FOCUS ON YOUR MALWARE, NOT INFRASTRUCTURE!

OMRI SEGEV MOYAL
@GelosSnake

WHAT DO SECURITY RESEARCHERS FIND MOST CHALLENGING WHEN CREATING A NEW APPLICATION?

Based on twitter survey - http://bit.ly/2MPAyyY

PRESENTATION AGENDA

01 Modern Research Practices

02 Serverless Introduction & Security Considerations

03 Current Usage & Pioneers

04 Hands-On Example

05 Live Demo

OMRI SEGEV MOYAL

RESEARCHER

Malware, APT, CryptoMiners, OSINT, Exploit Kits…

ENTREPRENEUR

Private Consultant
Co-Founder @ Minerva Labs
Strategic Advisor @ ClearSky Cyber Security

COMMUNITY ADVOCATE

Founder of world's largest and most active Malware Research Group with over 700 members world wide. Join us! https://malware-research.org/slack
Admin, 9723 Defcon Chapter

MHFC ULTRA FAN

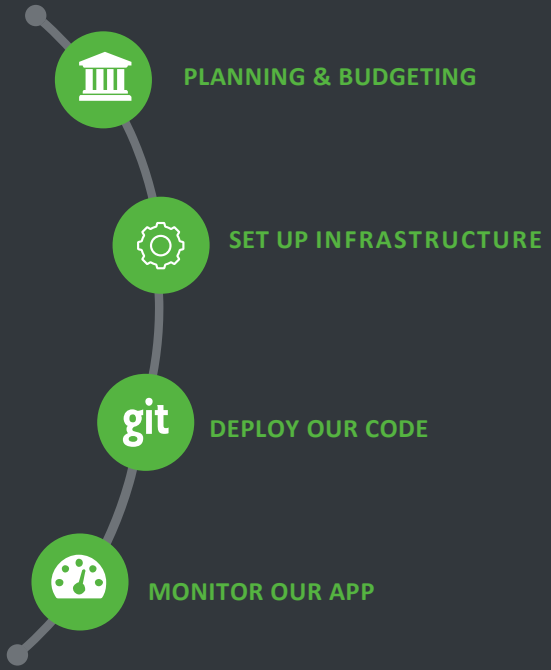
Maccabi Haifa sport club fan.
Born into it, never left.

