Log-Thoth Targeted Timeline Tool

Translator of windows logs from development to cybersecurity context

The Ancient Egypt God Thoth

Thoth (تحوت) was the Egyptian God of writing, wisdom, and magic. He was associated with order and justice and an advisor to the gods

Table of contents

01 **Current State of Security**

An increasing risk of breach merciful to no one.

02 **Incident Handling**

Time sensitive and consuming process.

03 **Seeking an Answer**

Dreaming of cost effective and setup-less solution.

04 **Development of LogThoth**

Transitioning from a script to a fully fledged solution.

01

Current State of Security

Multiple recent breaches but little accountability

Recent Cyber Breaches

Credit Card Company

An attacker claims that they managed to have access on a “big credit card company” and selling it on the dark web

Academic Institutions

Multiple data leaks were found on the dark web that contain personal students information to more than one University

Real Estate Company

A company operations slowed as their devices were infected with a ransomware

Critical Systems

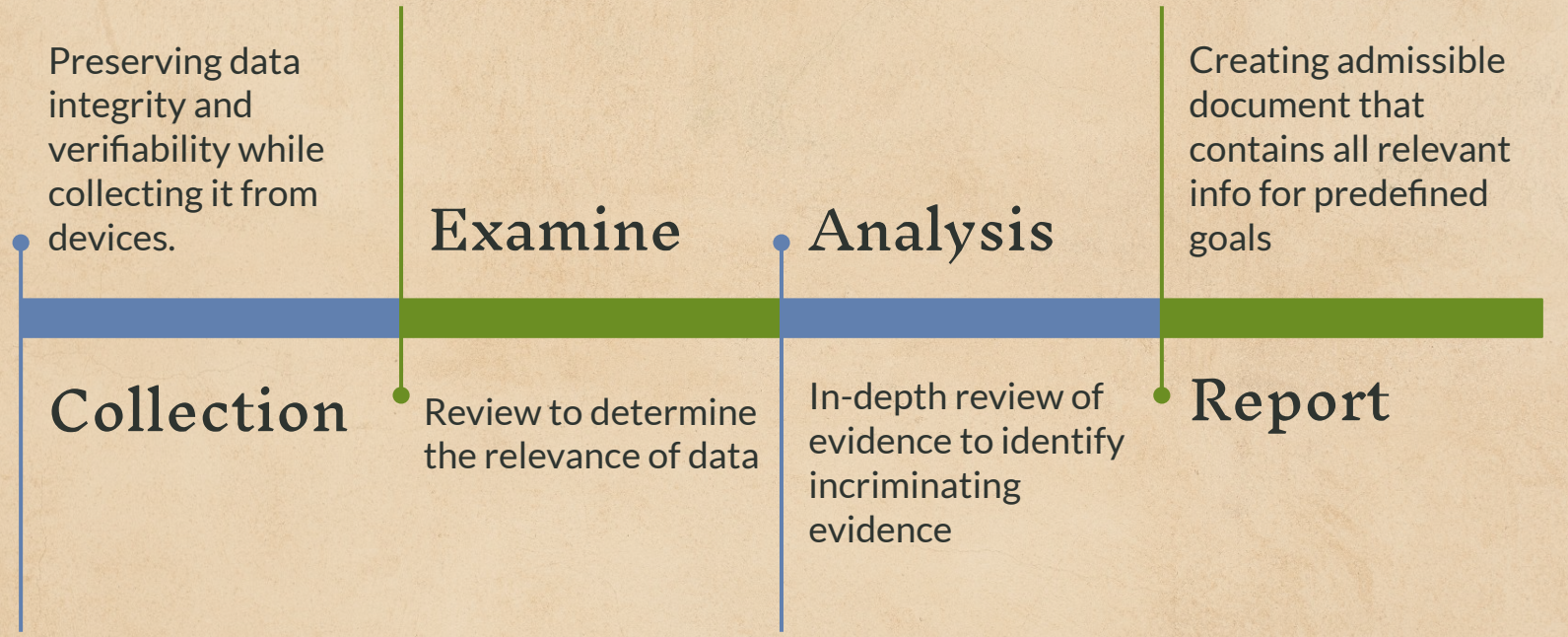
Many shops are running financial systems and queueing systems that operations may stop if not available

