

Never Ending Story

Black Cell's Mission

DEFENDING TOMORROW

At Black Cell, we're passionate about protecting what matters most—our clients' invaluable digital assets. Our mission is simple: to help organizations build strong, long-lasting security foundations while continually monitoring, evaluating and improving their cybersecurity resilience.

SPECIALIZATIONS

We specialize in reducing the risks that come with Industry 4.0, safeguarding both IT and OT environments. Whether on-premises or in the Microsoft Cloud, we're here to offer real-time protection with effective detection, prevention, and response to keep our clients ahead of cyber threats.



2010

founded



5

offices worldwide



50+

employees



200+

happy clients

Introduction

Protecting critical infrastructures.



Black Cell is a professional cybersecurity company providing end-to-end cybersecurity assurance within its Fusion Center, Integration, Offensive Security and Compliance solution areas, as well Cloud Security and ICS/OT Security specializations.

Goal

Our goal is not only advising to the best of our knowledge,
but creating bespoke & resilient cybersecurity ecosystems.

The goal of our leadership team is to provide clear direction,
foster collaboration and innovation in order to help our clients'
organization towards sustained growth and success.



Intro

Preview of what's to come



01

Threat landscape: power function

- Credentials, "the Key to the Kingdom" (Stealer logs);
- Skeleton key;



02

IRP (testing)

- TTX;
- Red Teaming; (OpenBAS)



03

Detection maturity

- Adequate visibility & measured coverage;
- Responders equipment (eg.:Rescue VLAN);
- Deception;



04

Processes

- Knowledge base;
- Etc.

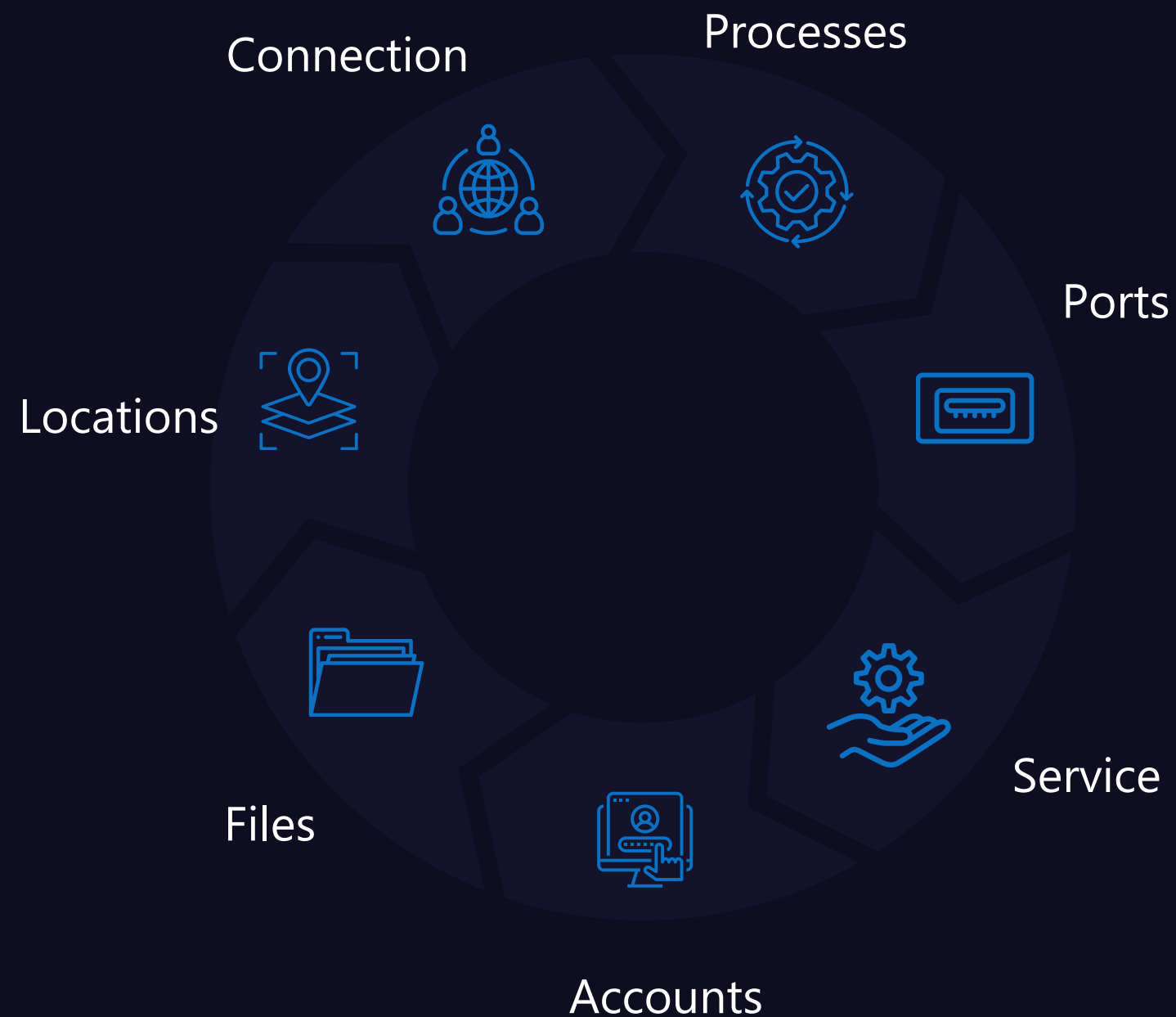


CMO







CMO

Current Mode of Operation

REMOTE TRIAGE



TOOLS

-  Log manipulation platform (SIEM)
-  Windows Management Infrastructure
-  PowerShell (Psexec)
-  Memory (Volatility)
-  Autoruns
-  Timeline analysis (Redline)
-  Internal network logs (mirroring)
-  Malware analysis (please stay local!)
-  SMB (Lateral Movement)
-  Kerberos (Golden Ticket)



