PRACTICAL – 3

Adversary Emulation – APT29 Simulation

Objective

Simulate real attacker behaviors using MITRE ATT&CK knowledge to evaluate detection capability.

Tools Used

MITRE Caldera, Evilginx2, Wazuh SIEM

Procedure

1 Created **phishing landing page** using Evilginx2
2 Captured authentication tokens & credentials
3 Used Caldera Agent to deploy persistence (Scheduled Task)
4 Observed defender alerts in Wazuh dashboard

Attack Log

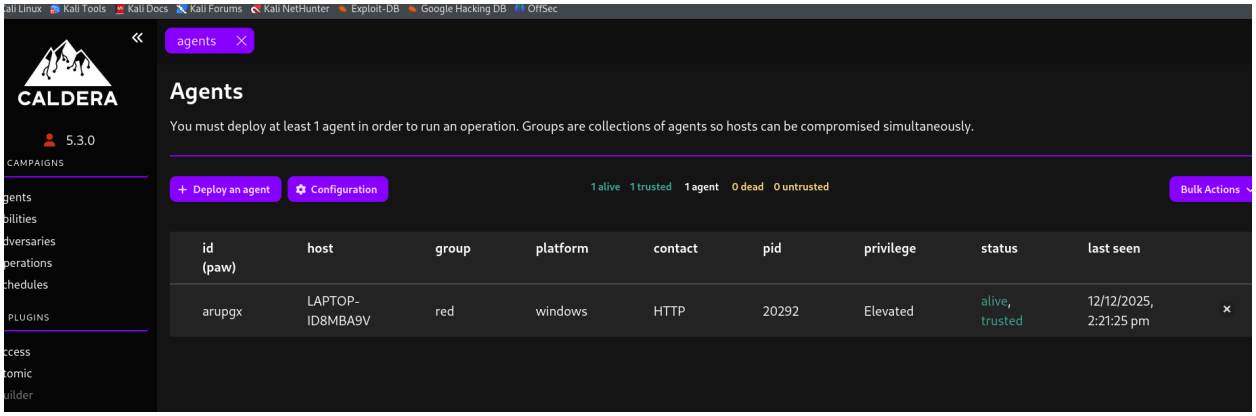
Phase	Technique	Tool	Impact
Initial Access	T1566.001 (Phishing)	Evilginx2	Credential Theft
Persistence	T1053 (Scheduled Task)	Caldera	Long-term Access

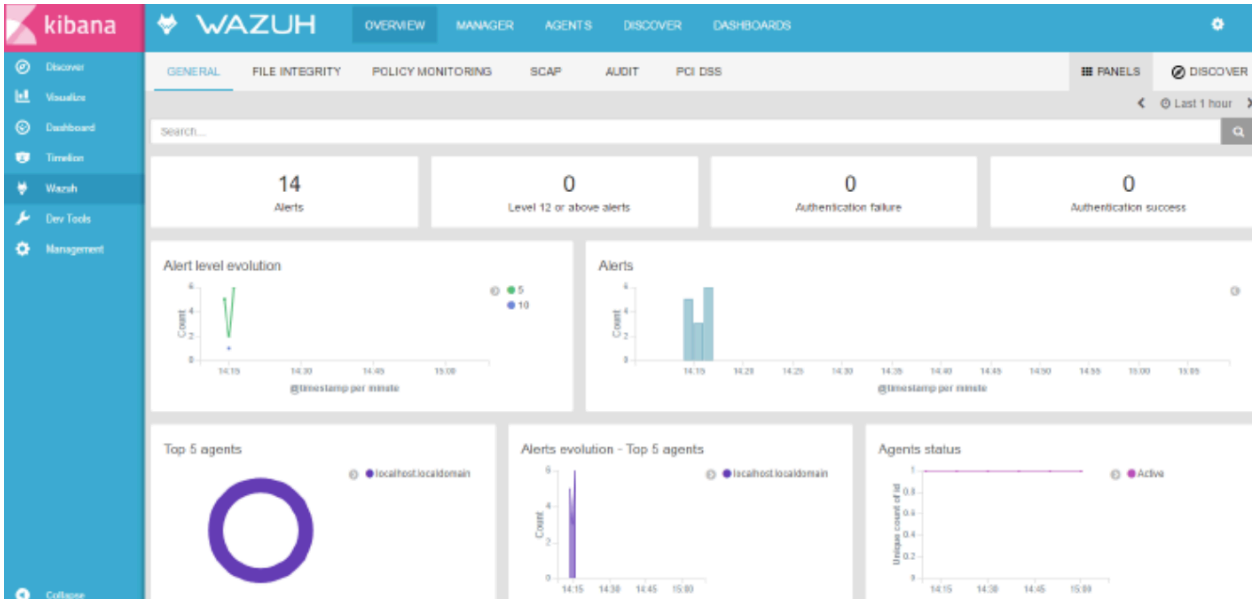
Detection Log

SOC alerted during persistence phase but **missed phishing attempt**.

Summary (50 Words)

This simulation validated SOC effectiveness against real APT techniques. Early access bypassed detection, proving need for stronger email security & user training.


Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
CALDERA
5.3.0
CAMPAIGNS
PLUGINS
agents
Agents
You must deploy at least 1 agent in order to run an operation. Groups are collections of agents so hosts can be compromised simultaneously.
Deploy an agent
Configuration
1 alive 1 trusted 1 agent 0 dead 0 untrusted
Bulk Actions
id (paw)
host
group
platform
contact
pid
privilege
status
last seen
arupgx
LAPTOP-ID8MBA9V
red
windows
HTTP
20292
Elevated
alive, trusted
12/12/2025, 2:21:25 pm


kibana
WAZUH
OVERVIEW
MANAGER
AGENTS
DISCOVER
DASHBOARDS
GENERAL
FILE INTEGRITY
POLICY MONITORING
SCAP
AUDIT
PCI DSS
PANELS
DISCOVER
Last 1 hour
Search...
14
Alerts
0
Level 12 or above alerts
0
Authentication failure
0
Authentication success
Alert level evolution
Alerts
Top 5 agents
Alerts evolution - Top 5 agents
Agents status
Active