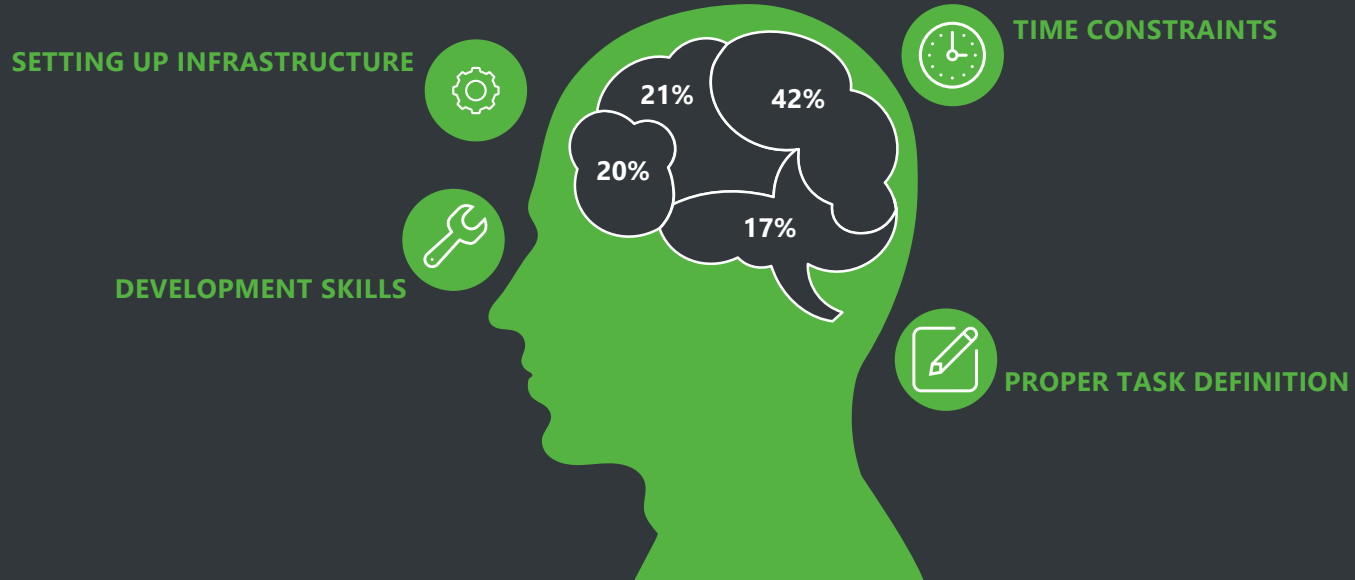

FOCUS ON YOUR
MALWARE, **NOT**
INFRASTRUCTURE!

OMRI SEGEV MOYAL

@GelosSnake

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



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

Omri Segev Moyal @GelosSnake

Focus on Your Malware, **Not Infrastructure!**

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.

Co-founded Malware-Media group to shorten
media and research gaps.

Admin, 9723 Defcon Chapter



MHFC ULTRA FAN

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



SECURITY RESEARCH TODAY

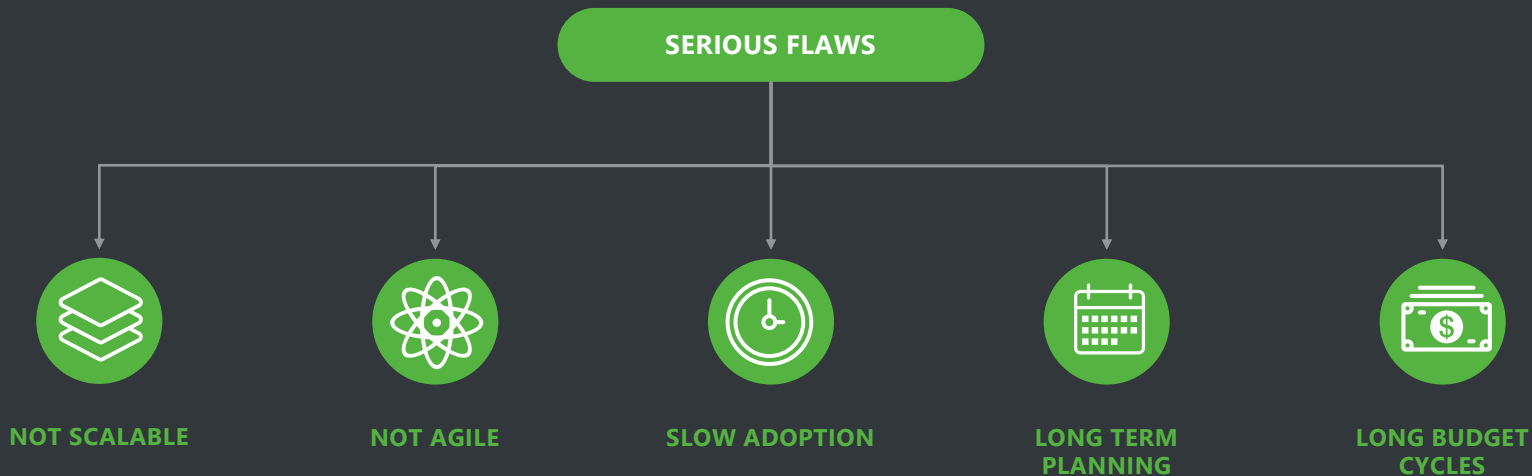
How do we build our research apps today?