#OSDFCON #SERVERLESS @GELOSSNAKE

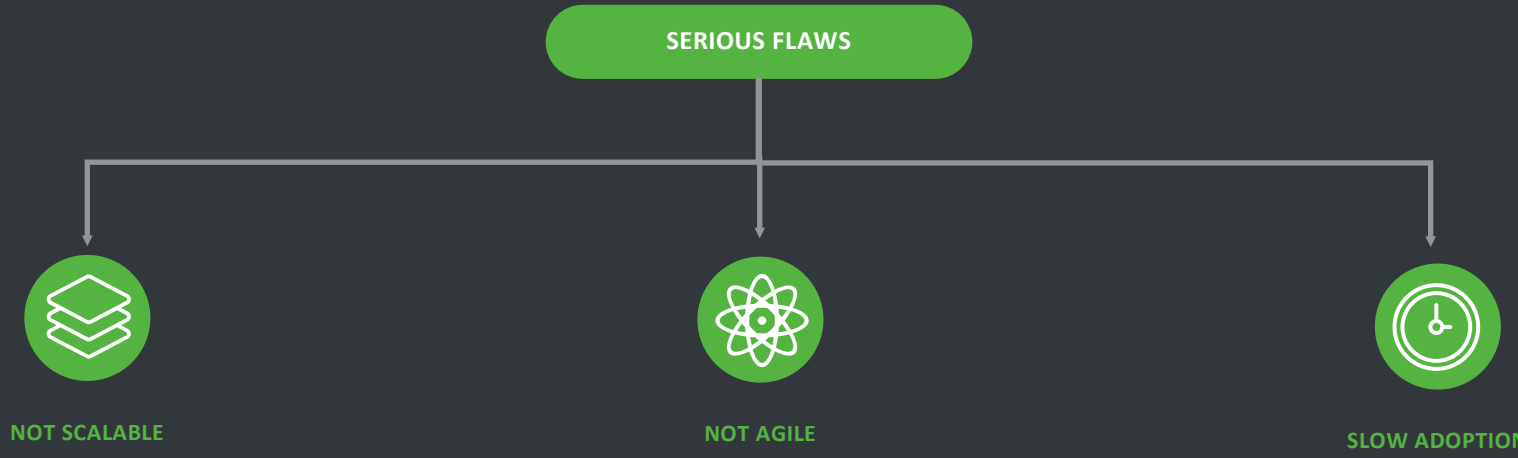
OMRI SEGEV MOYAL
@GelosSnake

SECURITY RESEARCH TODAY

How do we build our research apps today?