02

Incident Handling

Transforming chaotic state to absolute order and control

Investigation Process



Challenges

Delay

Time plays a great role in the investigation process as in business

Cost

Maintaining a secure environment is resources consuming

Skill

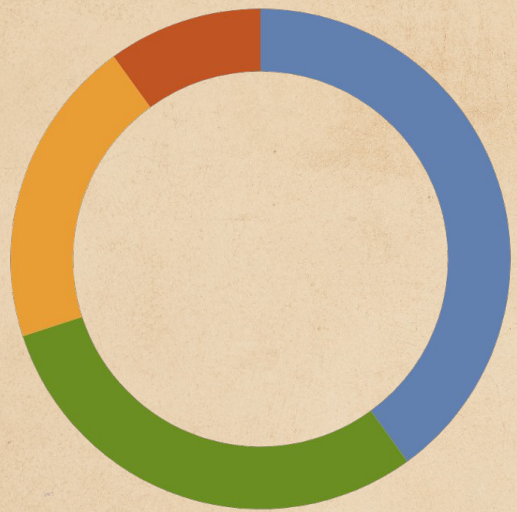
It can be challenge to find a skilled team of digital forensics investigators

03

Seeking an Answer

Looking back to before the beginning of security

Operating System Market Share



For more info, click here

42% - Android

Mostly are mobile phone devices

30% - Windows

The most used operating system

17% - Apple IOS

IPhone is alway on high demain in the US

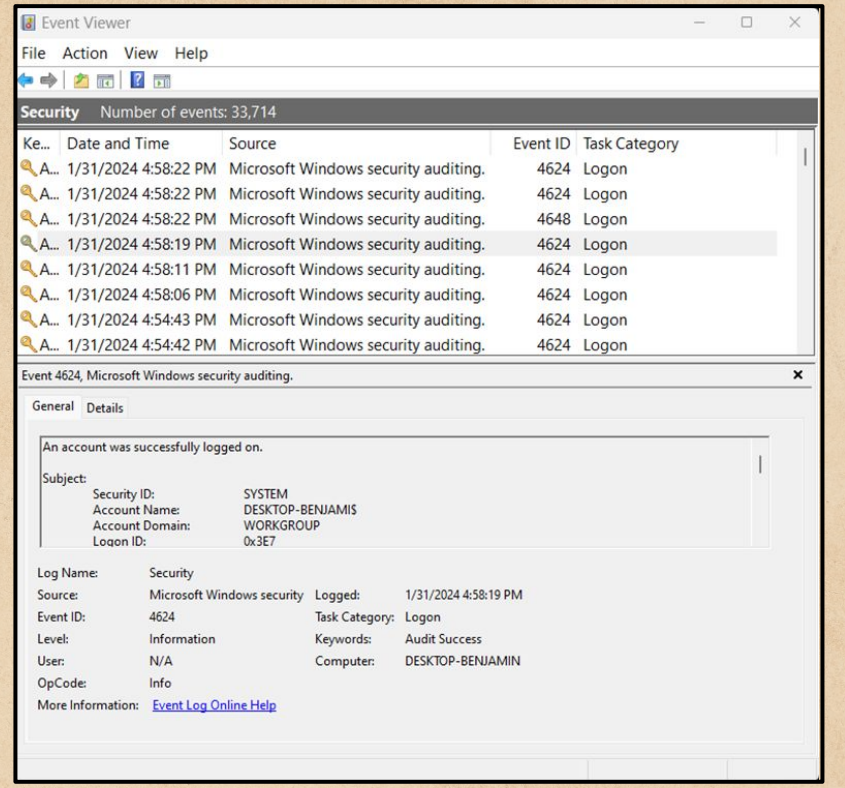
11% - Other

Mac IOS or unknown

Windows Logging Service

Windows Logging Service records events from various sources and stores them in a single collection called an event log.