Workflow

Sequence of tasks and processes



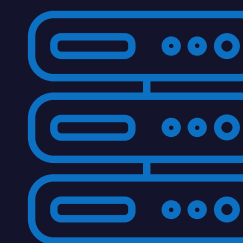
Step 1: Elasticsearch alerts



Step 2: AI Agents (Log Analysis & Threat Intel) - analyze



Step 3: Decision Agent assigns a risk score based on AI-driven insights



Step 4: Action Orchestrator (AI Agent) decides next steps:

- If automated response is possible → Triggers script (e.g., blocks IP, disables account).
- If human intervention is needed → Escalates to Analyst Dashboard

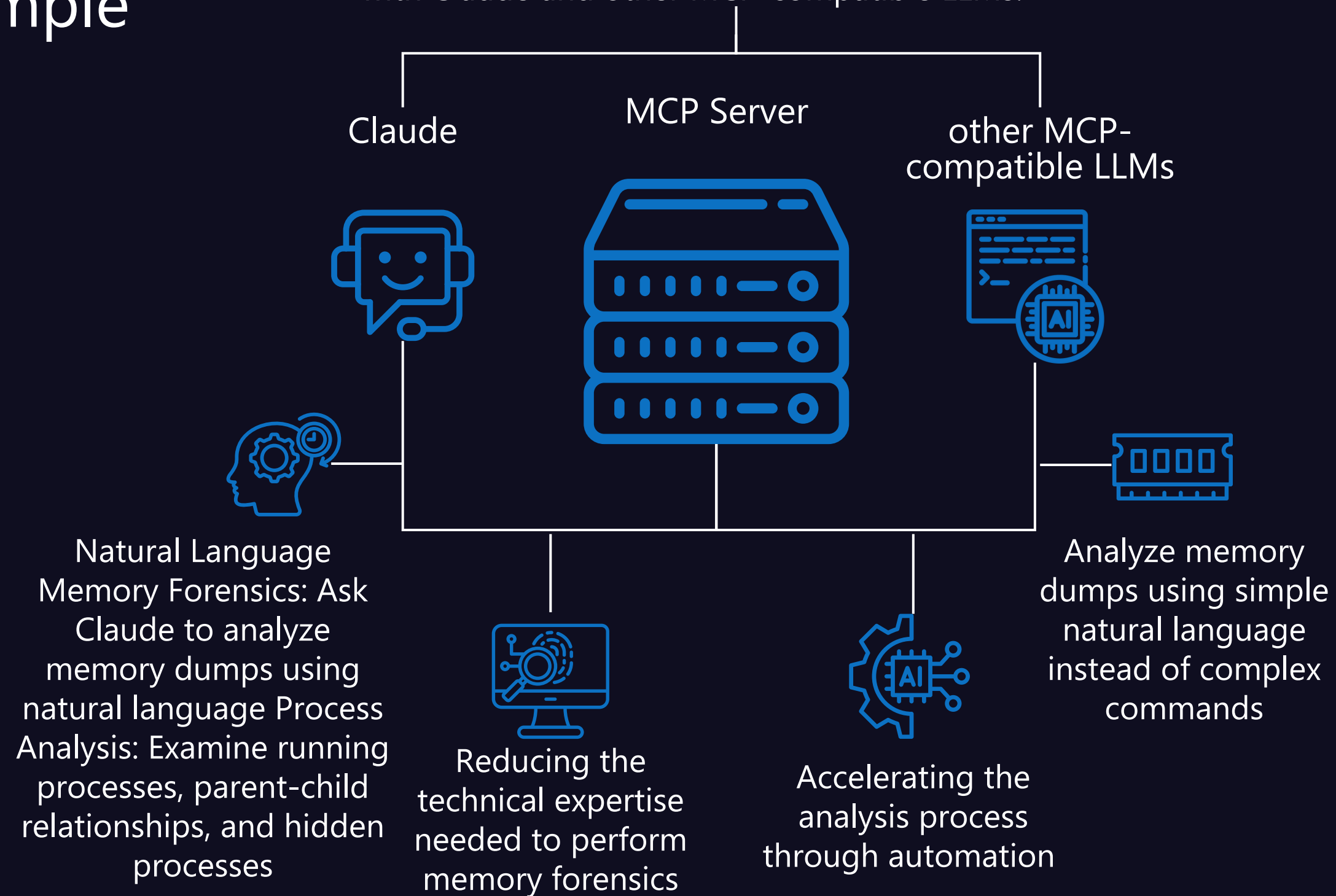








Step 5: Final results are visualized in Kibana for monitoring

Example

MCP Server Example

A Model Context Protocol (MCP) server that integrates Volatility 3 memory forensics framework with Claude and other MCP-compatible LLMs.



-  Network Forensics: Identify network connections in memory dumps
-  Malware Detection: Find potential code injection and other malicious artifacts
-  DLL Analysis: Examine loaded DLLs and modules
-  File Objects: Scan for file objects in memory
-  Custom Plugins: Run any Volatility plugin with custom arguments
-  Memory Dump Discovery: Automatically find memory dumps in a directory

Example

Knowledge Base

Example

msty.app



Contact

Keep in touch

Visit our website, drop us a mail
or contact your Account Executive!

Contact us

 info@blackcell.io

 www.blackcell.io

Thank you!

