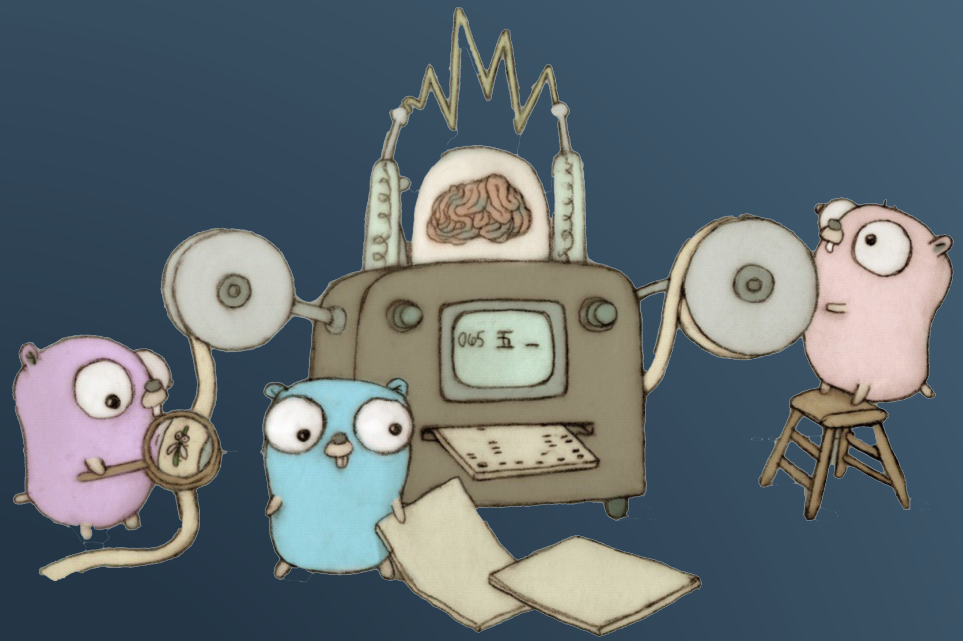
Booz | Allen | Hamilton®



PROJECT GO AHEAD

Building a Kubernetes-based Streaming Detection Platform

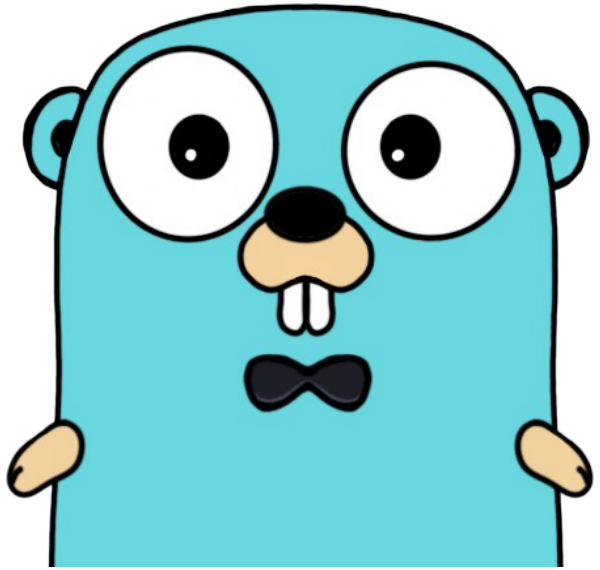
CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

Who We Are

Mike Saxton

Director or Federal Threat Hunt DFIR @ Booz Allen Hamilton

Background in large-scale enterprise Security programs



Jeffrey Wong

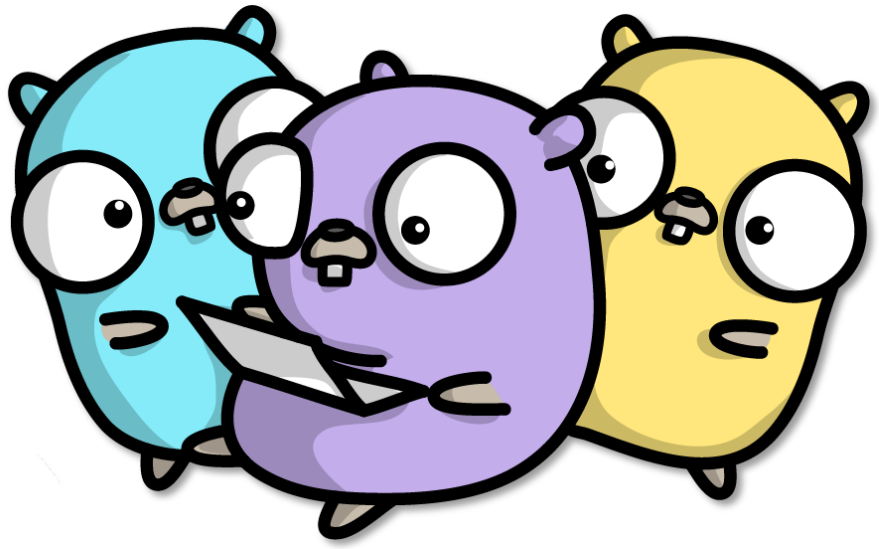
Lead PROJECT GOAHEAD Developer @ Booz Allen Hamilton

