(Research Highlight) Red Team Redemption: A Structured Comparison of Open-Source Tools for Adversary Emulation

MITRE Caldera · Follow

2 min read · Just now

Authors: Michael Kouremetis

The MITRE Caldera™ team just wanted to highlight what is, at least in our view, a well done survey of adversary emulation tools recently conducted by cyber security researchers out of the ***Center for Digital Safety & Security, of the Austrian Institute of Technology***. We found the survey to be of high quality, arguably the best methodical evaluation of adversary emulation tools (that we have seen), and most importantly useful. We can now just send back this survey when asked about a comparison of open source adversary emulation tooling , which happens a lot around here :). So a big thank you to the authors from the Caldera team.

Kudos to the authors ***Max Landauer, Klaus Mayer, Florian Skopik, Markus Wurzenberger,*** *and* ***Manuel Kern.***

Paper link: https://arxiv.org/abs/2408.15645

**Note on survey evaluation results:*

Yes, MITRE Caldera was ranked highly by the authors in their independent survey but that's not why we are sharing the survey. We are sharing the survey because it is a very good survey, period. Additionally, the Caldera team believes in having many tool suites, and always using the best tool for the job. Not to mention that our team uses at least half of the other tools surveyed, and that Caldera makes significant use of one of the other evaluated tools (i.e. Atomic Red Team).

Resources

Caldera Homepage

Caldera GitHub

Caldera Documentation

Caldera Users Slack

Adversary Emulation | Mitre Caldera | Cybersecurity | Red Teaming

Follow

Written by MITRE Caldera

623 Followers

MITRE Caldera Team

More from MITRE Caldera

MITRE Caldera

Emulating complete, realistic cyber attack chains with the new Caldera Bounty Hunter plugin

Authors: Louis Hackländer-Jansen

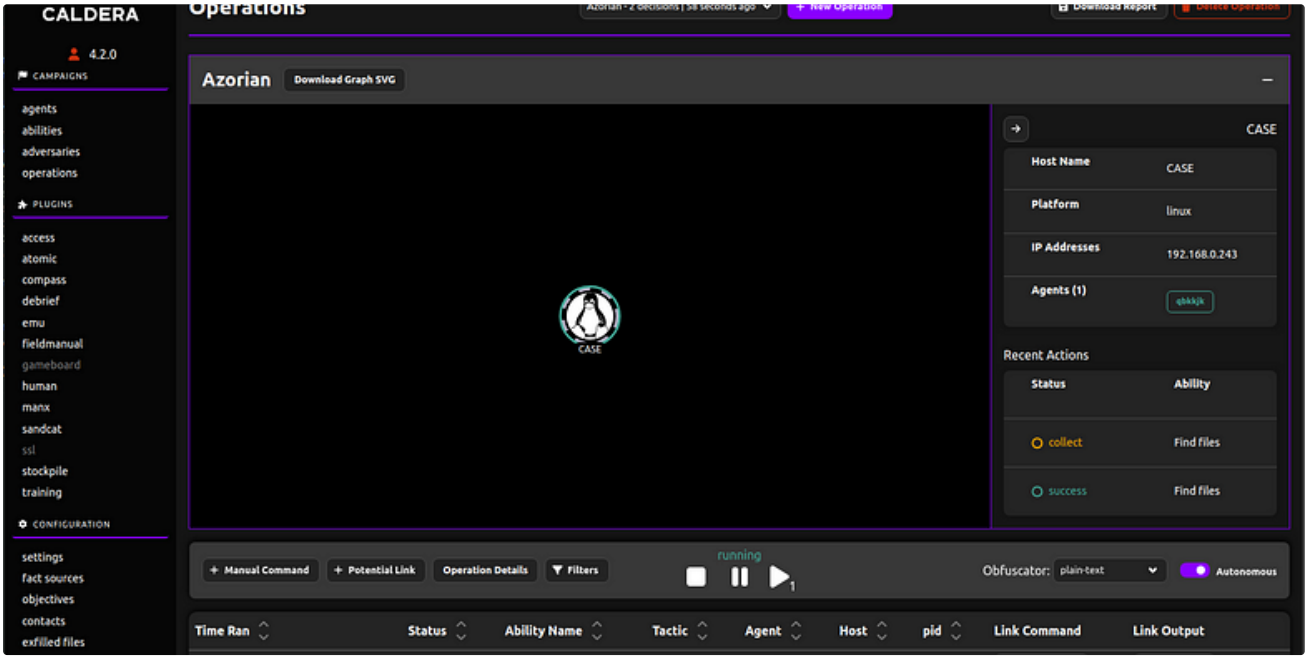
Oct 8 14

MITRE Caldera

A Beginner's Guide to MITRE Caldera™ User Training

Authors: Kate Esprit

Sep 13, 2022 88 1



MITRE Caldera

MITRE Caldera

Welcome to the official MITRE Caldera™ blog page!

