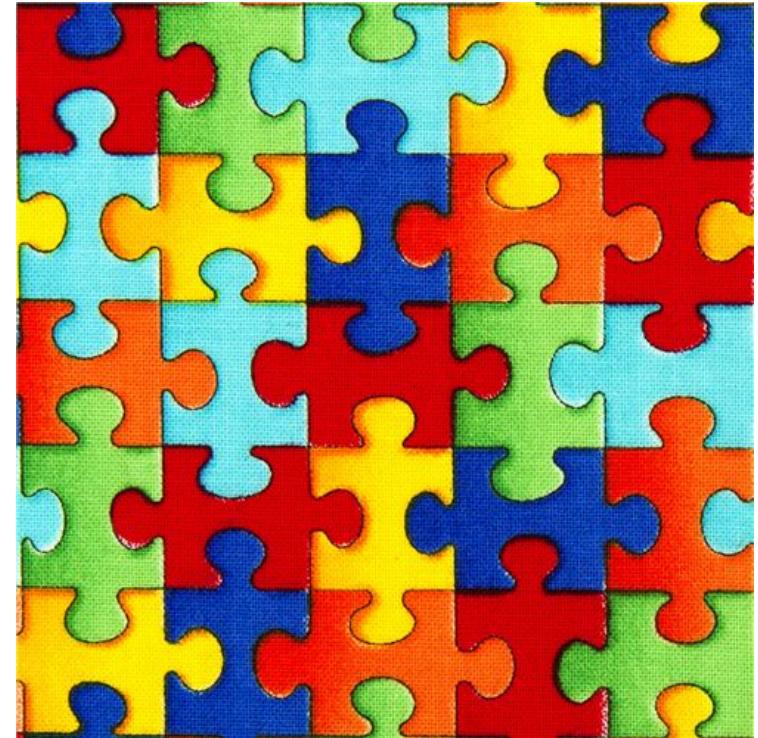
- Vision (What)



[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)

Infrastructure as Code

- IaC is a methodology-not a product!
- Treat systems like software
 - PowerShell
 - PowerShell DSC
 - Templates
 - Automation/Orchestration Tools

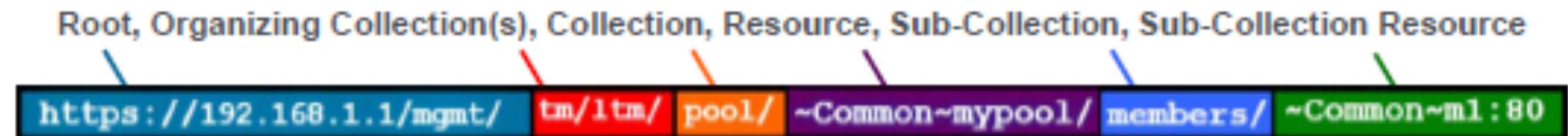


[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

Tools in Your Arsenal-REST API

- What makes up a REST API?
- From F5's NetOps Training:

ANATOMY OF A REST URI



Note: Resource names map ~ to / (e.g. ~Common~mypool is really /Common/mypool)

Tools in Your Arsenal-REST API Troubleshooting

- Authentication
 - API keys
 - For authentication, not authorization
- Access
 - Firewall Ports: usually TCP 80 & 443

Automating Firewalls and Other Appliances

Rest API

- Vendor specific
- Powerful
- Easy to integrate into programs

PowerShell

- PowerShell uses known syntax
- Modules are available from:
 - Vendor
 - Vendor site
 - Github
 - PowerShell Gallery

Tools in Your Arsenal-CloudFormation

Traits

- Simple, declarative
- Editable with your fav text editor
- Available from your fav vendors!

AWS WAF Example

```
Parameters:  
SqlInjectionProtectionParam:  
  Type: String  
  Default: 'yes'  
  Allowedvalues:  
    - 'yes'  
    - 'no'  
  Description: choose yes to enable t  
  
CrosssitescriptingProtectionParam:  
  Type: String  
  Default: 'yes'  
  Allowedvalues:  
    - 'yes'  
    - 'no'  
  Description: Choose yes to enable t
```

Tools in Your Arsenal-ARM Templates

Traits

- Simple, declarative
- Editable with your fav text editor
- Available from your fav vendors!