Go Guru

PROBLEM

Detection engineering and coverage is incredibly difficult across large organizations due to multi-vendor environments and lack of consistent standards

This results in attack surface differences leading to “weakest link” security and a lack of true awareness across the enterprise



CHALLENGE OVERVIEW

Our background is managing large, dispersed, and semi-autonomous Security environments. We wanted to build a solution that met one of the difficulties in managing our client's biggest detection problems.

We set off with 4 main rules…

1. Must decrease costs and improve detection
2. Detection must happen outside of the SIEM
3. Must enforce interoperability
4. Everything must be automated

HOW WE GOT HERE

Our research led us down a lot of great routes, but nothing fit *just* right. Until…

AirBNB's BinaryAlert was great, but is for YARA rules…

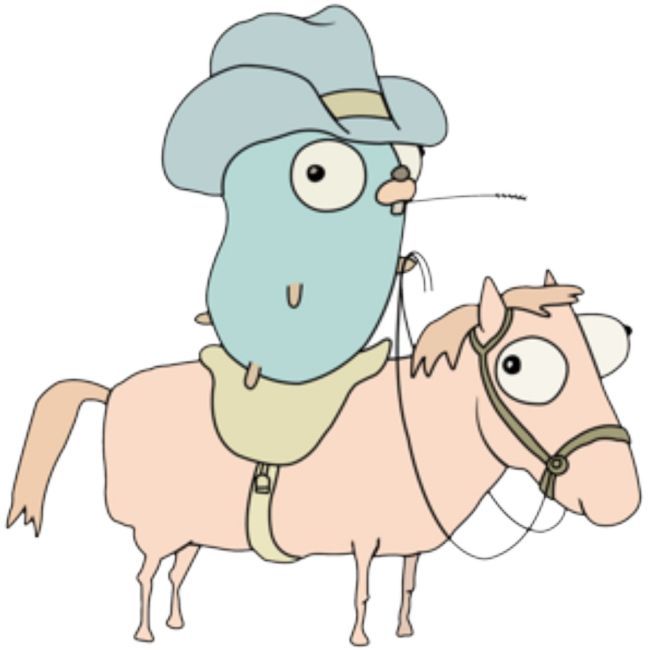
Same with Target's Strelka, but we REALLY liked the dog…

AirBnB's StreamAlert was closer, but is for AWS and written in Python…

Florian's LOKI/THOR got us closer, and we tinkered with it but….

Markus Kont and Mauno Pihelgas of NATO's Cooperative Cyber Defence Centre of Excellence (NCCDOE) were spot on. However, we needed the engine to work in environments with 1 million + systems, and automate signature pulls…

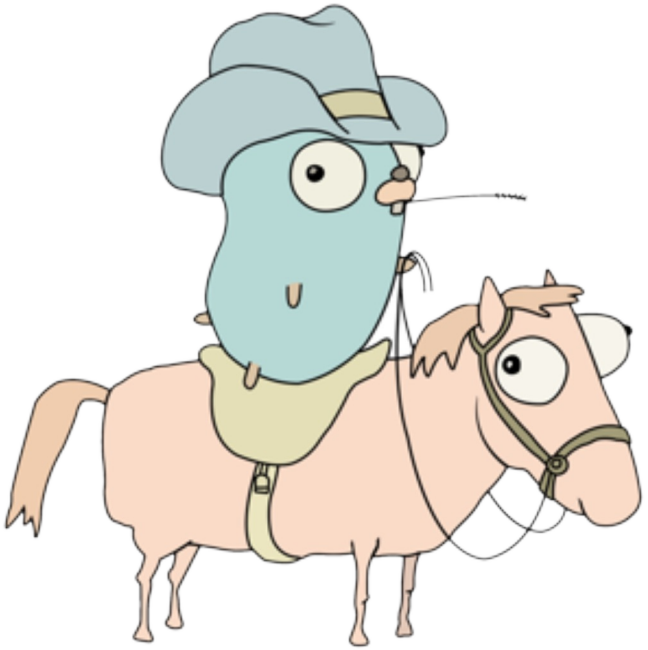
SOLUTION OVERVIEW



PROJECT GO AHEAD, our internal research name, resulted in a standardized method for scaling enterprise detection outside of a SIEM.

