THE OPENCANARY EXPERIENCE

LEE MÖSSNER

NOVEMBER 2023

INTRODUCTION

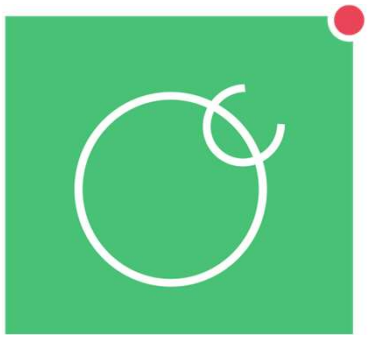
LEE MÖSSNER

HONEYPOT

THINKST CANARY

BUDGET!

$7500, NO APPROVAL



FREE & OPEN SOURCE

Oracle Cloud

Free Tier

Google Cloud Platform

Free(-ish) Tier

Hyper-V Server 2019

Free from Microsoft

Splunk Server

500Mb per day limit

Ubuntu 22.04 Server

Free from Canonical

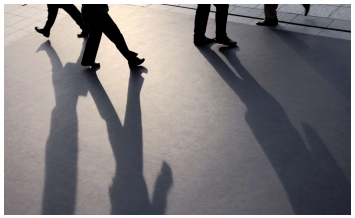
OpenCanary

Thinkst on Github

DEPLOYMENT MODELS

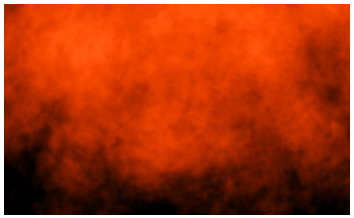
PERIMETER

- Provides Threat Intel and Indications of Compromise
- Is Distraction to Attackers
- Early Warning System



INTERNAL

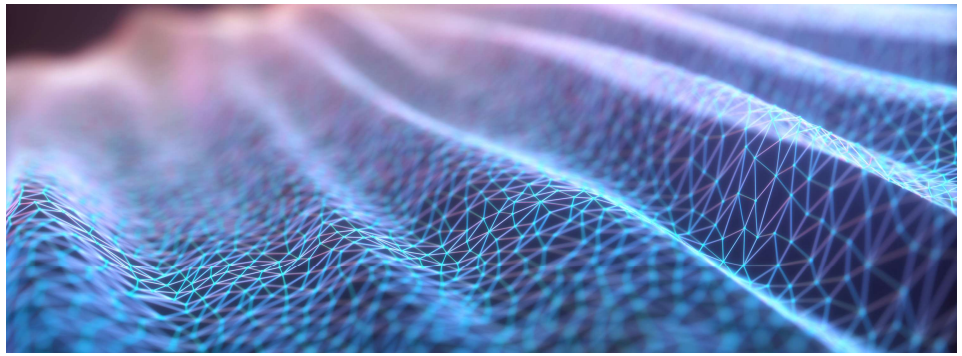
- Silence Expected….
- Insider Threat Warning
- Linked to Incident Process



RESEARCH

- Provides Threat Intel
- Shares Attacker Mindset
- May Fill Your Splunk

BUILD, DEPLOY, WAIT (NOT LONG)