Authors: Kate Esprit, Daniel Matthews & Turquoise Richardson

Aug 23, 2022 133

See all from MITRE Caldera

Recommended from Medium

Zammaar Malhi in Insightful Echoes

The Rising Tide of Linux Ransomware: Are Your Systems Secure Enough?

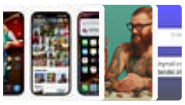
The Growing Menace of Linux Ransomware: Are You Ready? In the ever-evolving face of cybercrime, ransomware attacks are no longer restricted...

Aardvark Infinity in Aardvark Infinity

A Dance with the Dark Web: Monitoring Underground Activity with Python (Φ)

In the shadows of the internet, hidden beneath layers of encryption and anonymity, lies the dark web — a place where data, illegal goods...

Lists Oct 5



Tech & Tools

20 stories · 321 saves

Medium's Huge List of Publications Accepting Submissions

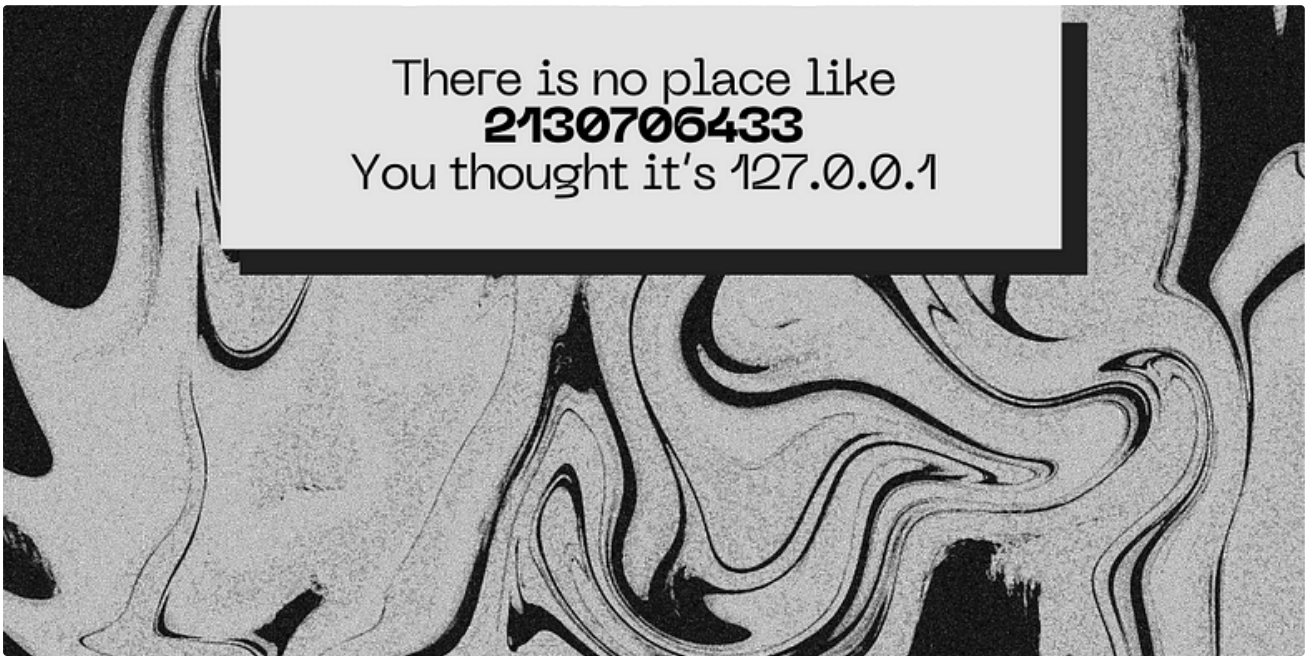
334 stories · 3690 saves

Staff Picks