Built with Go and Kubernetes and powered by Sigma rules to detect threats in stream and enforce a standardized CI/CD approach to Detection Engineering across SOC, IR, and Hunt operations.

SOLUTION OVERVIEW



Rules are applied by following a "Write once, detect everywhere" methodology

***PROJECT GO AHEAD* can scan 100% of logs, without license constraint, then stores data… wherever**

Kubernetes's Auto-Scaling helps the engine scale to meet any demand, when it needs it

A single signature repo provides instant rule sharing and removes reliance manual IOC sharing

DEMO WALKTHROUGH

Go Ahead automates the entire Detection Engineering processes from development, to testing, to deployment, while providing a standardized approach to multi-organization/agency deployments.

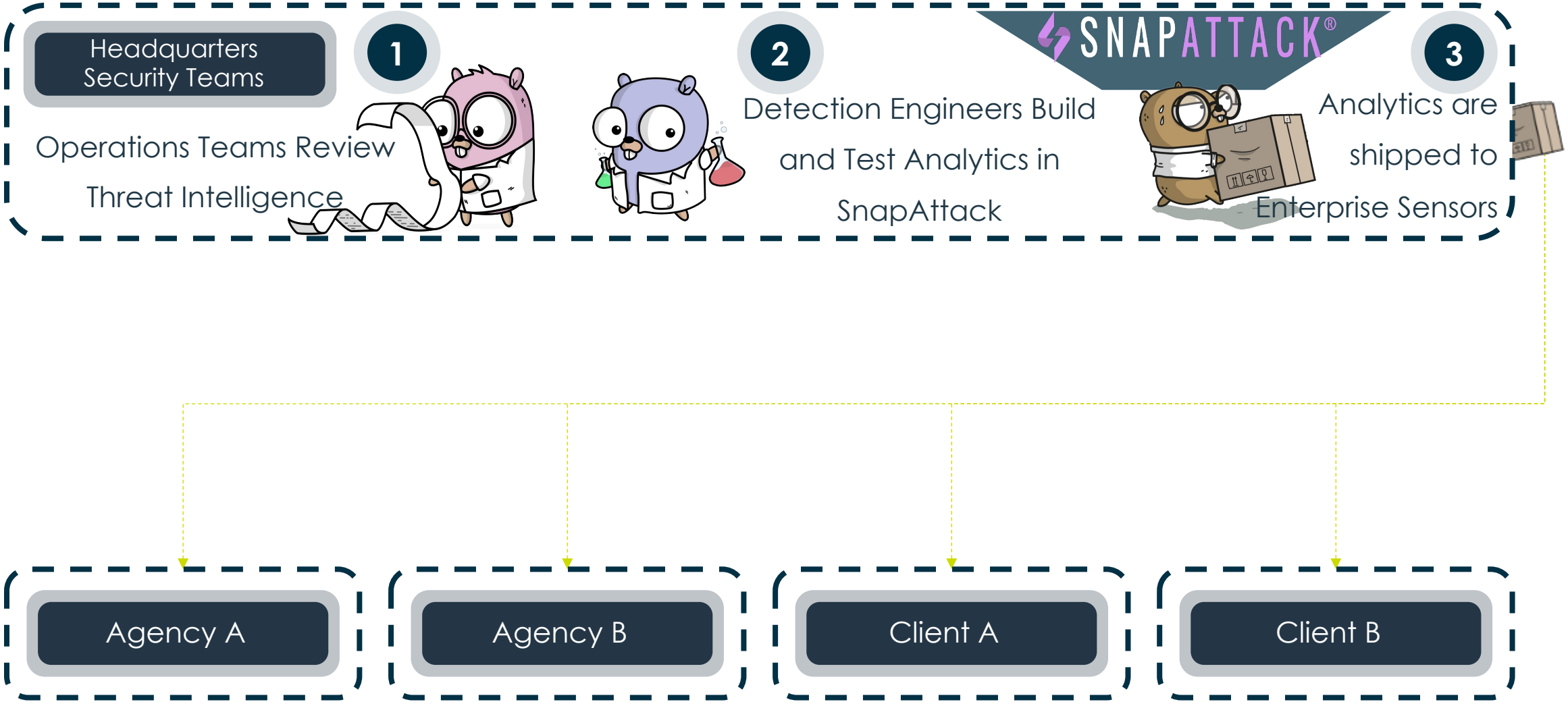
ALERT REVIEW

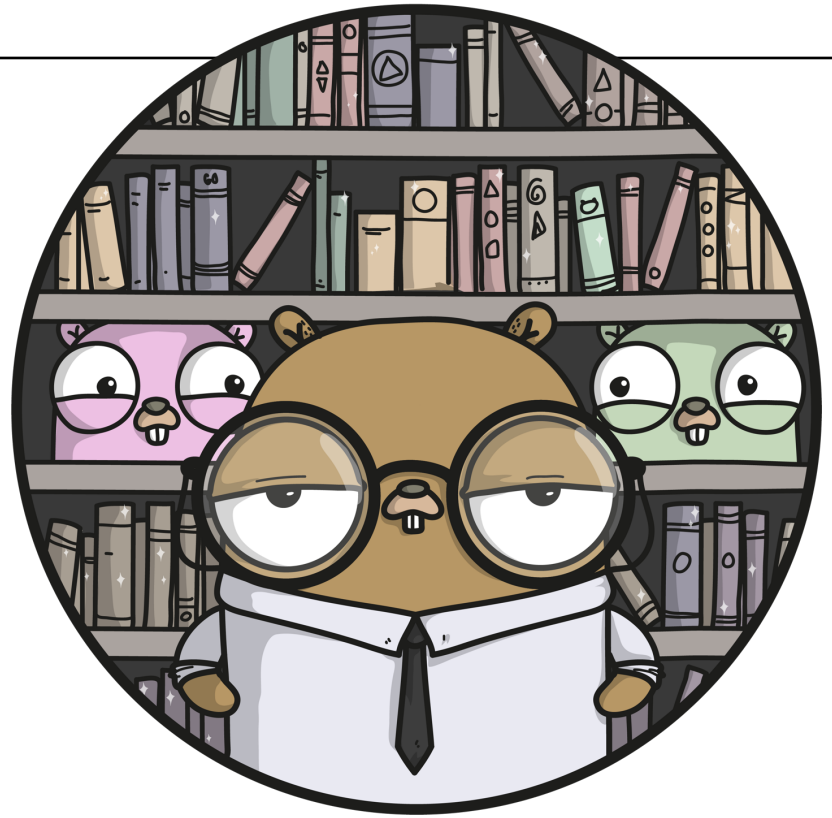

```
{
  "Event": {
    "ActivityID": "",
    "Channel": "Microsoft-Windows-Sysmon/Operational",
    "Computer": "MSEDGEWIN10",
    "DestinationHostname": "MSEDGEWIN10",
    "DestinationIp": "127.0.0.1",
    "DestinationIsIpv6": false,
    "DestinationPort": 5985,
    "EventID": 3,
    "EventRecordID": 196374,
    "Guid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}",
