

# GHOST IDENTITIES / NHIs

## 68% — SERVICE ACCOUNTS



```
token=ey...  
MongoDB / CVE  
API: *****
```

شنو هادا؟ 68%  
ديال الهجمات بسبب  
!service accounts

Ghost Identities  
خدامين!





45 identities per user

45 identities per user

**BOOM**

**SHING**

كاین  
Lateral Movement!

MongoDB access  
CVE-XXXX

MongoDB access  
CVE-XXXX

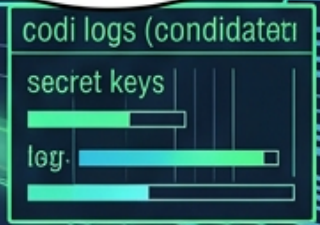
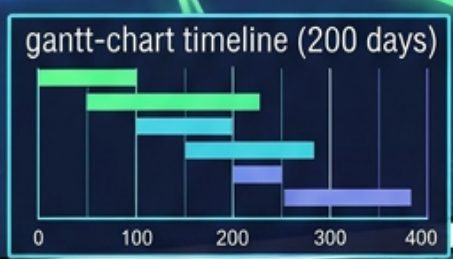
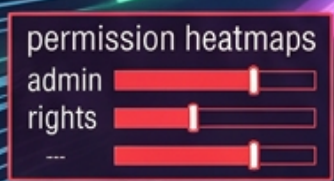
MAS

سمايقي الخوفارت  
و MongoDB CVE  
باينين هنا هنا.

غادي ندير  
full scan للخوادم  
secretلا



CVE و CVE  
MongoDB logs  
باينين هنا



```
Token inspector  
context: rotaten inspector {  
  returns {  
    coder: koy: "GGK",  
    return {  
      "key": "302925527633",  
      "preivate key": "92",  
      ooar: 294  
    };  
    rotation: keys 1  
  }  
}
```



```
API logs  
suot: tnes: {  
  "oes {  
    "seorier": 2,  
    "secet_key": "813a6993280e1996605e07903";  
  }  
}  
API logs: {  
  "arte_16": "6onTRadh49R06290cS20",  
  "aoc_0": "0220008700225a7587";  
};
```



# PLAYBOOK DEPLOYED

Discovery ✓

Right-Sizing ✓

Rotate Secrets ✓

Auto-Delete Dead Identities ✓

KABOOM!

منصّب Playbook!  
ندور keys ونمسح  
الهويات الشبحية

200 يوم؟ -  
دأبا بقاو 0 يوم!

200 >>> 0

CLICK

Policy rules automatically  
delete stale identities too to  
a, single permitted  
account. OK

Logs ROTATION SUCCESS  
Logs ROTATION SUCCESS  
Logs ROTATION SUCCESS

SHK

SHCK