



# Enabling SOAR and Automated Incident Response Using Comprehensive Ecosystem Integrations

*Chris Usserman, Principal Security Architect, Infoblox*



A Refresher—

# DAILY NEWS

Cyber Attack Exposes Millions of Customers' Data  
Company hit with massive fines, stock plummets



# Cyber Attacks Growing in Complexity and Scale



- \$2.7 billion monetary losses in 2018 per FBI<sup>1</sup>
- Cost of Remediation far outweighs the cost of prevention



- Notable public breaches have resulted in millions of records stolen
- Breach victim's future business jeopardized

1. FBI Internet Crime Report 2018



# But Security Teams Cannot Respond to Incidents Fast Enough



- 196 days on average between infection and detection
- Not all organizations have necessary people/tools/automation to correlate data from multiple systems

## ***Customer A***

Had a lot of data to analyze and decided to outsource SOC operations because they couldn't analyze it themselves



## ***Customer B***

Didn't know all the places in the network where they were using threat intel and failed to operationalize on it



# And Throwing More People at the Problem is Not Possible

92%

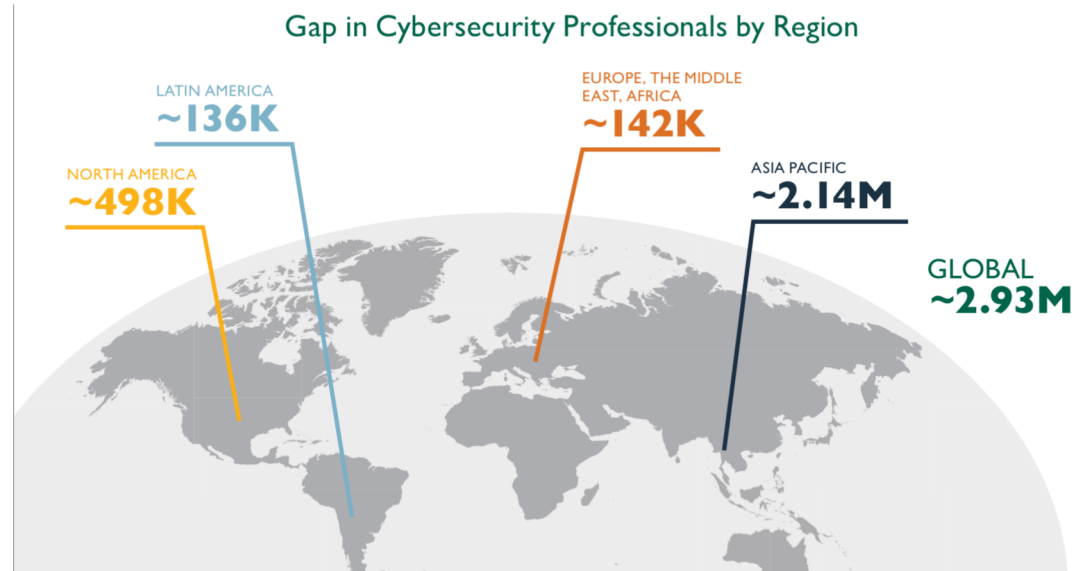
of companies get more than 500 alerts per day; a single cyber analyst can handle only ~10

4%

of alerts are investigated; not enough humans to keep organizations safe

30+

security tools in operation, with staff and expertise to manage ~12



# How Hard Is It To Rent A Botnet?



rent a botnet



All

News

Images

Shopping

Videos

More

Settings

Tools

About 237,000 results (0.46 seconds)

## DDoS for Hire | Booter, Stresser and DDoSer | Incapsula

<https://www.incapsula.com/ddos/booters-stressers-ddosers.html>

It turns out, not much is needed to actually **rent a botnet**. Usually, it boils down to a PayPal account, ill-will towards the target and willingness to break the law.

[Botnet](#) · [DDoS Attack Scripts](#) · [DDoS attacks](#)

## Build, buy, or lease? The 15-minute botnet - Cyren

<https://www.cyren.com/blog/articles/build-buy-or-lease-the-15-minute-botnet/>

Jul 10, 2017 - Because the software required to launch a proper **botnet** is complex ... in on **botnet** purchase and **rental** schemes by developing the software ...

