Live Response with GRR

Justin Hall, CBTS

Why do we do live response?

Incident response = answering questions

Our options are:

~~Walk from machine to machine~~

~~Ask a user to find something for us~~

~~Remotely access the machine and use native OS tools~~

Load an agent on the box that can interrogate it for us

Commercial tools are expensive $$$


GRR
RAPID RESPONSE

Getting started with GRR

1. Stand up GRR server using automated script
2. Install agents on endpoints
3. Begin looking for stuff

Important Terms

Flow: A request to a client to get some stuff

Artifact: A thing to look for

Collector: A flow that looks for artifact(s)

Hunt: A flow that runs across multiple hosts

Demo: Use Case 1

“I think this machine is compromised…”

Demo: Use Case 2

“Does this machine have this artifact?”

Demo: Use Case 3

“Which of my machines have this artifact?”

Using GRR's API

```
$user = "admin"
$pass = "someadminpassword"
$pair = "${user}:${pass}"
$bytes = [System.Text.Encoding]::ASCII.GetBytes($pair)
$base64 = [System.Convert]::ToBase64String($bytes)
$basicAuthValue = "Basic $base64"
$headers = @{ Authorization = $basicAuthValue }
$r = Invoke-WebRequest -uri "http://grrserver:8000/api/clients" -Headers $headers
$r.Content
```

Thanks! Back to you, Rick.