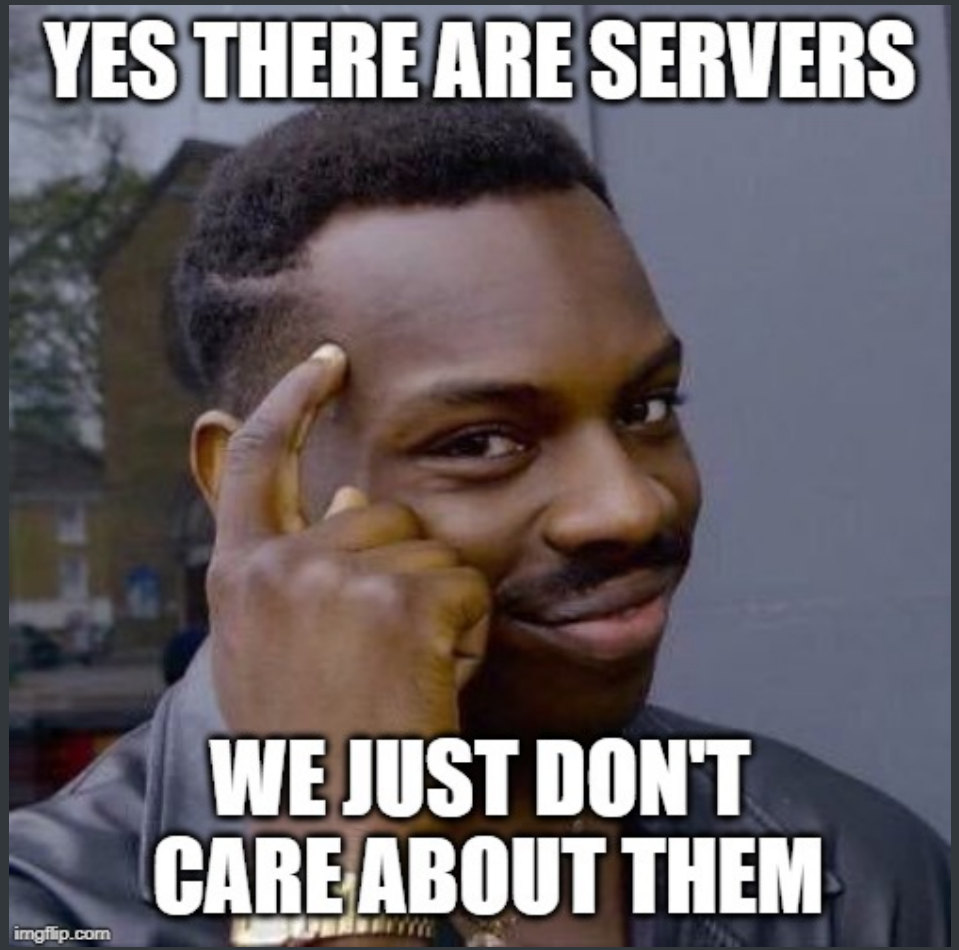


SECURITY RESEARCH TODAY



QUICK INTRODUCTION TO SERVERLESS

- FOCUS ON WRITING CODE
- EVENT DRIVEN
- NEVER PAY FOR IDLE RESOURCES
- SCALABLE


YES THERE ARE SERVERS
WE JUST DON'T CARE ABOUT THEM
imgflip.com

SERVERLESS CONS & LIMITATIONS

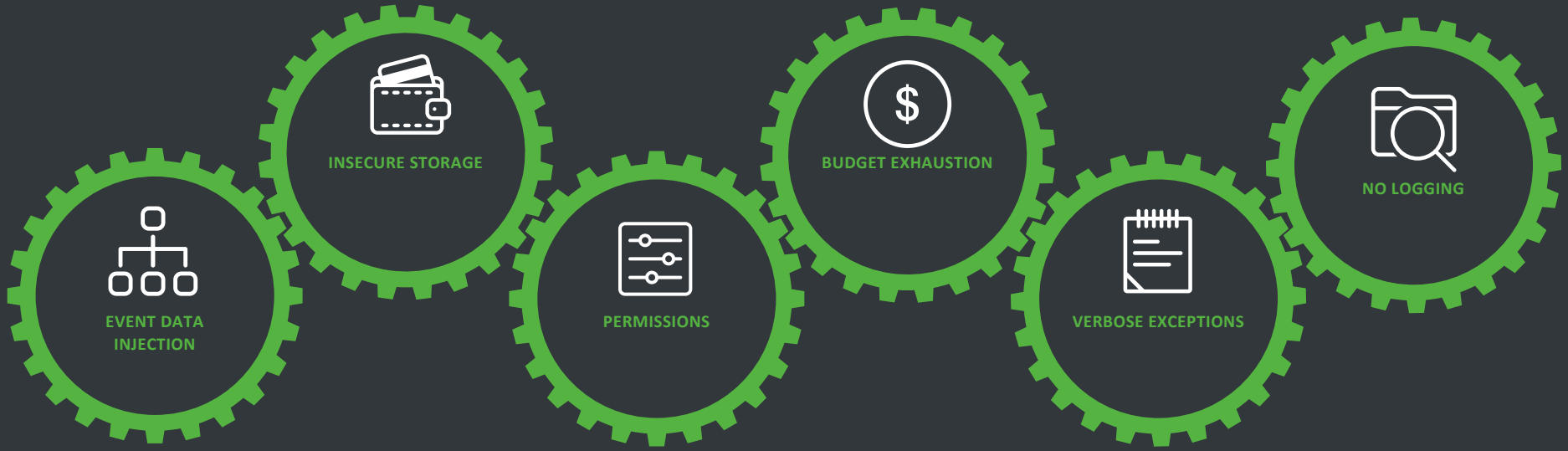