## Do You Know How Much It Costs to Rent an IoT Botnet? | Secplicity ...

<https://www.secplicity.org/2017/03/07/know-much-costs-rent-iot-botnet/>

Mar 7, 2017 - **Renting** an IoT **botnet** is probably less expensive than you think. IoT **botnets** are the new Flavor of the Month when it comes to cyber attack ...

## You Can Now Rent a Mirai Botnet of 400,000 Bots - Bleeping Computer

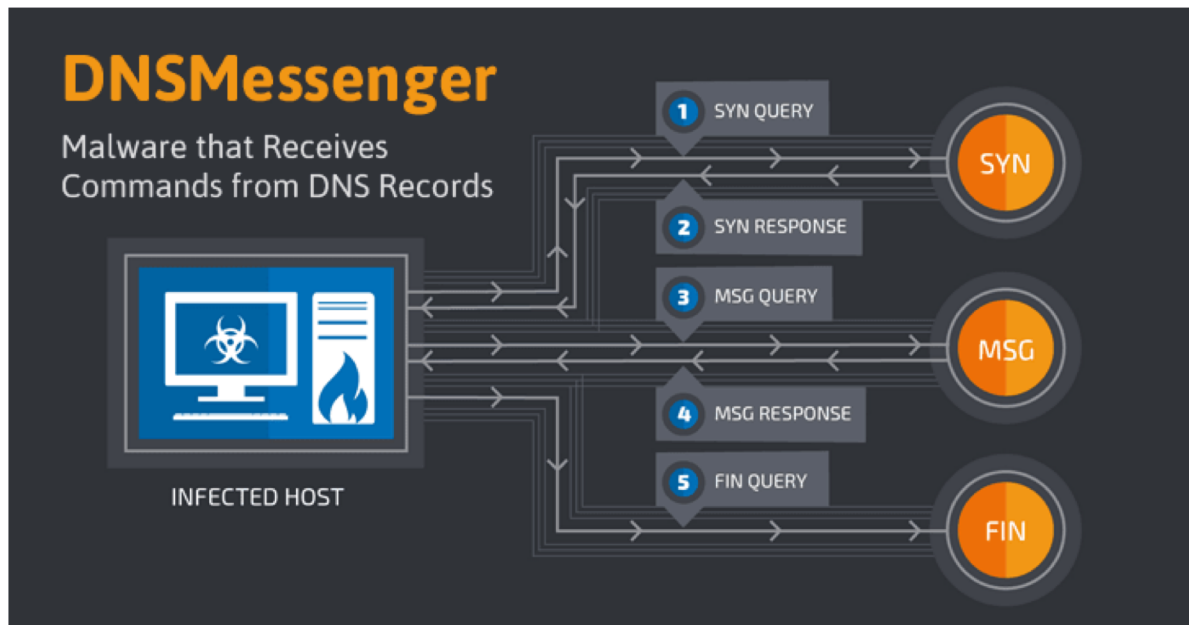
<https://www.bleepingcomputer.com> · [News](#) · [Security](#)

Nov 24, 2016 - Two hackers are **renting** access to a massive Mirai **botnet**, which they claim has more than 400000 infected bots, ready to carry out DDoS ...



# DNS Infil-/Exfiltration

- -TEXTMATE (FireEye) DNS Tunneling **via fileless attack**
- Made cyber news in Mar '17
- Involved 4 stages of attack beginning with a malicious attachment
- Bi-directional communications via DNS TXT records



Source: [thehackernews\[.\]com/2017/03/powershell-dns-malware.html](http://thehackernews[.]com/2017/03/powershell-dns-malware.html)





Arno0x / DNSExfiltrator

Watch 21

Star 243

Fork 69

Code

Issues 1

Pull requests 0

Projects 0

Insights

**Join GitHub today**

GitHub is home to over 28 million developers working together to host and review code, manage projects, and build software together.