750 stories · 1372 saves

Natural Language Processing

1754 stories · 1352 saves

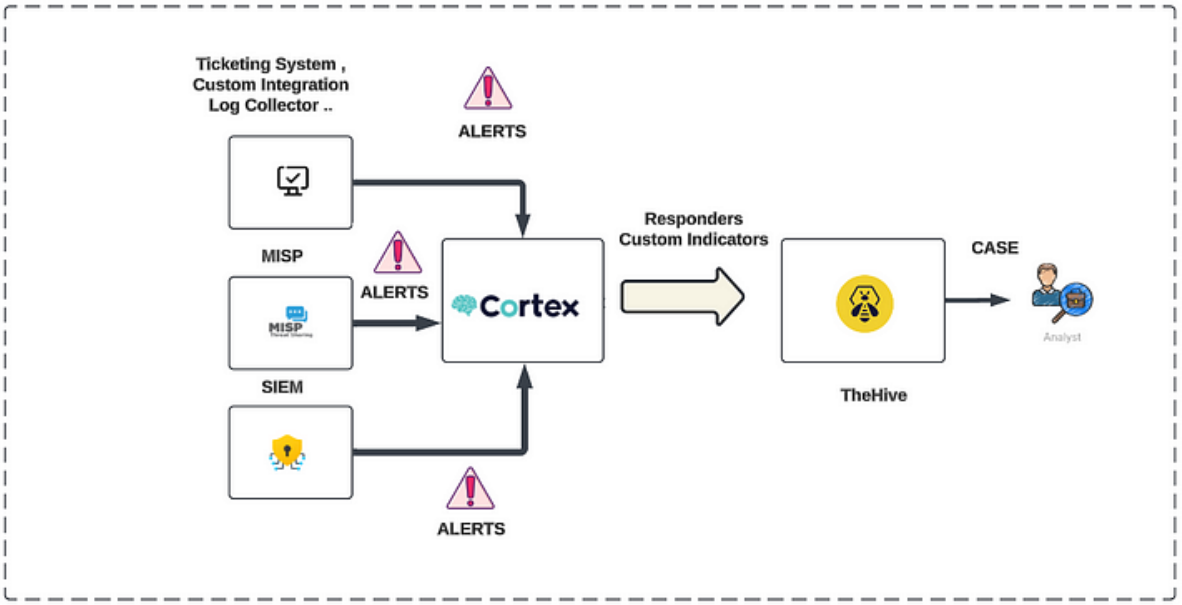


Rahul Sharma in Level Up Coding

You Won't Believe What I Discovered About IP Addresses!

I am sure you will learn something new today!

Oct 3 921 20

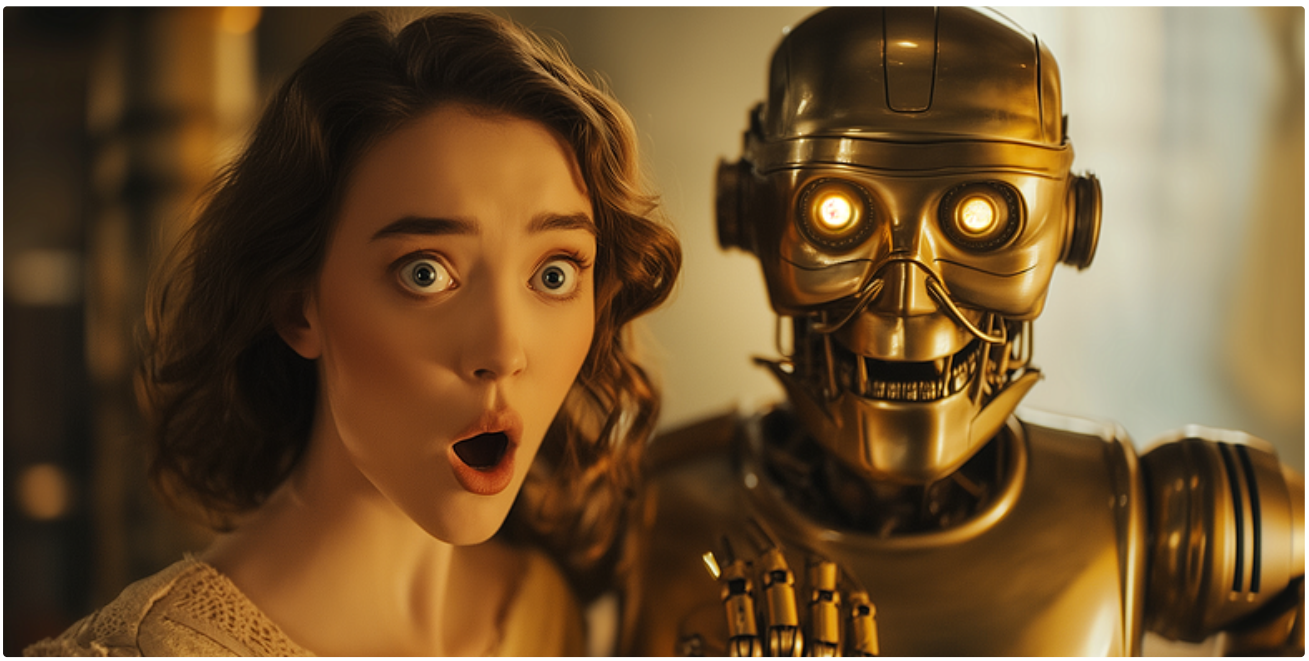


Tamir Suliman

Streamlining Cyber Incident Response: Deploying TheHive with Docker Simplified

TheHive Deployment with Docker: A Step-by-Step Guide

Jul 4 2 1



Henrique Centieiro & Bee Lee in Limitless Investor

AI: 99% of You Are NOT Ready for What's Coming in 2027

AI's Insane Leap — You Likely Don't Want to Be Left Behind

Mr.PlanB

Top VDI Solutions for Homelabs and Small Businesses: From RDP to Proxmox and Beyond

As virtual desktop infrastructure (VDI) becomes an essential tool for businesses and IT environments of all sizes, it's important to...

3d ago 6