Incident Response with Velociraptor



RAPID7
Velociraptor

Miroslav Sidor

WHOAMI

- **Miroslav Sidor**
- **10+ years in Security**
- **ESET employee**
- **Started in Ceský Statistický Úřad**
- **CTFs player**





Agenda

- **Incident Response 101**
- **IR Process**
- **Introduction to Velociraptor**
- **Deployment**
- **Live IR DEMO**

Incident Response 101

- **Incident is any event that threatens confidentiality, integrity, or availability (CIA Triad)**
- **Incident Response is an organized approach to addressing incidents, with the goal of limiting damage and reducing recovery time and cost.**
- **You can NOT investigate big incidents alone!**

Incident Response 101



IR Process

Durin incident response we want to answare 5Ws and 1H:

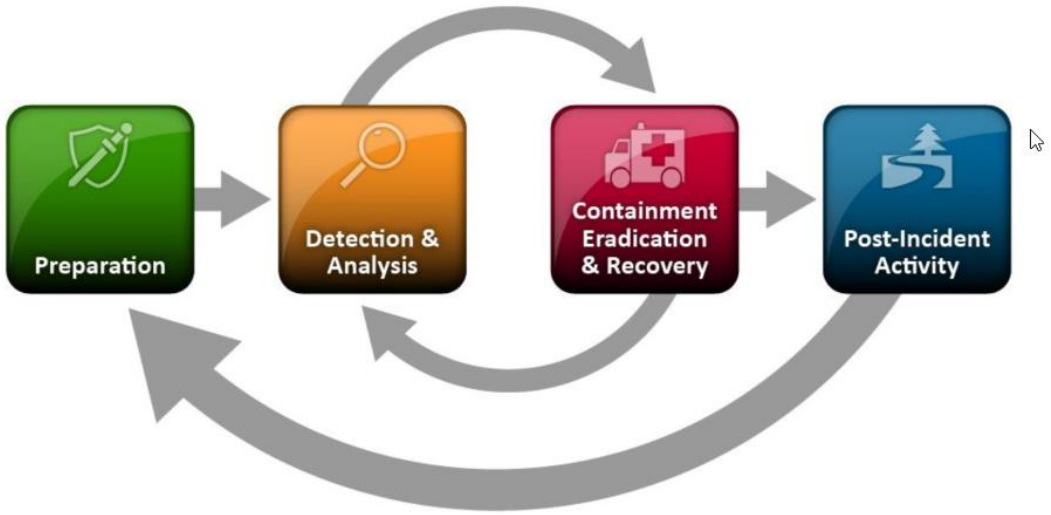
- **Who – did it ?**
- **What – happened ?**
- **When – did it happen ?**
- **Where – did the incident occur ?**
- **Why – did it happen ?**
- **How – did happen ?**