[Sign up](#)

Dismiss

Data exfiltration over DNS request covert channel





# The Bottomline

- Threats growing exponentially in quantity and capability
- Impossible to match skills of a well trained, distributed, global malware developer
- Threat actors aren't bound by political or legal limitations
- Enterprise visibility suffers at the rate of expansion
- Human-in-the-loop security analysis cannot scale at the rate of security events



# Maturing your Cyber Security Program



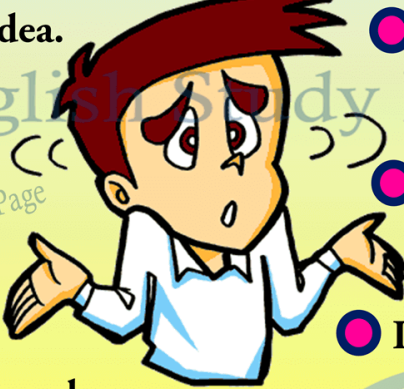
" MAYBE WE SHOULD TRY A DIFFERENT SECURITY APPROACH THIS YEAR. "



# The 3 Worst Words You Can Say in Cyber Security?

---

## WAYS TO SAY I DON'T KNOW

- 
- I have no idea.
  - I am unsure.
  - Search me.
  - Don't ask me.
  - Beats me.
  - I am not sure.
  - I don't have a clue.
  - That's a good question. I'll check it.
  - I don't know anything about ...
  - I don't have any information about that.

[www.englishstudypage.com](http://www.englishstudypage.com)  [facebook.com/englishstudypage](https://facebook.com/englishstudypage)



# Elements of a Mature Cyber Security Program

Actionable Network Intelligence (IT)

+

Actionable Threat Intelligence (Security)