ARM WAF Example

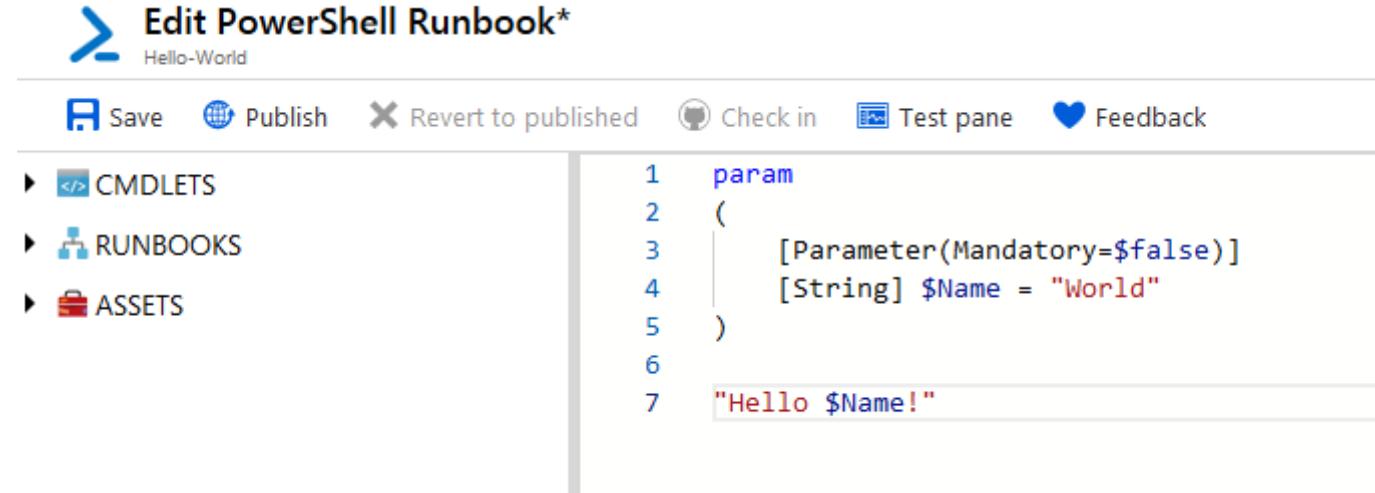
```
"applicationGatewaySize": {  
    "type": "string",  
    "allowedValues": [  
        "WAF_Medium",  
        "WAF_Large"  
    ],  
    "defaultValue": "WAF_Medium",  
    "metadata": {  
        "description": "application gateway size"  
    }  
}
```

Tools in Your Arsenal-Azure Automation

Traits

- Editable with Azure's graphical editor
- Sample runbooks available from the Azure Marketplace

Runbook Example



The screenshot shows the Azure portal interface for editing a PowerShell runbook named "Hello-World". The top navigation bar includes Save, Publish, Revert to published, Check in, Test pane, and Feedback buttons. On the left, there are navigation links for CMDLETS, RUNBOOKS, and ASSETS. The main code editor area contains the following PowerShell script:

```
param()
[Parameter(Mandatory=$false)]
[String] $Name = "World"
Hello $Name!
```

JSON Troubleshooting

- Trailing comma – your arch nemesis

```
try {  
    var json = `  
        {  
            "first": "Hedy",  
            "last": "Lamarr",  
        }`  
}
```



```
try {  
    var json = `  
        {  
            "first": "Hedy",  
            "last": "Lamarr"  
        }`  
}
```



Automation Tools

Chef

- Tons of free training
- Azure/AWS native support
- DevOps Focus



Puppet

- Paid and Free Training
- Azure/AWS native support
- Operations/System Admin Focus



Recap-Tying Things Together

- Automate routine tasks
- You don't have to be a developer to benefit...
- You can go on vacation!



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

“Apply” Slide

- Next week you should:
 - Define at least one use case where you can start using DevSecOps to improve your life
- In the first three months following this presentation you should:
 - Get more comfortable with PowerShell and PowerShell DSC if you are not already
 - Play with JSON and get familiar with the syntax
- Within six months you should:
 - Be working on your first use case...

Learning Resources-Videos

- Pluralsight
 - Paths: Windows PowerShell: Essentials
 - Windows PowerShell Desired State Configuration Fundamentals
 - Automating AWS with CloudFormation
 - Getting Started with Azure Automation
 - Getting Productive with Chef Cookbooks
 - Paths: Configuration Management using Puppet

Learning Resources-Books

- Learn Windows PowerShell in a Month of Lunches, 3rd Edition
 - By Don Jones and Jeffery Hicks
- Pro PowerShell Desired State Configuration
 - By Ravikanth Chagani
- Implementing DevOps with Microsoft Azure
 - By Mitesh Soni
- Effective DevOps with AWS
 - By Nathaniel Felsen
- Windows Server 2019 & PowerShell All-in-One Desk Reference For Dummies (Release date: April 30, 2019)
 - By Sara Perrott

Learning Resources-Other

- Other Training
 - F5 NetOps Training <https://f5.com/education/super-netops-training>
 - Chef Training <https://learn.chef.io/#/>
 - Puppet Training <https://learn.puppet.com/category/self-paced-training>

Learning Resources-Tools

AWS CloudFormation

- AWS Sample Templates
 - <https://aws.amazon.com/cloudformation/aws-cloudformation-templates/>
- Check Point Firewalls
 - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111013
- Palo Alto Firewalls
 - <https://github.com/PaloAltoNetworks/aws>

Azure ARM

- Azure Sample Templates
 - <https://azure.microsoft.com/en-us/resources/templates/>
- Palo Alto Firewalls
 - <https://github.com/PaloAltoNetworks/azure>
- Cisco Firewalls
 - <https://github.com/cisco-security/public-cloud>

Q&A

Sara Perrott

saraperrott@icloud.com

Twitter: @PerrottSara

<https://www.saraperrott.com>

<https://github.com/sara-perrott/RSAC2019>