Yet the service is by architecture is designed to track application execution overlooking it’s value in cyber security investigations.



04

Development of LogThoth

One must go where no one ever dared to look

The tool relies only on Windows as an OS being itself and does not interfere nor run as a service nor exist on the device unless desired by an investigator in case it was needed. A different approach that does not reinvent nor replace an existing feature but fully utilizes all available info to paint a comperhinedable picture that describes an event, when it happened and by who.

01 Less computing resources

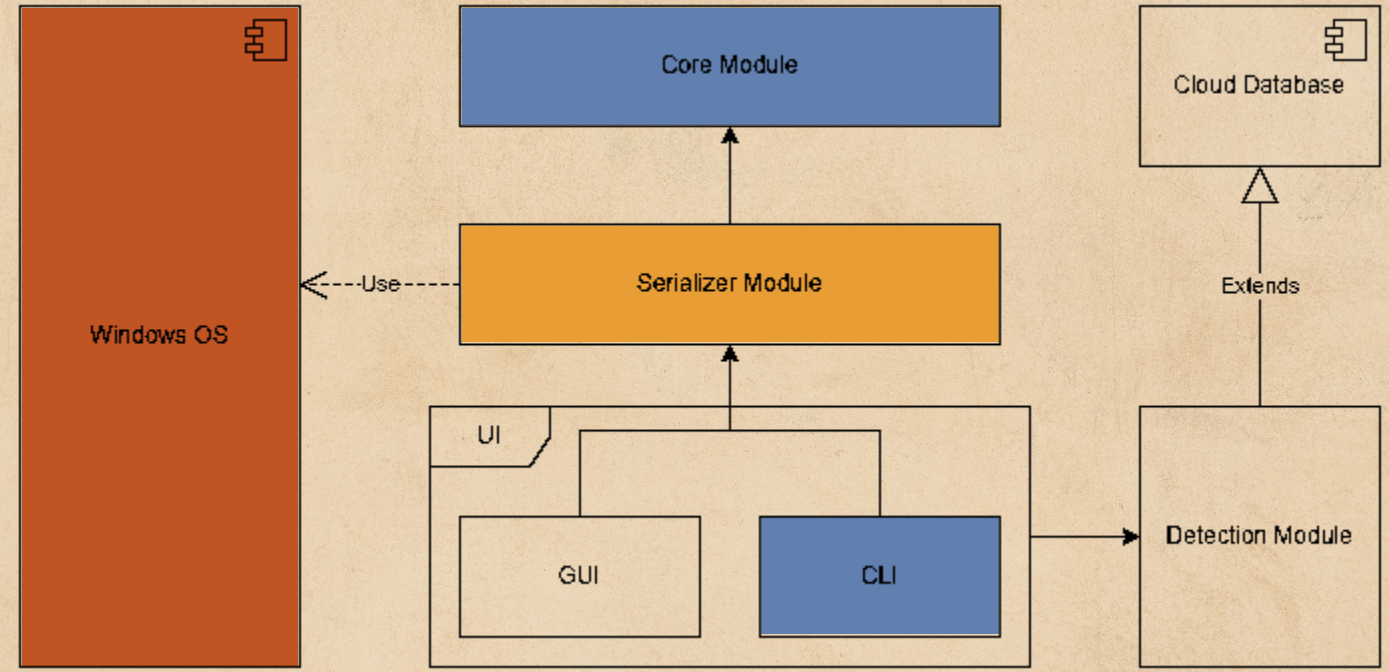
02 No preparation required

03 Simple to use

04 Reduce analysis time

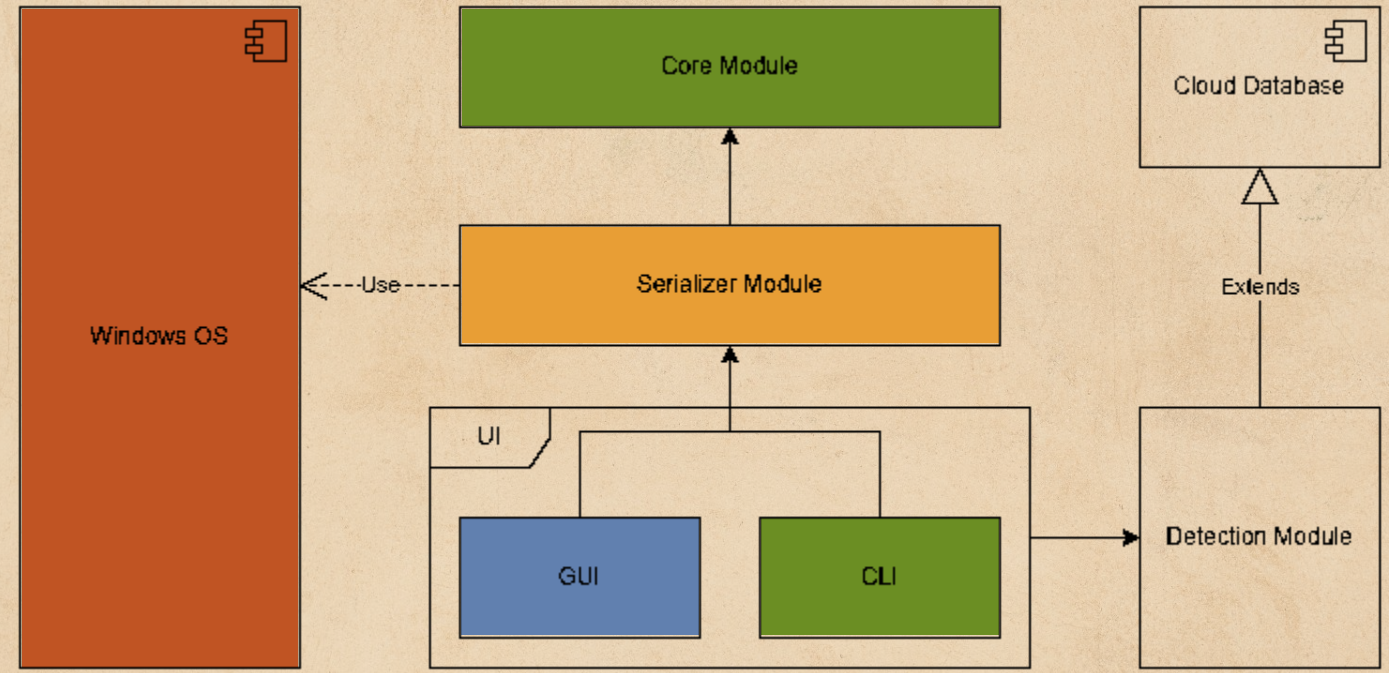
05 Auto generated report

Development Phase 1



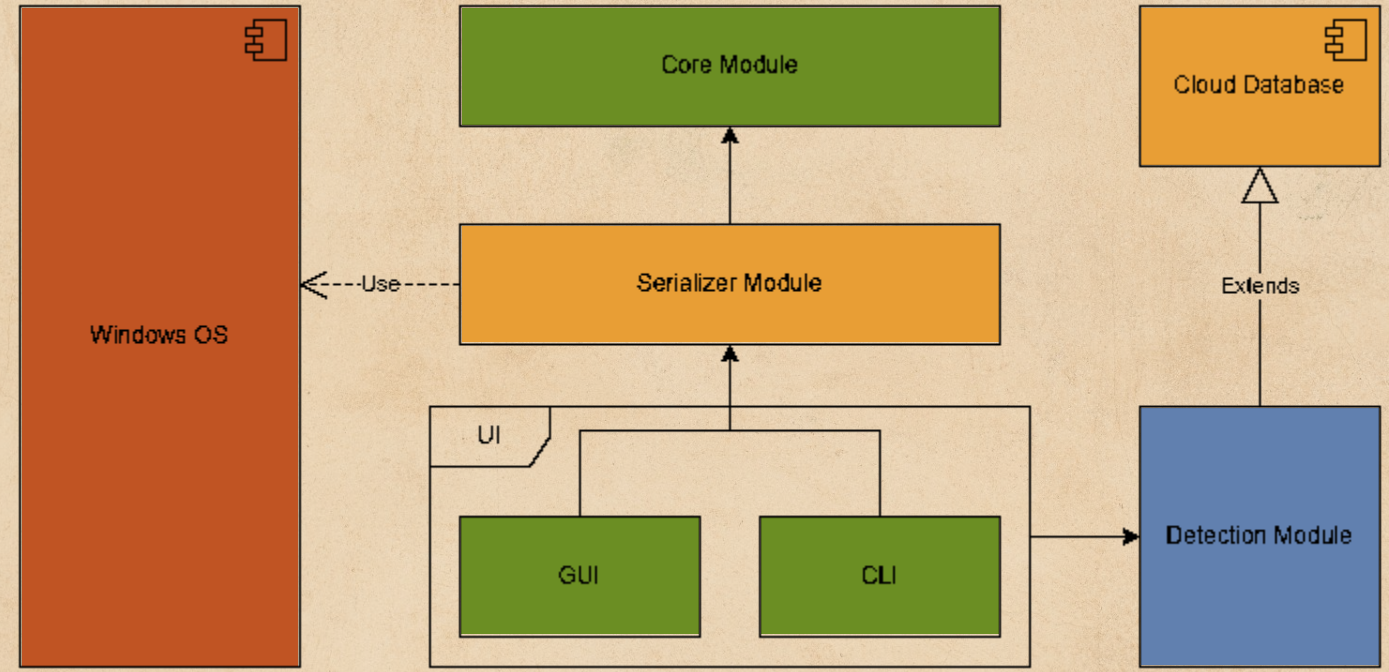