+

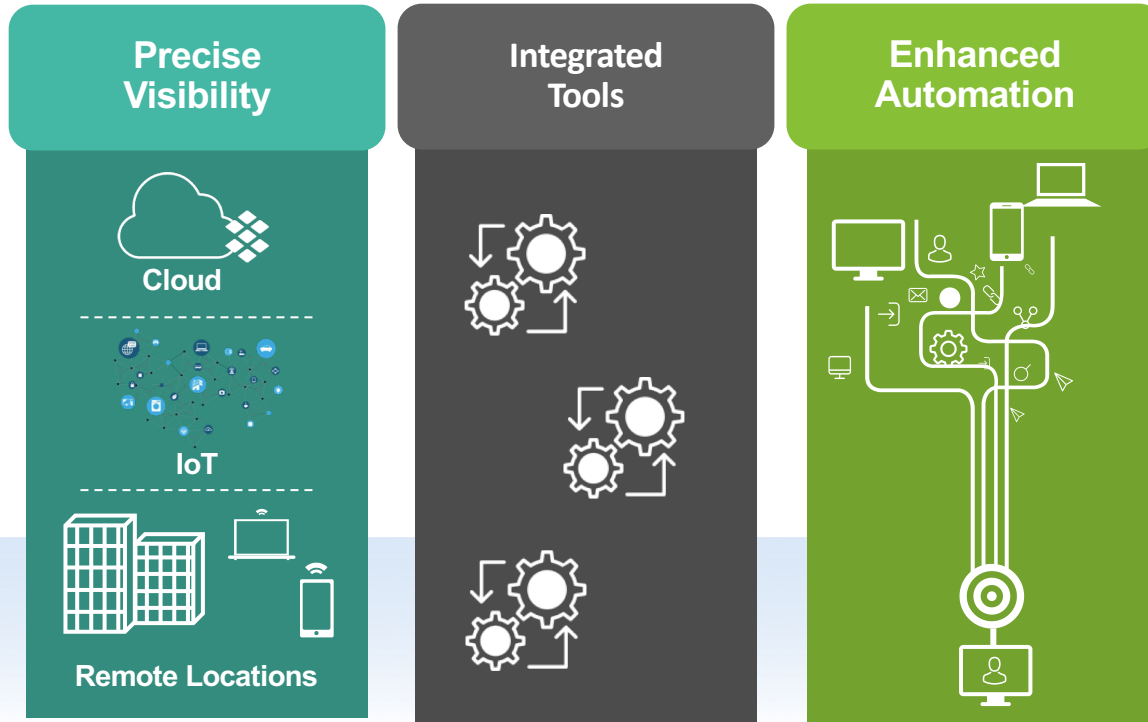
Informed Ecosystem

=

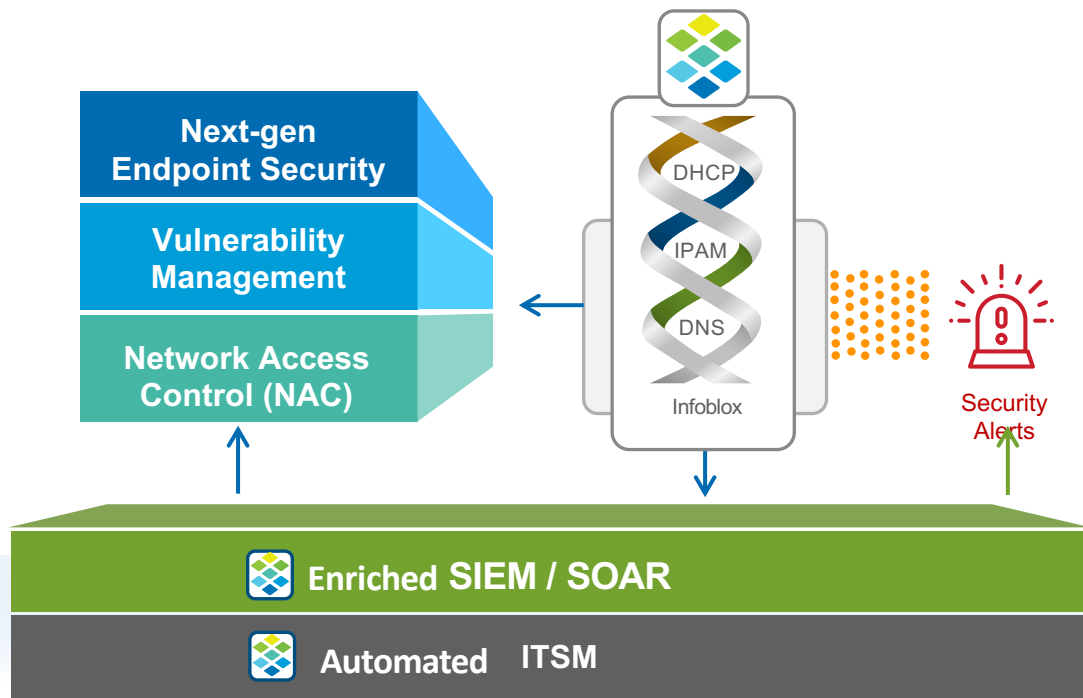
Holistic and Mature Cyber Security Program



# Key Tenets of Efficient Security Operations



# Improve Productivity and Enhance Automation



## DNS

- Malicious activity inside the security perimeter
- Includes BYOD and IoT device
- Profile device & user activity

## DHCP

- Device Audit Trail and Fingerprinting
- Device info, MAC, lease history

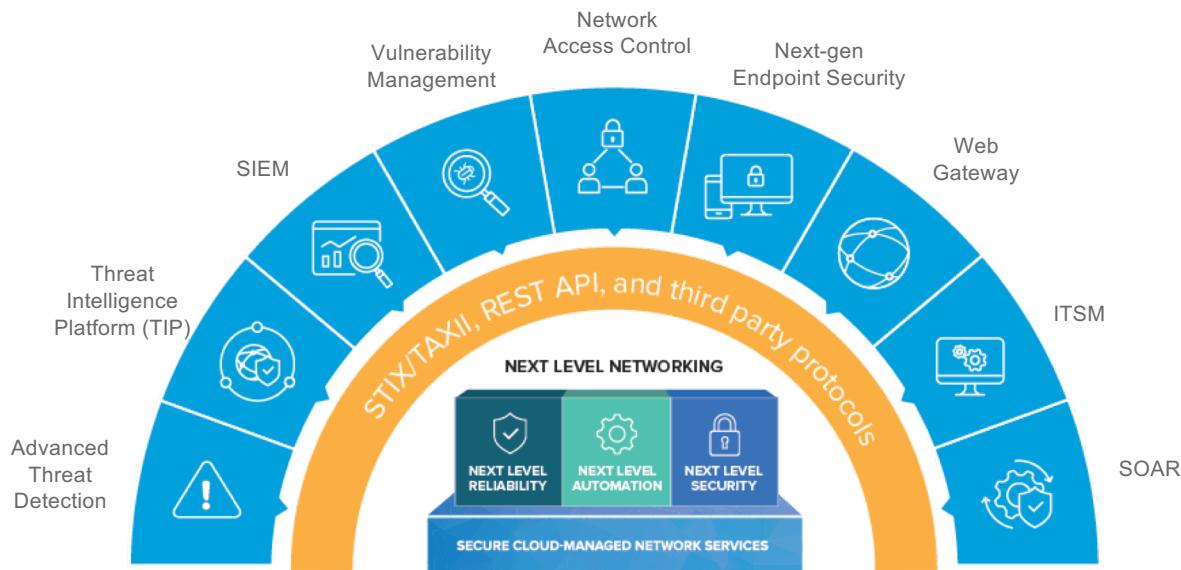
## IPAM

- Application and Business Context
- "Metadata" via Extended Attributes: Owner, app, security level, location, ticket number
  - Context for accurate risk assessment and event prioritization