    "Image": "C:\\Users\\IEUser\\Tools\\PrivEsc\\RogueWinRM.exe",
    "Initiated": false,
    "Keywords": "0x8000000000000000",
    "Level": 4,
    "Name": "Microsoft-Windows-Sysmon",
    "Opcode": 0,
    "ProcessGuid": "{747f3d96-ca4b-5ec9-0000-0010b8cb3700}",
    "ProcessID": 2812,
    "ProcessId": 3960,
    "Protocol": "tcp",
    "Qualifiers": "",
    "SourceHostname": "MSEDGEWIN10",
    "SourceIp": "127.0.0.1",
    "SourceIsIpv6": false,
    "SourcePort": 49680,
    "SystemTime": "2020-05-24 01:13:51.206385",
    "Task": 3,
    "ThreadID": 3488,
    "User": "NT AUTHORITY\\LOCAL SERVICE",
    "UserID": "S-1-5-18",
    "UtcTime": "2020-05-24 01:13:50.129",
    "Version": 5
  },
  "Result": [
    {
      "Tags": [
        "attack.execution",
        "attack.t1059.001",
        "attack.t1086",
        "attack.lateral_movement",
        "attack.t1021.006",
        "attack.t1028"
      ],
      "ID": "c539afac-c12a-46ed-b1bd-5a5567c9f045",
      "Title": "Remote PowerShell Session"
    }
  ]
}
```



```
"Result": [
  {
    "Tags": [
      "attack.execution",
      "attack.t1059.001",
      "attack.t1086",
      "attack.lateral_movement",
      "attack.t1021.006",
      "attack.t1028"
    ],
    "ID": "c539afac-c12a-46ed-b1bd-5a5567c9f045",
    "Title": "Remote PowerShell Session"
```