LEARNING CURVE

TECHNICAL LIMITATIONS

TOUGH TO DEBUG

WARM AND COLD BOOTS

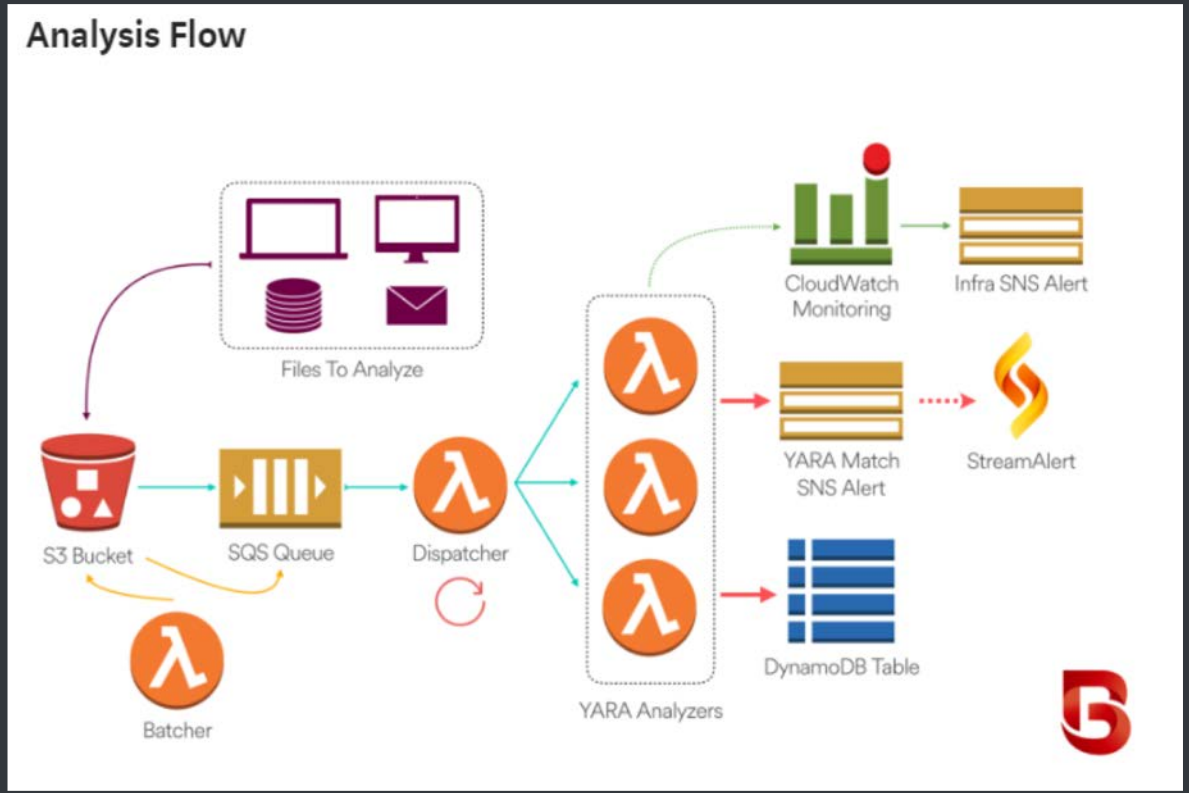
COMMON SECURITY PROBLEMS



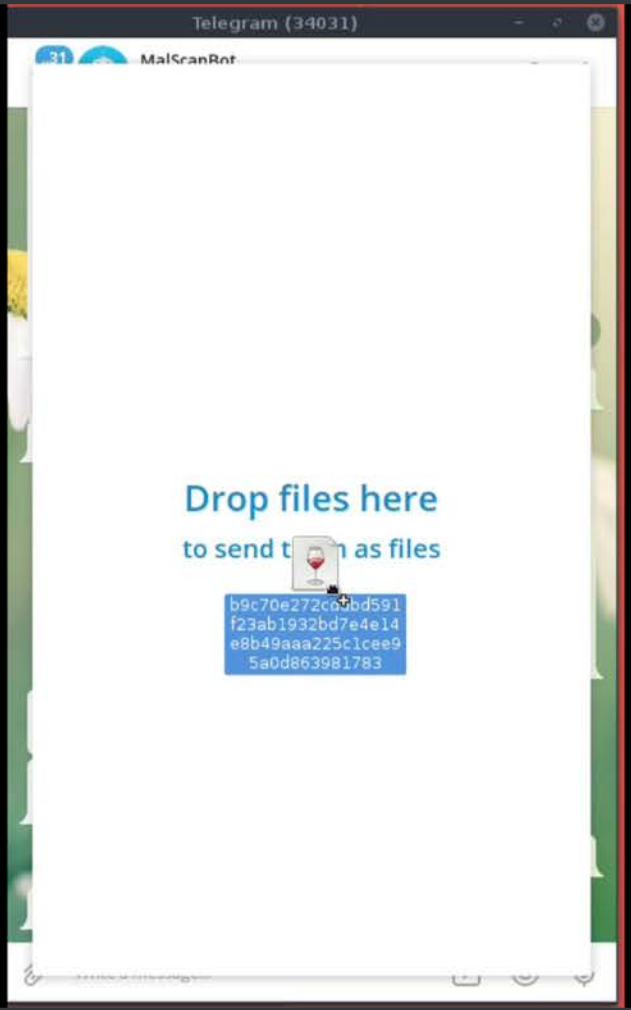
“A VERY INTERESTING QUOTE FROM THE ART OF WAR.”

Omri Segev Moyal, who could not find any Sun Tzu related quote.