IR Process

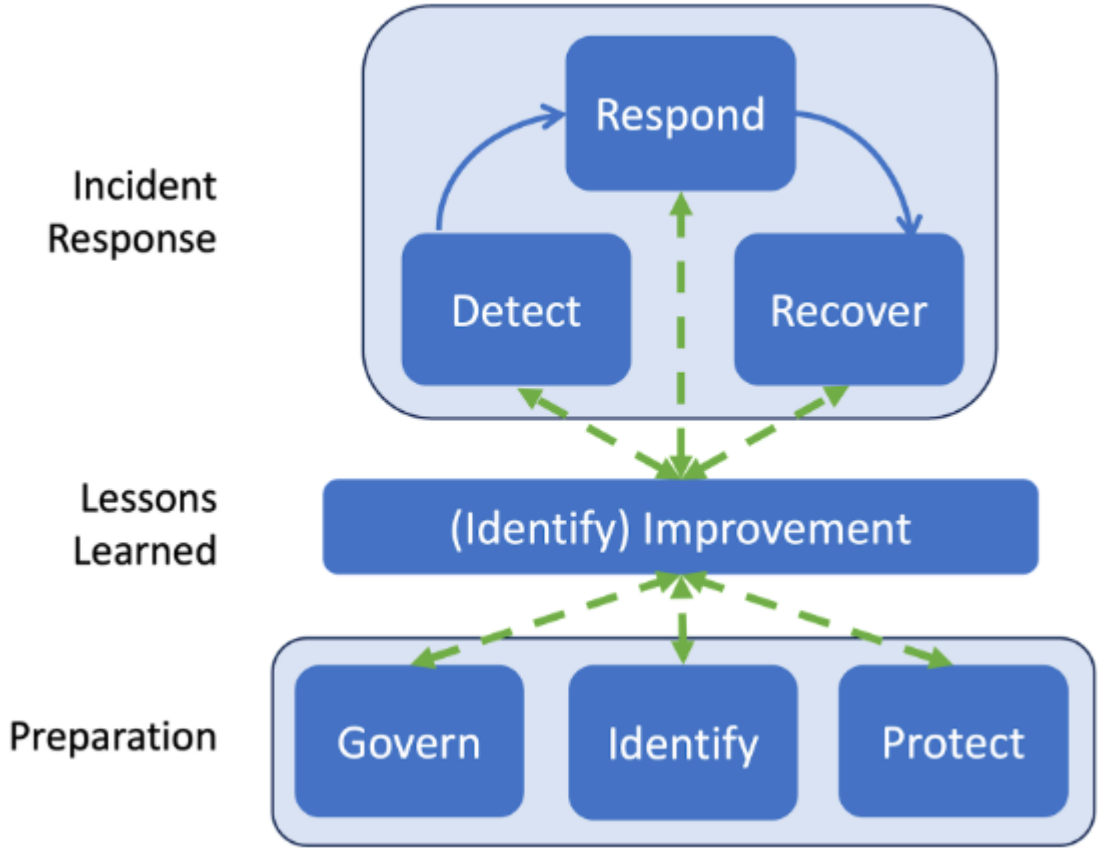
To guide us through the incident response process, we can rely on established frameworks:

- **NIST SP 800-61** – Computer Security Incident Handling Guide (Rev. 2) / Incident Response Recommendations (Rev. 3)
- **SANS Incident Response** – PICERL and the newer **Dynamic Incident Response (DAIR)**