HOW WE'VE DEPLOY IN LARGE AND MANAGED ENVIRONMENTS





Contact Us

Github:

https://github.com/Adversary-Informed-Defense/k8s-go-sigma-streamer

Github Repo –
It's safe, promise ☺

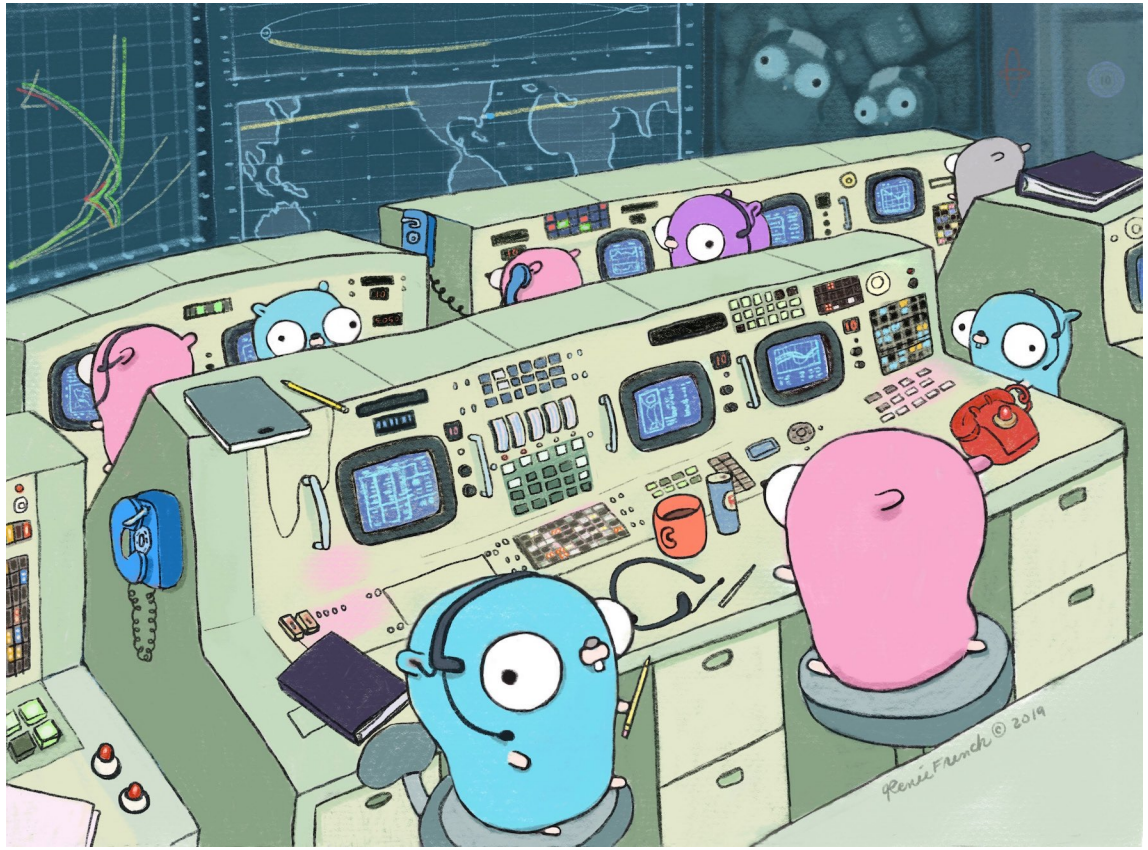
Email:

goahead@bah.com

saxton_micahel@bah.com

Wong_jeffrey2@bah.com

Thank you…



Credits and Acknowledgements for work, code, or logos…

Cover Slide – Gopher image by Renee French, licensed under Creative Commons 3.0 Attributions license.

Slide 2 – Custom Logos from Gopher Konstructor

Slide 3 – Gopher image by Ashley McNamara, licensed under, Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Slide 5 – AirBnb BinaryAlert, AirBnB StreamAlert, THOR Lite, NCCDCOE White Paper, Markus Kont's Go Sigma Engine Code

Slide 6 - Gopher image by Renee French, licensed under Creative Commons 3.0 Attributions license.

Slide 7 - Gopher image by Ashley McNamara, licensed under, Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Slide 8 – #1, 2, 3, 4 Gopher image by Marcus Olsson, , licensed under, Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

#5) Gopher image by Ashley McNamara, licensed under, Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Slide 9 - Gopher image by Ashley McNamara, licensed under, Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Slide 10 - Gopher image by Renee French, licensed under Creative Commons 3.0 Attributions license.