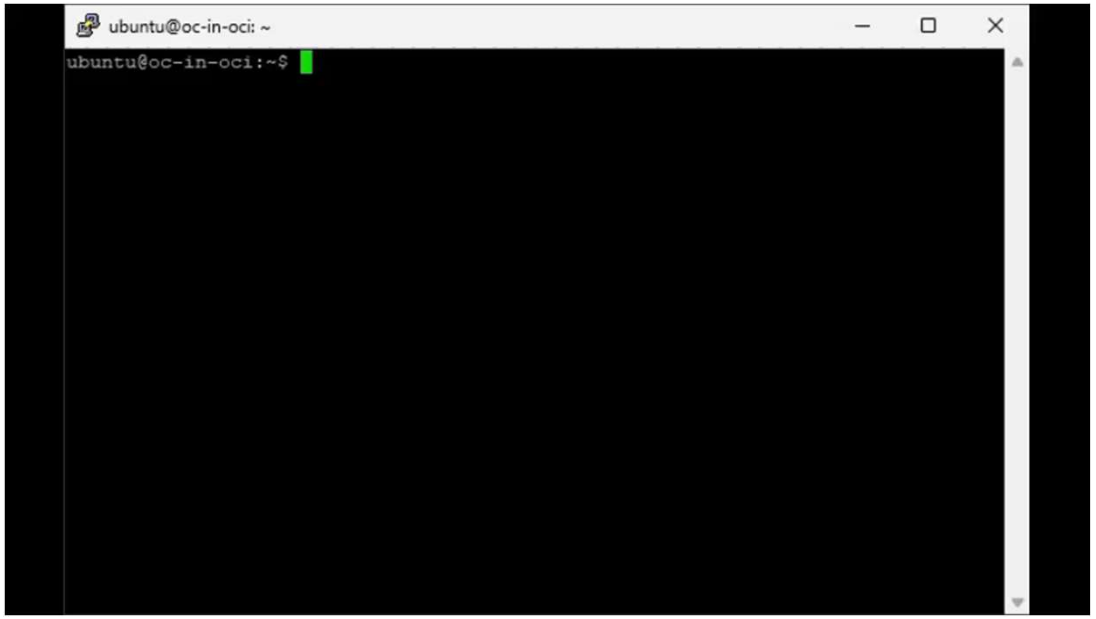


Build and Deploy your Host(s)

- Internet connection, firewall rule
- Python environment
- OpenCanary

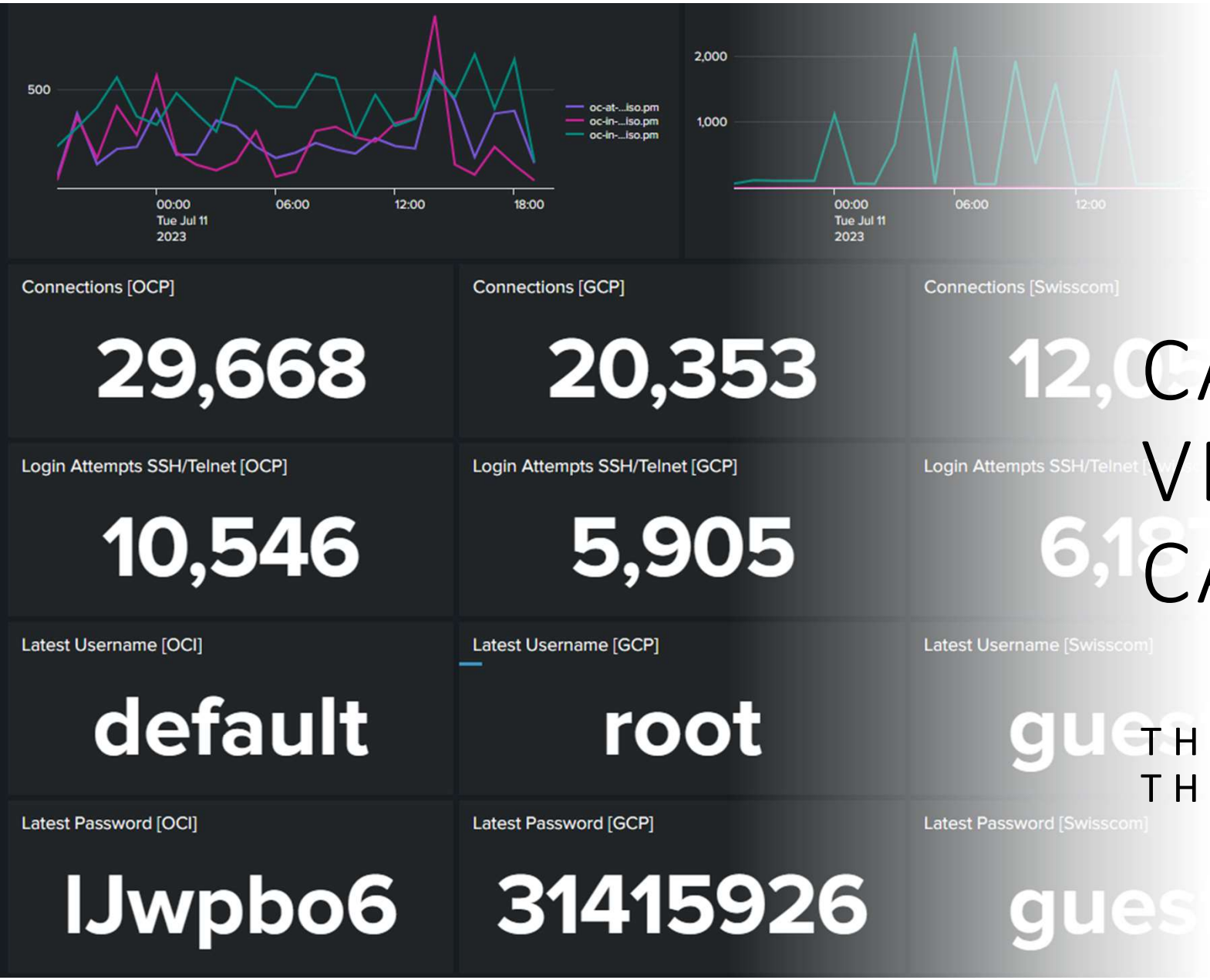
(Instructions are available)