# Combined DDI, Threat Intel and Context to Power SOAR Platforms

Enriched data and integrations that can be relied upon to build automation



## DNS

- Malicious activity inside the security perimeter
- Includes BYOD and IoT device
- Profile device & user activity

## DHCP

- Device Audit Trail and Fingerprinting
- Device info, MAC, lease history

## IPAM

- Application and Business Context
- “Metadata” via Extended Attributes: Owner, app, security level, location, ticket number
  - Context for accurate risk assessment and event prioritization

Prioritize 100s of alerts | Automate incident response | Reduce cost of human touch/error





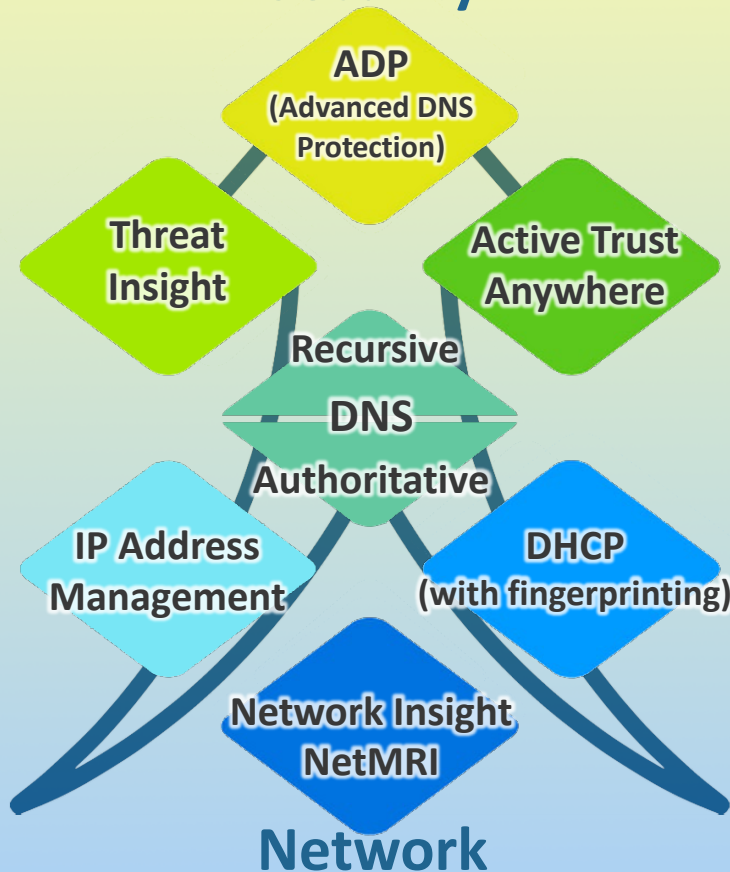
Carbon Black.



...and many more.

Infoblox Security Ecosystem

# Infoblox TIDE and Dossier Security



Know the Threats: Proactive / Reactive

DDoS Resilience

Protect Your Data from Leaving

Protect Where You are Going from Anywhere

Where are they going?

Provide Your DNS

Where are they?

Who and what is on my network?