NIST SP 800-61 v3



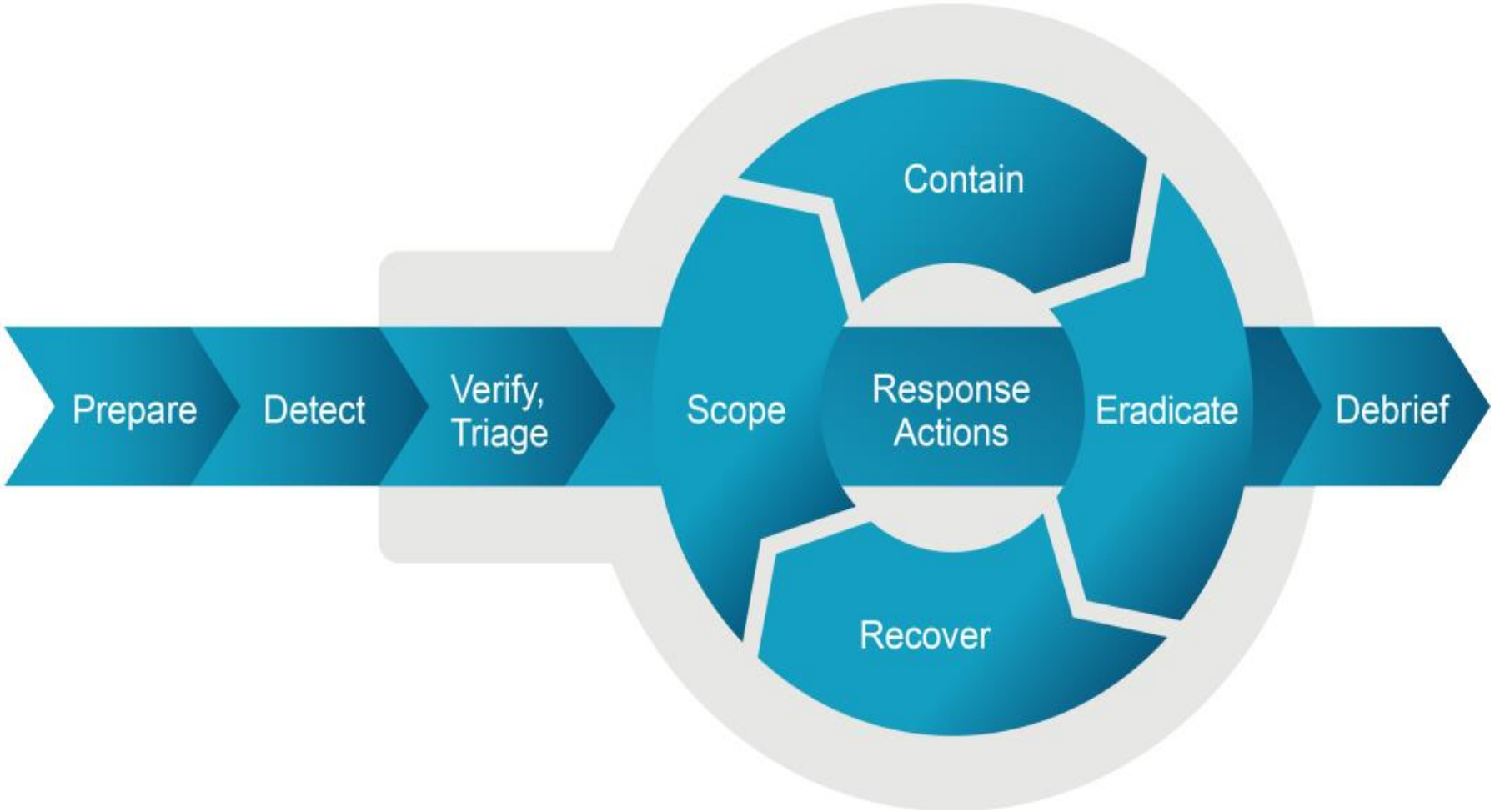
NIST SP 800-61 v2



NIST SP 800-61 v3

Source: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r3.pdf

SANS DAIR



Source: https://www.sans.org/engage/dynamic-incident-response

SANS DAIR

Incident response is not a linear process.

- Traditional frameworks often present incident response as a sequence of predefined phases.
- Real-world incidents are unpredictable and constantly evolving.
- New evidence can change our understanding of the incident, its scope, and priorities.
- DAIR promotes **flexibility, continuous reassessment, and evidence-driven decisions.**
- Responders can revisit previous activities as the investigation evolves.

SANS DAIR

Prepare – Establish visibility, tools, and response capabilities.

Detect – Identify suspicious activity and potential incidents.

Verify & Triage – Validate findings and assess urgency.

Scope – Determine affected systems, accounts, and the extent of compromise.

Contain, Eradicate & Recover – Take appropriate response actions based on available evidence.

Debrief – Capture lessons learned and improve future response.