[2024-01-25 21:38:38] Boot
[2024-01-27 13:48:17] Login user
[2024-01-28 19:03:10] Process Creation C\Windows\System32\lsass.exe
[2024-01-28 19:03:08] Process Creation C\Windows\System32\csrss.exe
[2024-01-28 19:03:03] Process Creation C\Windows\System32\smss.exe
[2024-01-28 19:03:02] Process Creation C\Windows\System32\autochk.exe
[2024-01-26 22:16:17] Login user
[2024-01-25 21:38:53] Login user
[2024-01-24 14:06:09] Boot
[2024-01-25 20:29:19] Login user
[2024-01-25 21:38:50] Process Creation C\Windows\System32\lsass.exe
[2024-01-25 21:38:48] Process Creation C\Windows\System32\csrss.exe
[2024-01-25 21:38:43] Process Creation C\Windows\System32\smss.exe
[2024-01-25 21:38:42] Process Creation C\Windows\System32\autochk.exe

Development Phase 2




5:00:30 AM
5:01:00 AM
5:01:30 AM
T1567: Exfiltration begins
MITRE ATT&CK
T1043: Command & control
T1567: Exfiltration
URLs
/honeypot/BSidesDFW%20-%202014.i...
/squid/access.log.gz
/tg/b.zip
/robots.txt
/tg/a.zip
/maccdc2012/conn.log.gz
IP Addresses
Asia
China
Shenyang
123.184.217.240
182.201.219.140
182.201.217.12
182.200.25.81
Nanyang
C2: 182.118.13.8
Hohhot
1.180.208.148

Development Phase 3



Principles related to Thoth

Mentalism

All is mind; everything originates from the mental realm.

Correspondence

There is a connection between the macrocosm and microcosm.

Vibration

Everything is in a constant change yet the rate differs

Polarity

Everything has dual aspects; opposites are merely extremes of the same thing.

Rhythm

There are natural cycles and patterns that govern existence; everything has its ebb and flow.

Causality

Every cause has an effect, and every effect has a cause; there is no chance or randomness.

Thanks!

by Mohamed Gabr & Ahmed Mamdouh