Start your Engines



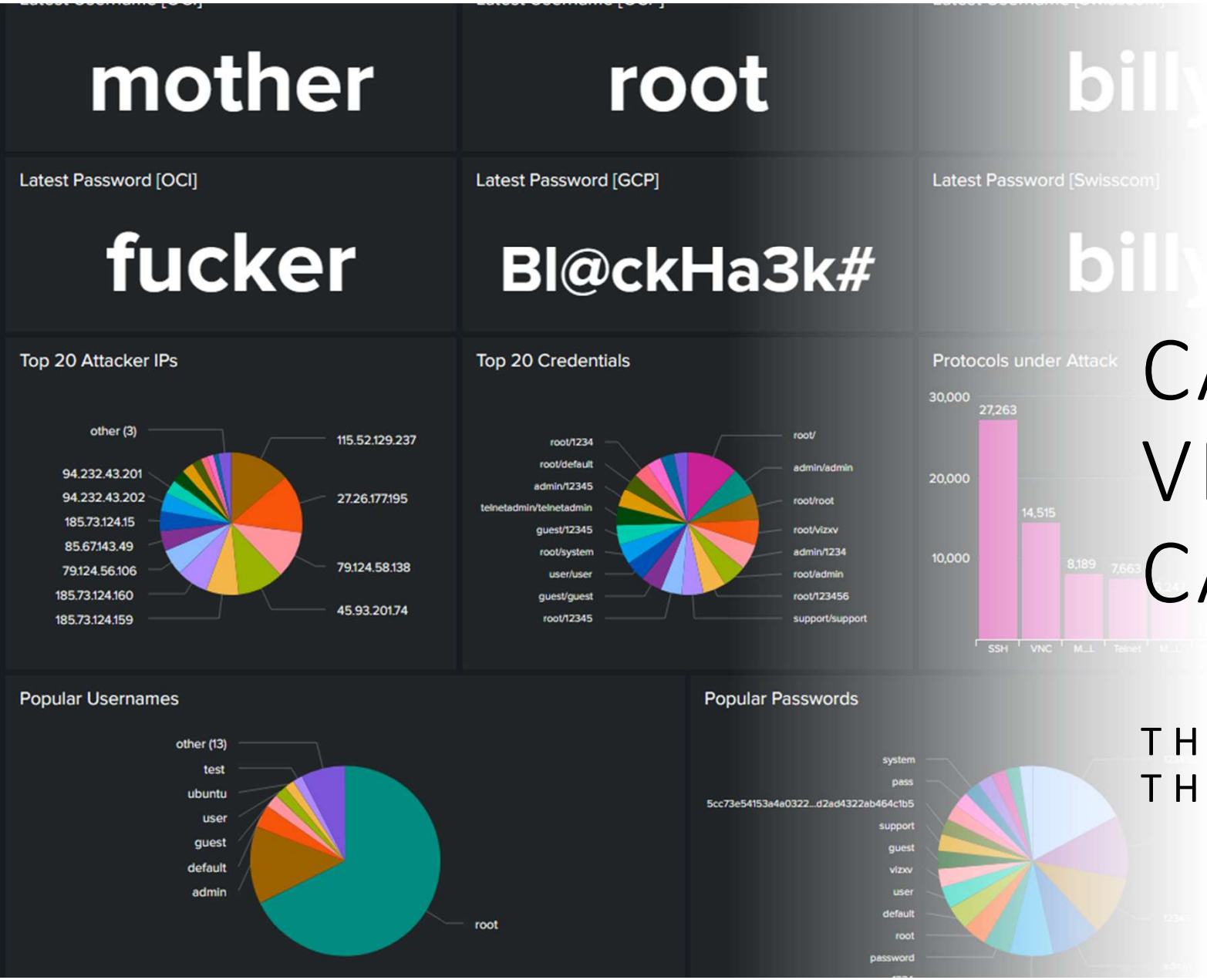
SPLUNK DASHBOARDS

WITH DEMO



CANARY VERSUS CANARY

THE RACE TO THE BOTTOM



CANARY VERSUS CANARY

THE RACE TO THE BOTTOM

DASHBOARD DEMO

THE OBVIOUS

CONNECTIONS

Around 4 million connection attempts across 3 instances/month

CREDENTIALS

Around 3.2 million credentials across VNC, SSH and Telnet

Typically **default credentials** being exploited

PROTOCOLS & POINT

The focus is on **stealing data** from insecure systems (MySQL, MSSQL and REDIS) or to obtain a **persistent foothold** on a host (SSH, Telnet and VNC)

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

TLP:CLEAR

1. Default configurations of software and applications

Default configurations of systems, services, and applications can permit unauthorized access or other malicious activity. Common default configurations include:

- Default credentials
- Default service permissions and configurations settings

Default credentials