Velociraptor

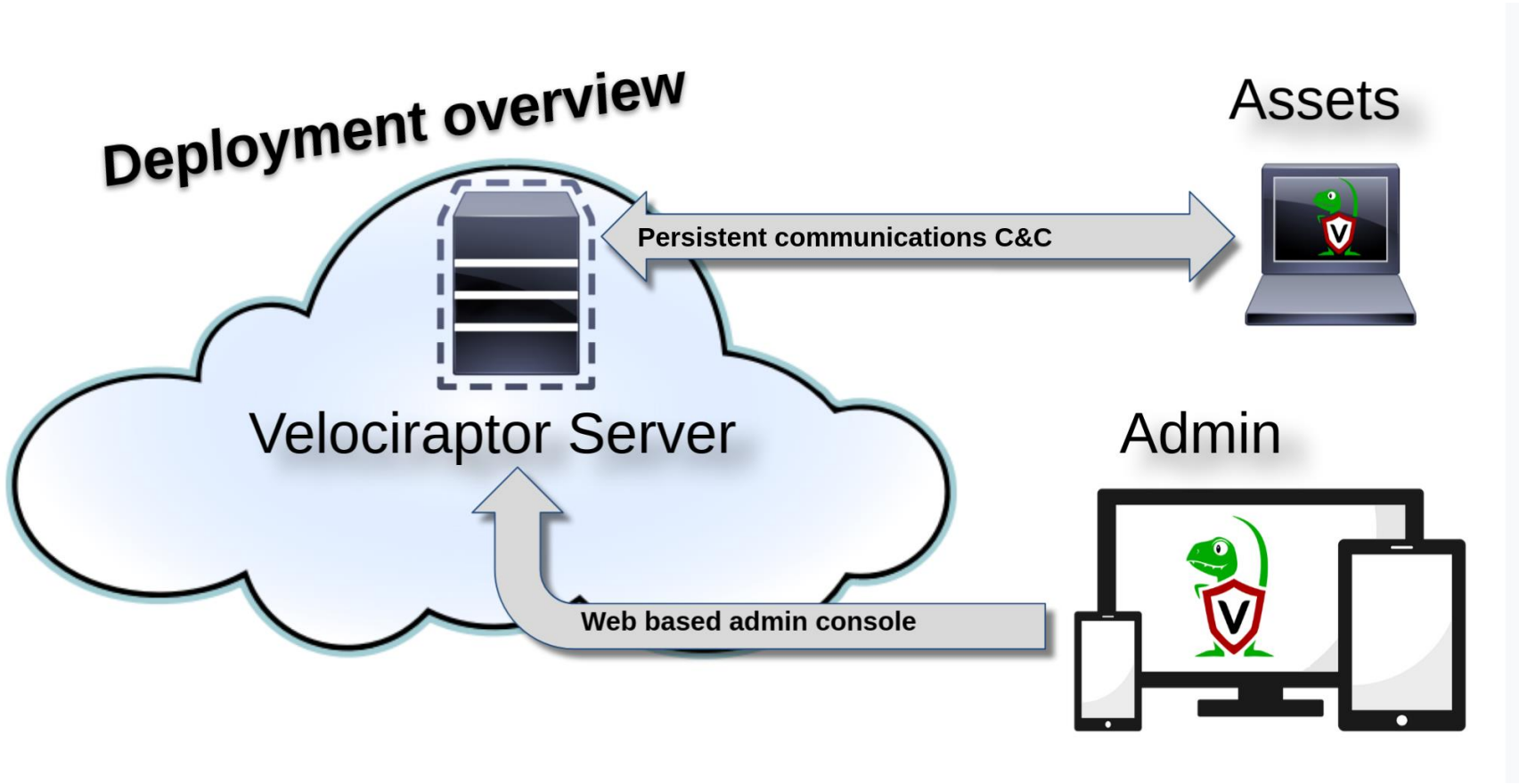
Velociraptor is a unique, enterprise grade, open-source platform for endpoint monitoring, digital forensic and cyber response. Velociraptor covers the entirety of the attack life cycle, providing responders a powerful capability to address past, present and future events.