MODERN SECURITY RESEARCH TOOLS



SECURITY RESEARCH TODAY



QUICK INTRODUCTION TO SERVERLESS



FOCUS ON WRITING CODE



EVENT DRIVEN

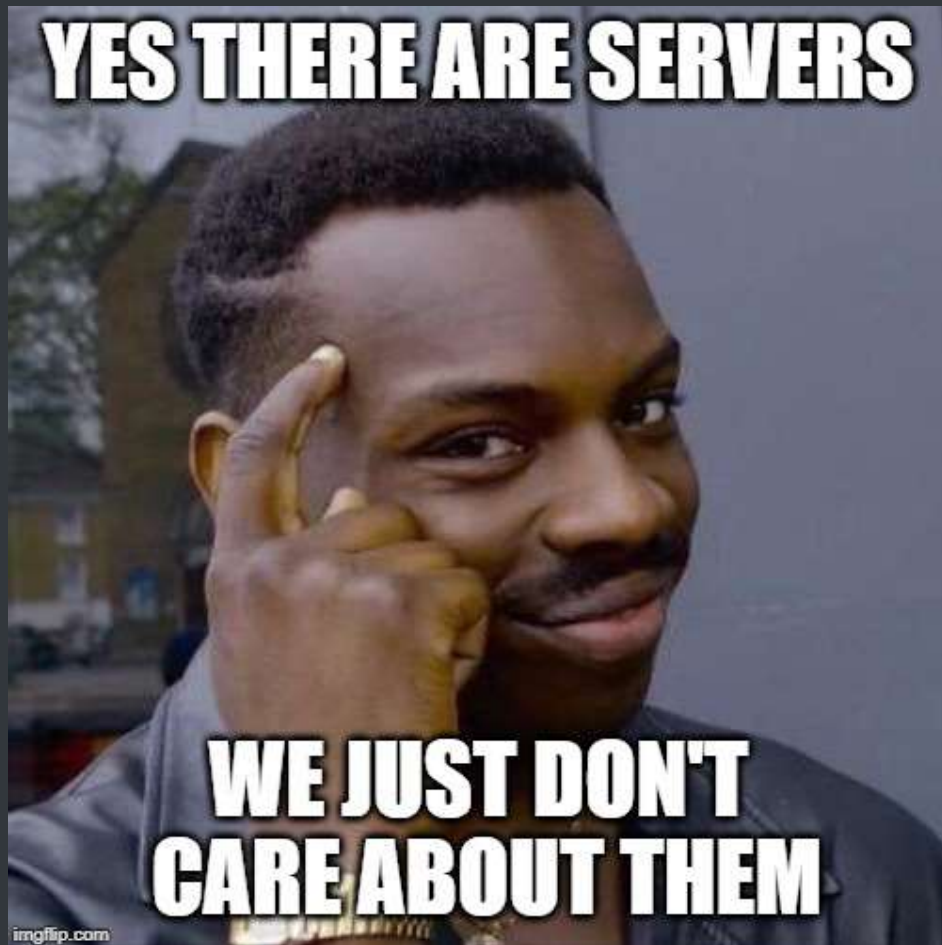


NEVER PAY FOR IDLE
RESOURCES



SCALABLE





SERVERLESS CONS & LIMITATIONS



LEARNING CURVE