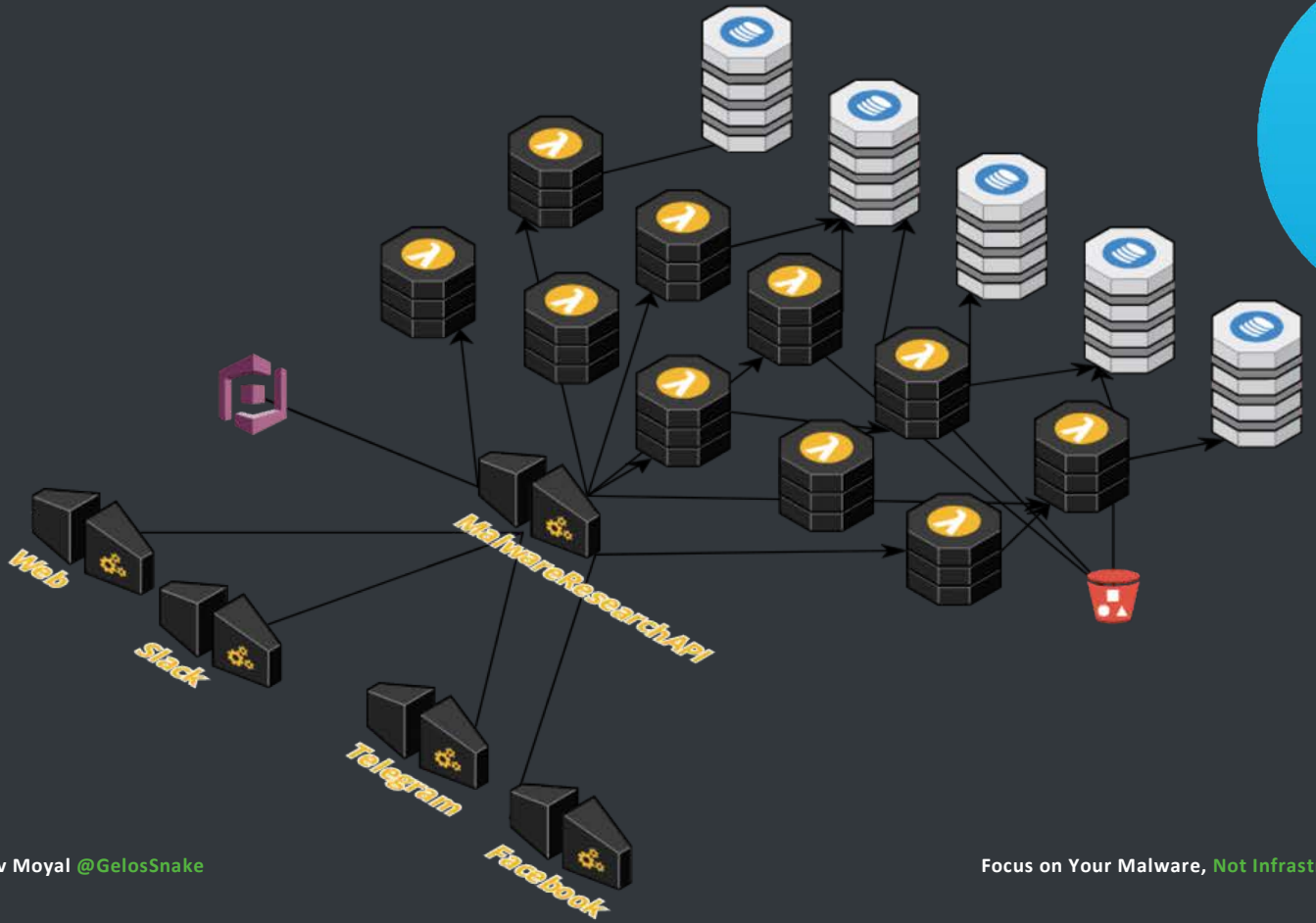
AIRBNB BINARY ALERT



http://www.binaryalert.io/

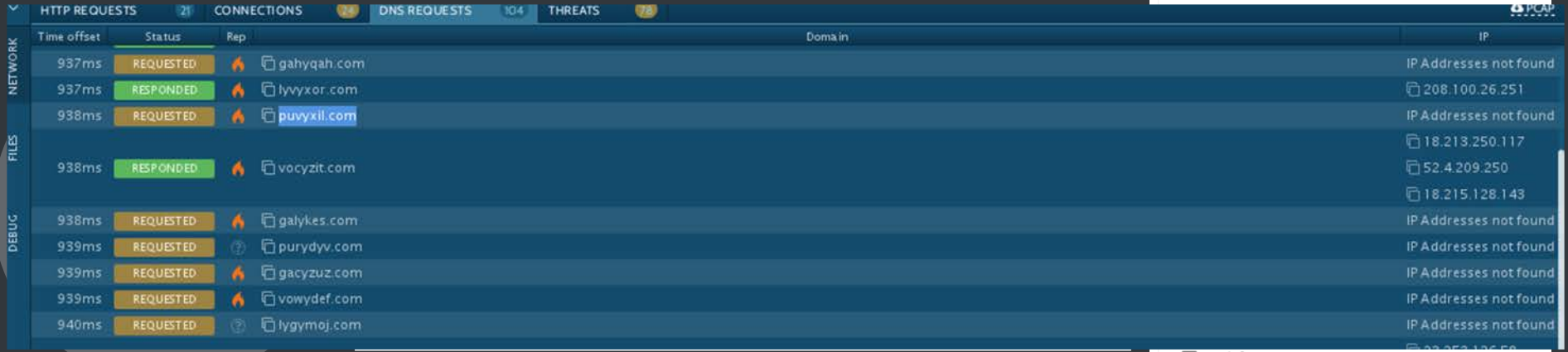

Telegram (34031)
MalScanBot
Drop files here
to send t n as files
b9c70e272c0bbd591
f23ab1932bd7e4e14
e8b49aaa225c1cee9
5a0d863981783

MALSCANBOT SERVERLESS BACKEND

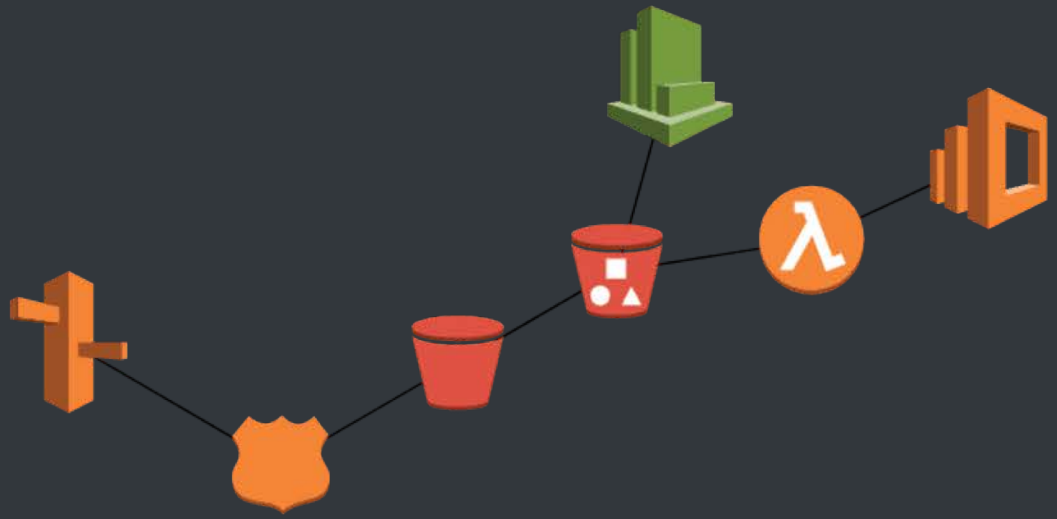


PRACTICAL EXAMPLE – BUILDING A SERVERLESS SINKHOLE

FINDING “SINKABLE” MALWARE



BUILDING A SERVERLESS SINKHOLE



MONITORING RESULTS

DEMO TIME

PRESENTATION RECAP

01 Modern Research Practices

02 Serverless Introduction & Security Considerations

03 Current Usage & Pioneers

04 Hands-On Example

05 Live Demo

OMRI SEGEV MOYAL

@GELOSSNAKE

GELOSSNAKE

THANK YOU

OMRIMOYAL

OMRI@PROFERO.IO