Many software manufacturers release commercial off-the-shelf (COTS) network devices —which provide user access via applications or web portals—containing predefined default credentials for their built-in administrative accounts.[9] Malicious actors and assessment teams regularly abuse default credentials by:

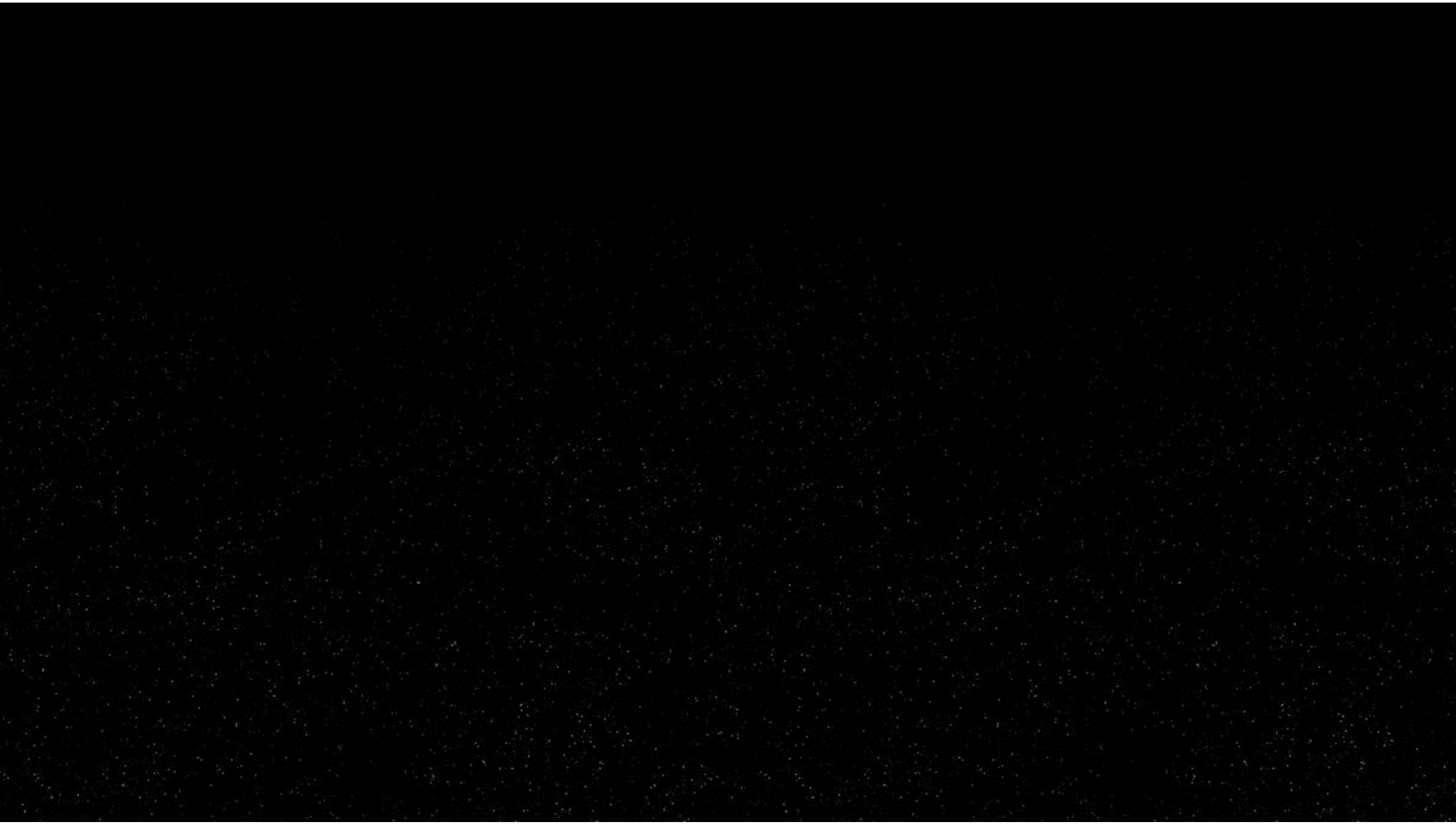
- Finding credentials with a simple web search [T1589.001] and using them [T1078.001] to gain authenticated access to a device.
- Resetting built-in administrative accounts [T1098] via predictable forgotten passwords questions.
- Leveraging default virtual private network (VPN) credentials for internal network access [T1133].
- Leveraging publicly available setup information to identify built-in administrative credentials for web applications and gaining access to the application and its underlying database.
- Leveraging default credentials on software deployment tools [T1072] for code execution and lateral movement.