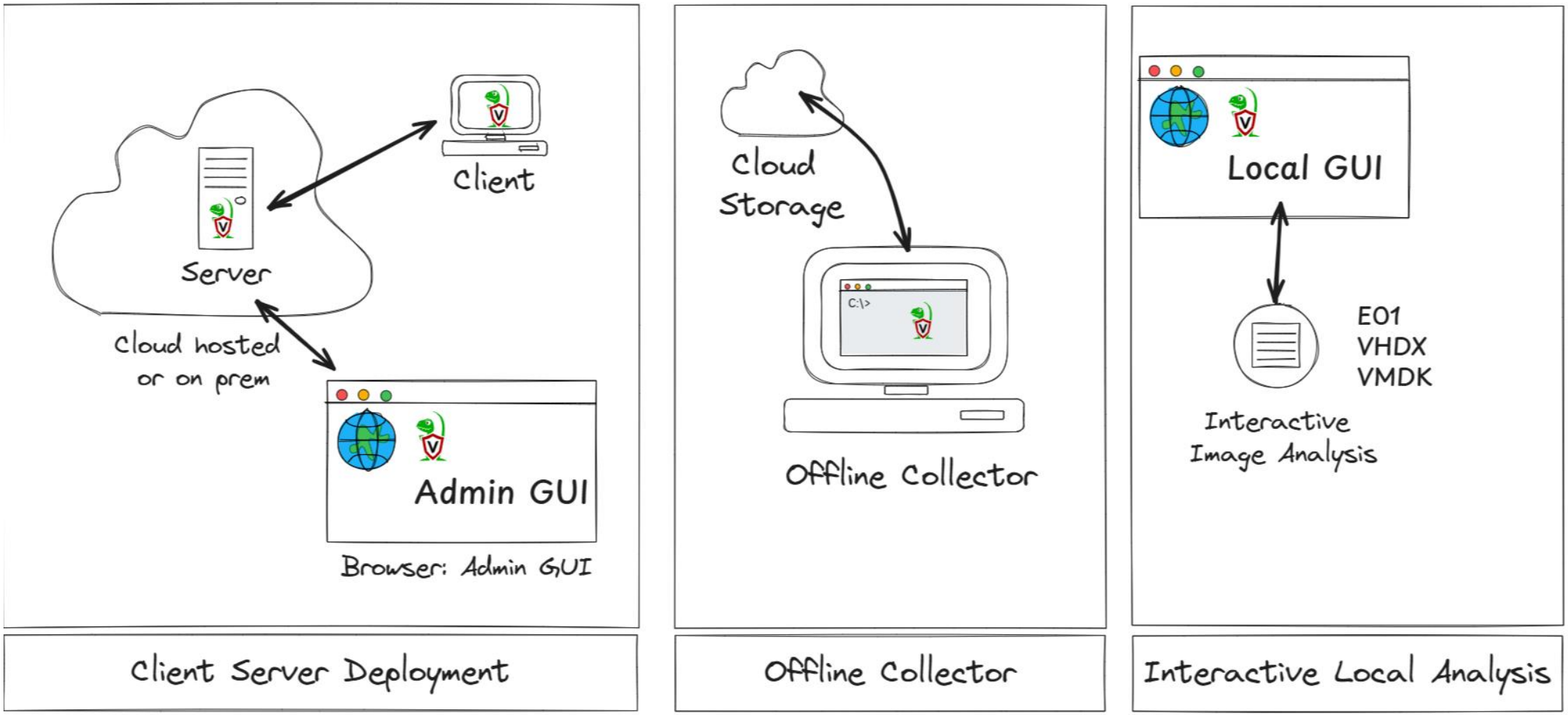
Mike Cohen

Velociraptor



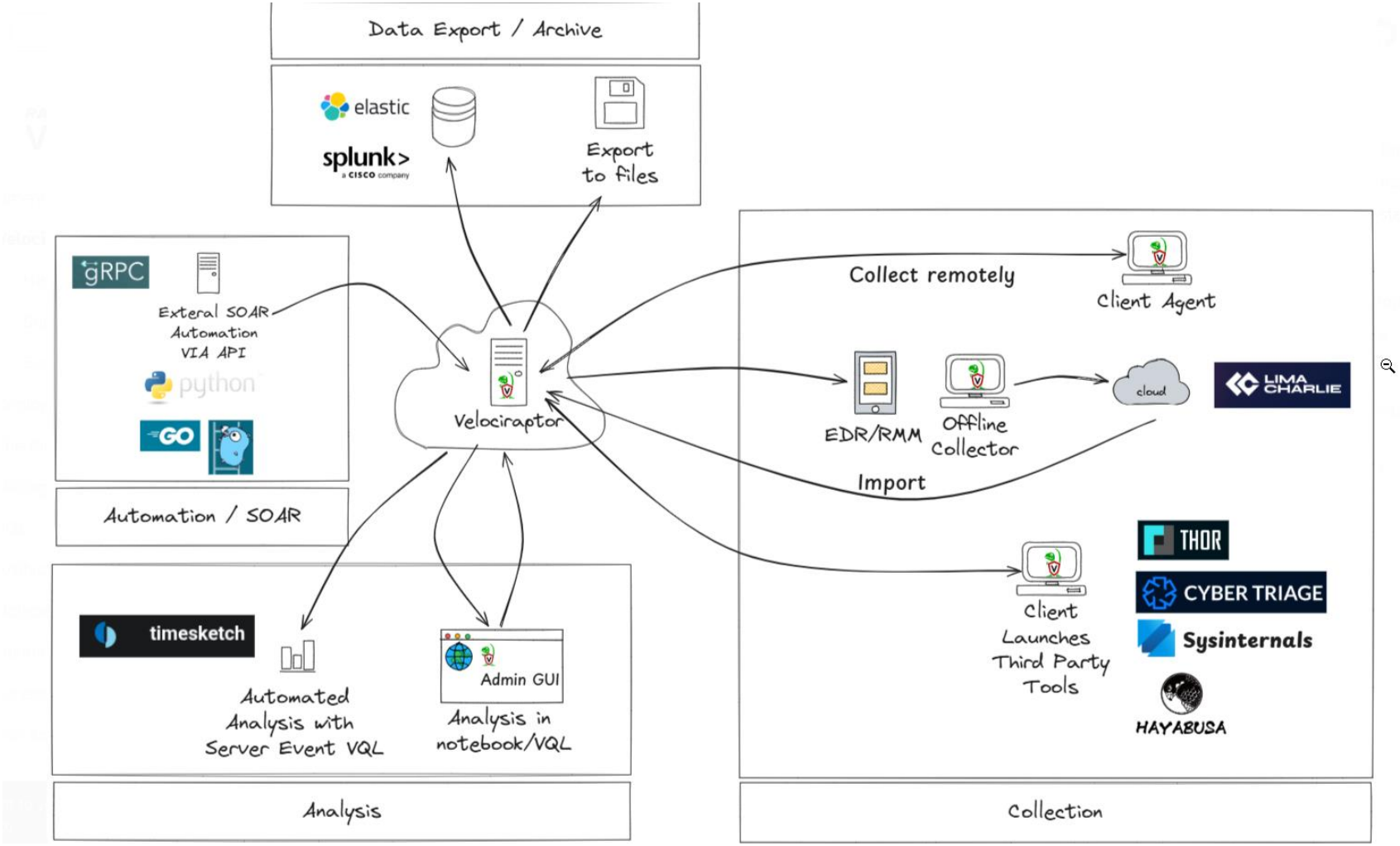
Source:https://docs.velociraptor.app/docs/deployment/