WARM AND COLD BOOTS



TOUGH TO DEBUG

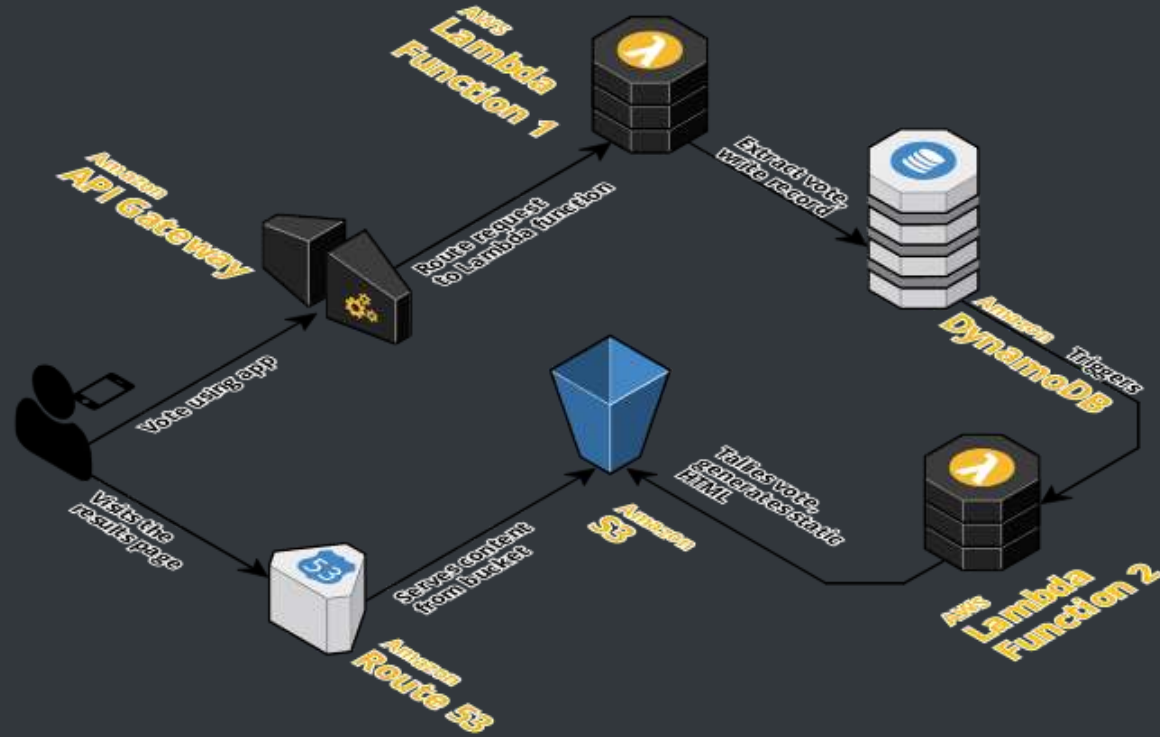


INFRASTRUCTURE OWNED BY SERVICE PROVIDER



TECHNICAL LIMITATIONS

| SIMPLE SERVERLESS VOTING APP



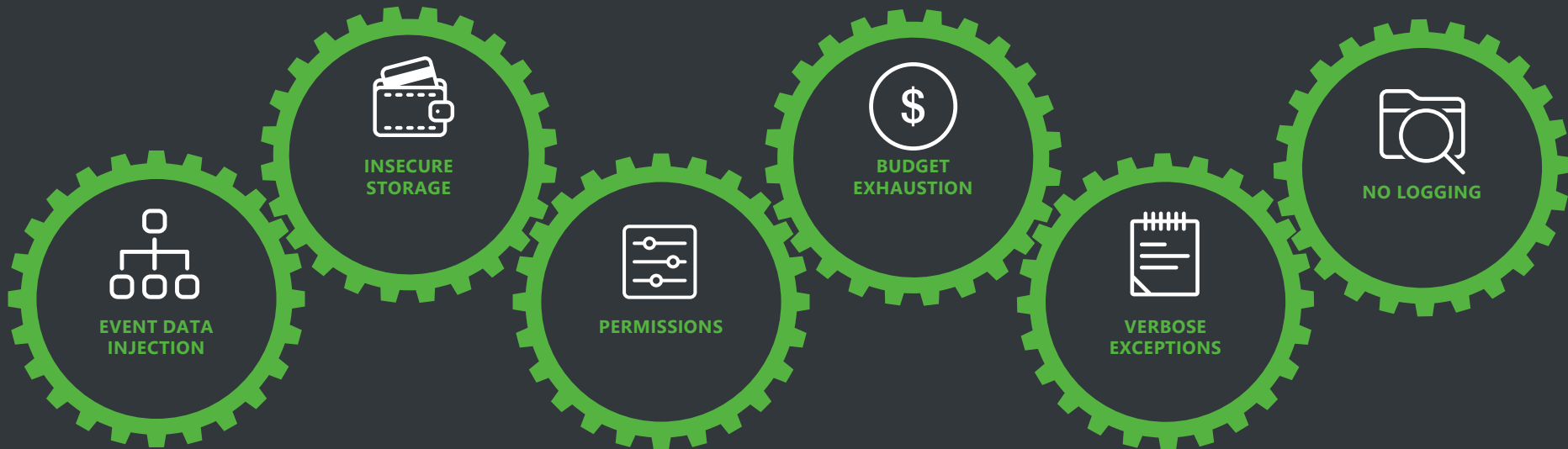
Created via <https://cloudcraft.co>