THE OBVIOUS

In October 2023, the NSA and CISA issued their “Top Ten” security misconfigurations.

The Number One finding is...

Source: NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations



THE NOT-SO-OBVIOUS

MALWARE DROPS

You host their malware. VirusTotal has an API for that...

RANSOMWARE

All your data has been backup and remove 😆

```
ubuntu@oc-in-oci:~/samba$ ls -l
total 228
-rwxr--r-- 1 ubuntu ubuntu 56320 Jul 13 00:12 EHnEPCWZ.exe
-rwxr--r-- 1 ubuntu ubuntu     0 Aug 23 21:23 NCGfmePg.exe
-rwxr--r-- 1 ubuntu ubuntu     0 Jul 17 11:44 QByoCaxW.exe
-rwxr--r-- 1 ubuntu ubuntu   301 Jul 10 15:33 README_FOR_RESTORE_FILES.txt
-rwxr--r-- 1 ubuntu ubuntu     0 Jul 17 14:07 gDvFtzgx.exe
-rwxr--r-- 1 ubuntu ubuntu 56320 Jul 13 00:14 iyyJvWvg.exe
-rwxr--r-- 1 ubuntu ubuntu 56320 Jul 24 16:29 oTAUGixH.exe
-rwxr--r-- 1 ubuntu ubuntu 56320 Jul 25 06:15 oracAPlw.exe
-rwxr--r-- 1 ubuntu ubuntu     0 Aug 23 21:22 uJIimugh.exe
-rwxr--r-- 1 ubuntu ubuntu     0 Aug  9 07:17 udfEIbiB.exe
ubuntu@oc-in-oci:~/samba$ more README_FOR_RESTORE_FILES.txt

All your data has been backup and remove.
If you want receive back your data pay 0.01 BTC to this address: 17KddJw3y8FycFk6eGsQjLPGFf1BRYgsHa
After payment send message to email addr: recoverydata6666@proton.me

How to buy and send BTC(bitcoin):
https://duckduckgo.com/?q=how+to+buy+and+send+bitcoin
ubuntu@oc-in-oci:~/samba$
```

FEATURE ENHANCEMENTS

Thinkst leverages Github and listens; I've suggested enhancements:

SMTP "Relay"

Gaining more information from email

ACME Protocol

TLS certificates for protocols would lend credibility to the instances in the Internet

CONCLUSIONS AND QUESTIONS

- Q: Do you need to deploy one or more honeypots?
  - A: It depends; is the rest of your house in order?
    (e.g. ISO27001 Annex A.14 covering System Acquisition, Development and Maintenance – this should drive changing default credentials before deployment)
- Q: Will a honeypot protect me?
  - A: Not really – but it might help with IoCs (Indications of Compromise) both externally and internally
- Q: What could be the biggest challenges with owning and operating a honeypot?
  - A: Managing the Signal-to-Noise ratio; avoiding both False Positives and False Negatives

THANK YOU

Lee Mössner

lee@toce.ch

Presentation

LinkedIn

Learn More