Velociraptor



Source: https://www.velociraptor-docs.org/docs/overview/

Velociraptor

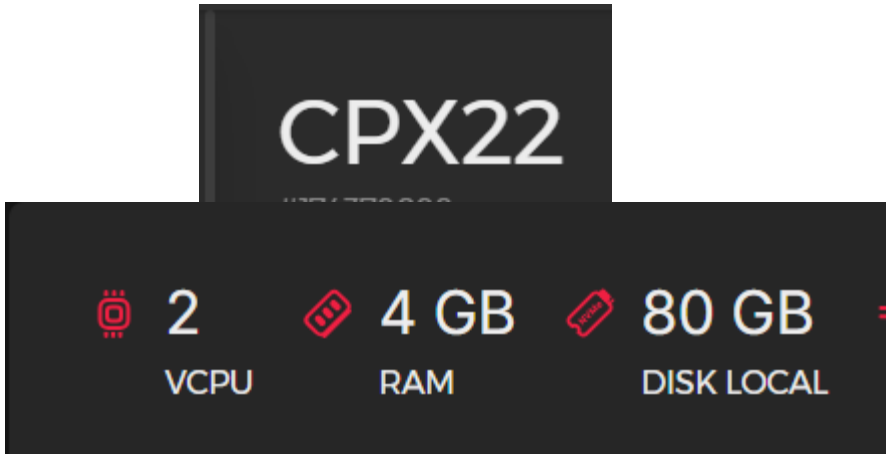


Source: https://www.velociraptor-docs.org/docs/overview/

Velociraptor

HW REQ for 10 000 agents
CPU: 2 Core
RAM: 8 GB
Disk: 1TB till infinty
OS: Debian, Ubuntu, RedHat,

Our Velociraptor



Live Demo Time

Velo artifacts

- **Windows.Network.NetstatEnriched**
- **Windows.Search.FileFinder**
- **Windows.Applications.Chrome.History**
- **Generic.Forensic.SQLiteHunter**
- **Windows.Applications.NirsoftBrowserViewer**
- **Windows.NTFS.ADSHunter**
- **Windows.Hayabusa.Rules**
- **Windows.Detection.Yara.Process**

Resources

- https://www.sans.org/engage/dynamic-incident-response
- https://www.velociraptor-docs.org/
- https://github.com/Immersive-Labs-Sec/SliverC2-Forensics/blob/main/Rules/sliver.yar
- https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r3.pdf