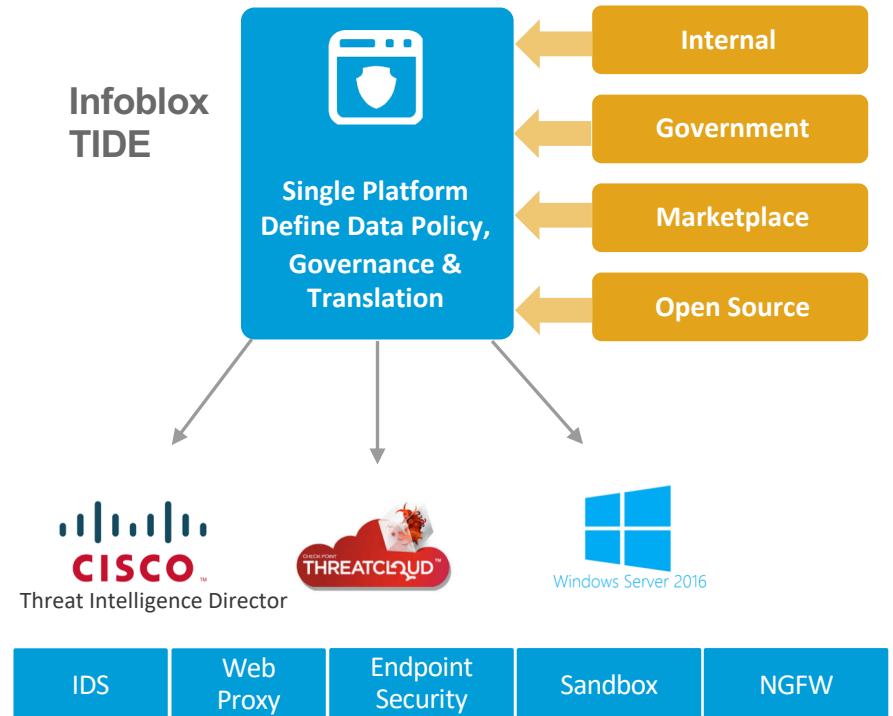
What is on your network?





# Security Policy Unification

- 3rd party platform receives malicious host names, IP addresses and URLs from TIDE
- 3rd party platform can now block/monitor more threats
- Improves effectiveness and delivers better ROI for your security stack





For the second year, Lucky Strike B-AR Honda brings you its 00E Formula One car stripped bare. From recognisable components such as the front and rear wings and the wheels right down to the electrical assembly systems and engine management controls, B-A-R presents you with the picture you want to see. For more information on the B-AR Honda 00E visit:

**BARf1.com**

**Key components**

- 1 Front wing/noose assembly
- 2 Monocoque
- 3 Mirror assembly
- 4 Honda V10 engine
- 5 Exhaust system
- 6 Hydraulic plate assembly
- 7 Clutch actuator assembly
- 8 Gearbox assembly
- 9 Rear impact structure
- 10 Rear wing assembly
- 11 Fuel tank
- 12 Headrest
- 13 Steering wheel
- 14 Radiator duct assembly
- 15 Engine coverside pods
- 16 Drivers seat
- 17 Bargeboard
- 18 Lower front wishbone
- 19 Top front wishbone
- 20 Front brake ducts
- 21 Steering rack assembly
- 22 Front suspension damper
- 23 Front strutrod
- 24 Lower rear wishbone
- 25 Top rear wishbone
- 26 Rear pushrod
- 27 Rear trackrod
- 28 Driveshaft
- 29 Brake disc assembly
- 30 Brake caliper
- 31 BES wheels with Bridgestone tyres
- 32 Water radotor
- 33 Oil tank assembly
- 34 Main electrical harness
- 35 Aircox and air filter
- 36 Left-hand electrical assembly
- 37 Fire extinguisher
- 38 Oil cooler
- 39 Plank
- 40 Main foot assembly with diffuser
- 41 Splitter assembly
- 42 Engine management controller
- 43 Battery
- 44 Steering column
- 45 Throttle and brake pedal assembly
- 46 Rear brake ducts
- 47 Wheel nut
- 48 Damper cover
- 49 Engine heatshields
- 50 Seat belt
- 51 Camera
- 52 Airspring
- 63 Front anti roll bar



# Customer Story: Major Insurance Company

## Customer Use Case:

- Customer says: “I’m not interested in your DNS firewall. I have a Palo Alto Network Firewall, it can do all the things Infoblox can.”
- But they did have security operations challenges
  - Inefficient and ineffective vulnerability scanning for compliance; hours of wasted time and resources
  - Sandbox solution does not scale for mitigation; expensive and can’t block in remote offices
  - Query logging (for feeding into their SIEM) on Microsoft DNS can’t be enabled

**Solution:** ActiveTrust with cybersecurity ecosystem

## Outcomes:

- Infoblox tells vulnerability scanner when a new device is on the network, making it more effective
- Enable sandbox to add domains to RPZ – block across entire DNS infrastructure
- Enables DNS Query data to be sent to their SIEM





# Live Demo

Provisioning New Web Server