Omri Segev Moyal @GelosSnake

Focus on Your Malware, Not Infrastructure!



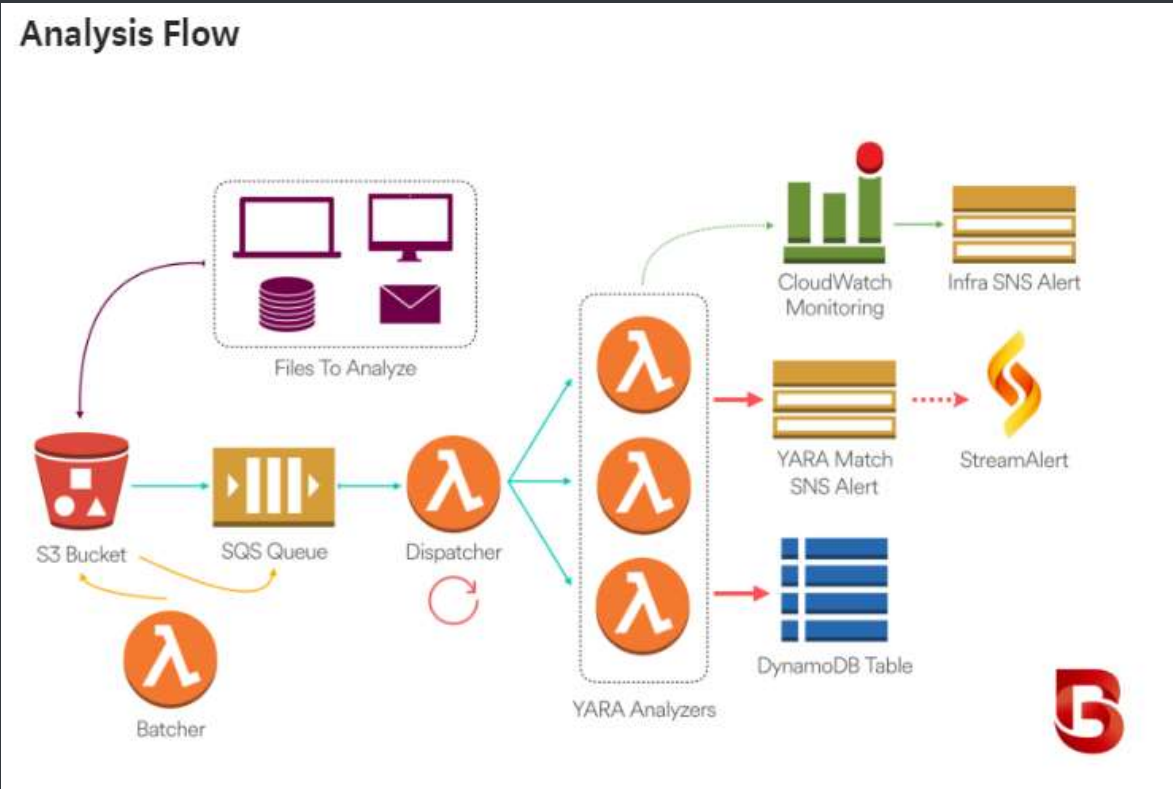
COMMON SECURITY PROBLEMS



"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/>

Omri Segev Moyal @GelosSnake

Focus on Your Malware, Not Infrastructure!

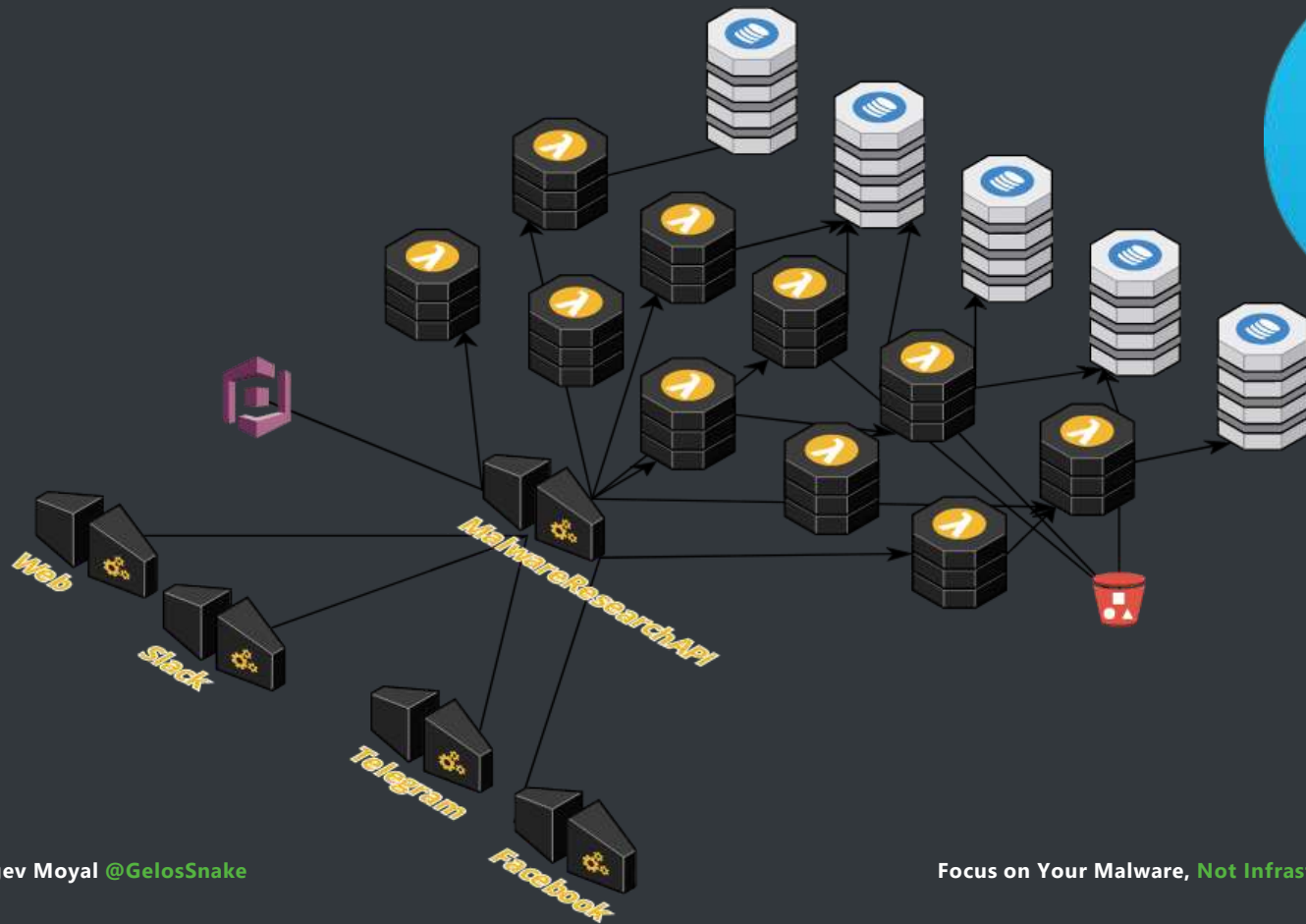


Drop files here
to send them as files



```
b9c70e272c65bd591  
f23ab1932bd7e4e14  
e1b49aaa225c1cee9  
5a0d8c39a1783
```


MALSCANBOT SERVERLESS BACKEND



PRACTICAL EXAMPLE – BUILDING A SERVERLESS SINKHOLE



FINDING "SINKABLE" MALWARE

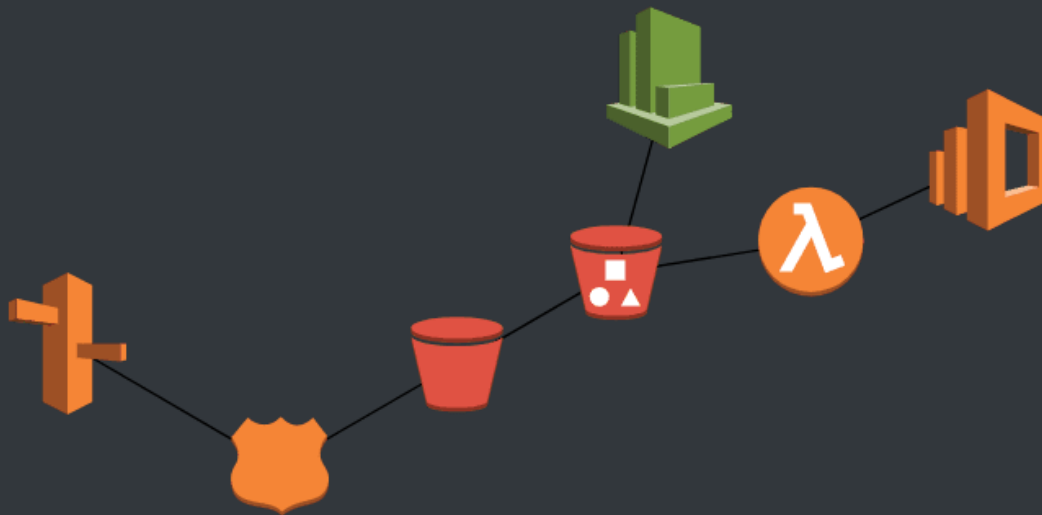
The screenshot displays a network analysis tool interface with a sidebar on the left containing 'NETWORK', 'FILES', and 'DEBUG' sections. The main window is titled 'DNS REQUESTS' and shows a list of DNS requests. The columns are 'Time offset', 'Status', 'Rep', 'Domain', and 'IP'. The 'Status' column contains labels like '#REQUESTED' (orange) and '#RESOLVED' (green). The 'Rep' column contains a flame icon. The 'Domain' column lists various domains, and the 'IP' column shows either 'IP Addresses not found' or specific IP addresses.

Time offset	Status	Rep	Domain	IP
937ms	#REQUESTED	🔥	gahyqah.com	IP Addresses not found
937ms	#RESOLVED	🔥	lyvyxor.com	208.100.26.251
938ms	#REQUESTED	🔥	puvyxil.com	IP Addresses not found
938ms	#RESOLVED	🔥	vecydl.com	18.213.250.117 52.4.209.250 18.215.128.143
938ms	#REQUESTED	🔥	gmyles.com	IP Addresses not found
938ms	#REQUESTED	🔥	purdydy.com	IP Addresses not found
939ms	#REQUESTED	🔥	gacyzuz.com	IP Addresses not found
939ms	#REQUESTED	🔥	vowdyef.com	IP Addresses not found
940ms	#REQUESTED	🔥	lygymoj.com	IP Addresses not found

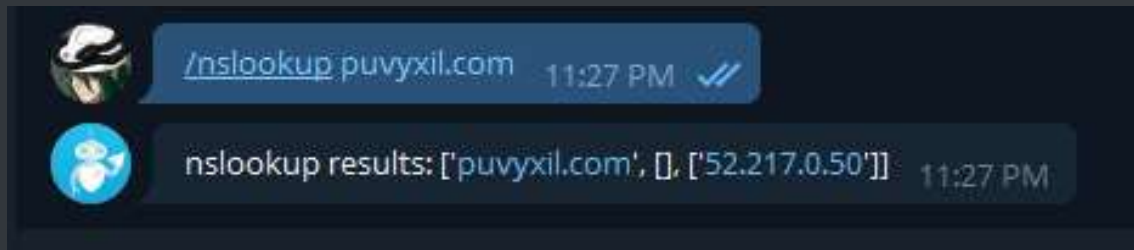
Below the main table, a 'DNS Resolutions' window is open, showing details for two domains:

- getyfluv.com**: 104.239.157.210
- puvyxil.com**: No resolutions recorded

BUILDING A SERVERLESS SINKHOLE



MONITORING RESULTS



```
f6db3748ffe482d91860ac6d6626f4b014aa8b253eb6b889466c808e8d42807f puvyxil.com [04/Jun/2019:21:47:00 +0000] 65.154.226.109 - 9105123F58C08FE0
WEBSITE.GET.OBJECT login.php "GET /login.php HTTP/1.1" 200 - 108 108 16 16 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)" -
qEREcvVxy5bL9ERsMB80T1wcl/yPusdAen6y9yg6C2+XjaX56JSRvc1qszl1XEvYMGgNok9LRg= - - - puvyxil.com -
```

SHOWING OFF



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