OPEN–SOURCE TOOLS IN INFOSEC

Building a SOC on the Cheap

By: Marco Palacios

**** DISCLAIMER ****

The views and opinions expressed in this presentation are my own, and they do not represent the opinions of my employer. Any questions or concerns about the content of this presentation, please contact me directly.

About Me

- **Marco Palacios**
  - *Incident Handler*
  - *IT Operations 12+ years*
  - *Security Operations 4+ years*
  - *SSCP, GSEC, GCED, Net+, A+*
  - *Veteran – 8 Years in the Air Force Reserve, 1 Deployment*


HONORING ALL
VETERANS
THANK YOU FOR YOUR SERVICE


Thank You
VETERANS

Agenda

- Define Open–Source
- SOC Operations
- Defense–in–Depth
- Infrastructure Review
- Comparison of Tools
- TheHive Project

What is Open–Source?

The term "open–source" refers to something people can modify and share because its design is publicly accessible. The term originated in the context of software development to designate a specific approach to creating computer programs. Open source projects, products, or initiatives embrace and celebrate principles of open exchange, collaborative participation, rapid prototyping, transparency, meritocracy, and community–oriented development.

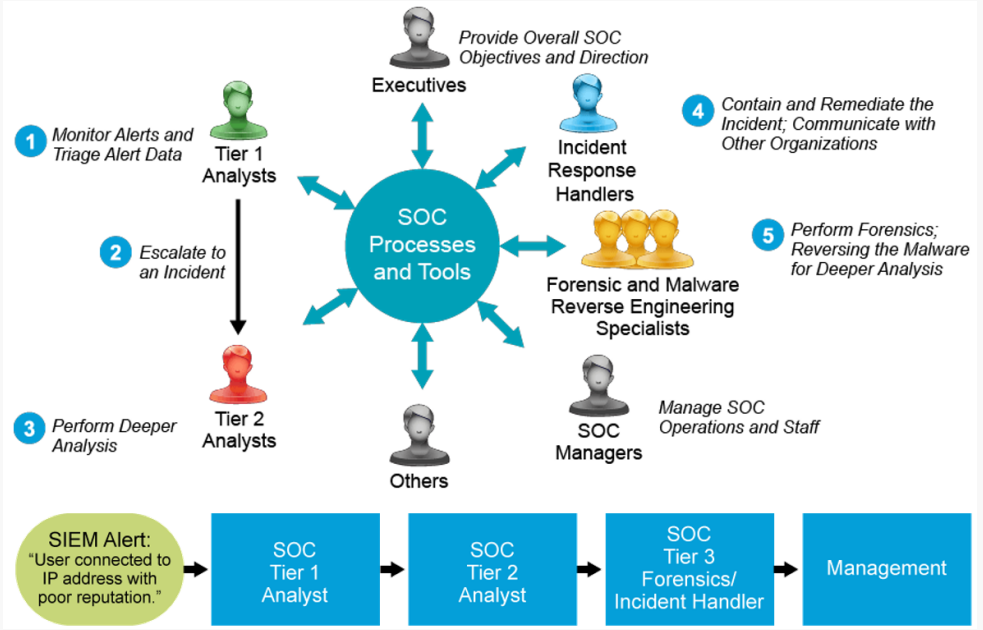
Is it Free?

- Open" vs. "free" vs. "free and open"
  - *Free and open-source software (FOSS) or Free/libre and open-source software (FLOSS) is openly shared source code that is licensed without any restrictions on usage, modification, or distribution.*
  - *Confusion persists about this completely unrestricted definition because the "Free", also known as "Libre", refers to the freedom or the product not the price, expense, cost, or charge.*
- Licenses
  - *Every organization has its own guidelines*
    - Free Software Foundation
    - Debian Free Software Guidelines
  - *Free software or Open-Source software.*

Security Operations Center (SOC)

- The heart of Security Operations
  - *24/7/365*
  - *People, Technology, Processes*
- Becoming a necessity
- The three types of SOCs are:
  - *Threat-centric SOCs*
  - *Compliance-based SOCs*
  - *Operational-based SOCs*

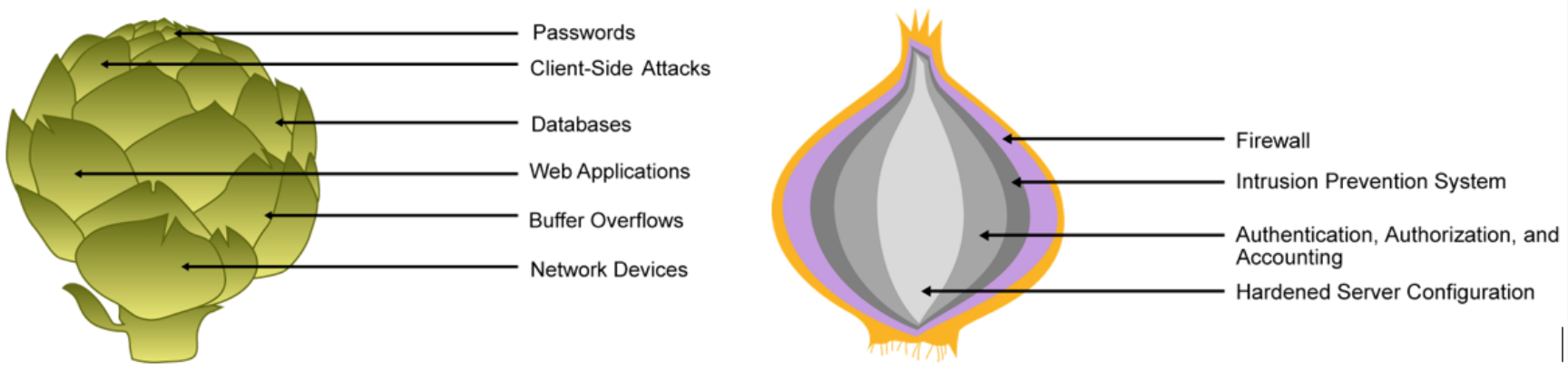
Roles in a SOC



- Tier 1
  - *Continuously monitors the alert queue*
  - *Triages security alerts*
  - *Monitors the health of the security sensors and endpoints*
  - *Collects data and context necessary to initiate Tier 2 work*
- Tier 2
  - *Performs deep-dive incident analysis by correlating data from various sources*
  - *Determines if a critical system or data set has been impacted*
  - *Advises on remediation*
  - *Provides support for new analytic methods that are used in threat detection*
- Tier 3（Security Engineer roles）
  - *Possesses in-depth technical knowledge on the network, endpoint, threat intelligence, forensics, malware reverse engineering, and the functioning of specific applications or underlying IT infrastructure*
  - *Acts as an incident hunter, not waiting for escalated incidents*
  - *Closely involved in developing, tuning, and implementing threat detection analytics*

Defense–in–Depth

- Layers of Security
- Robust Security
- In networking, we say your entire path to your destination is only as fast as your slowest link in the path. And in security, it's often said that the system is as strong as its weakest link.



Infrastructure Review

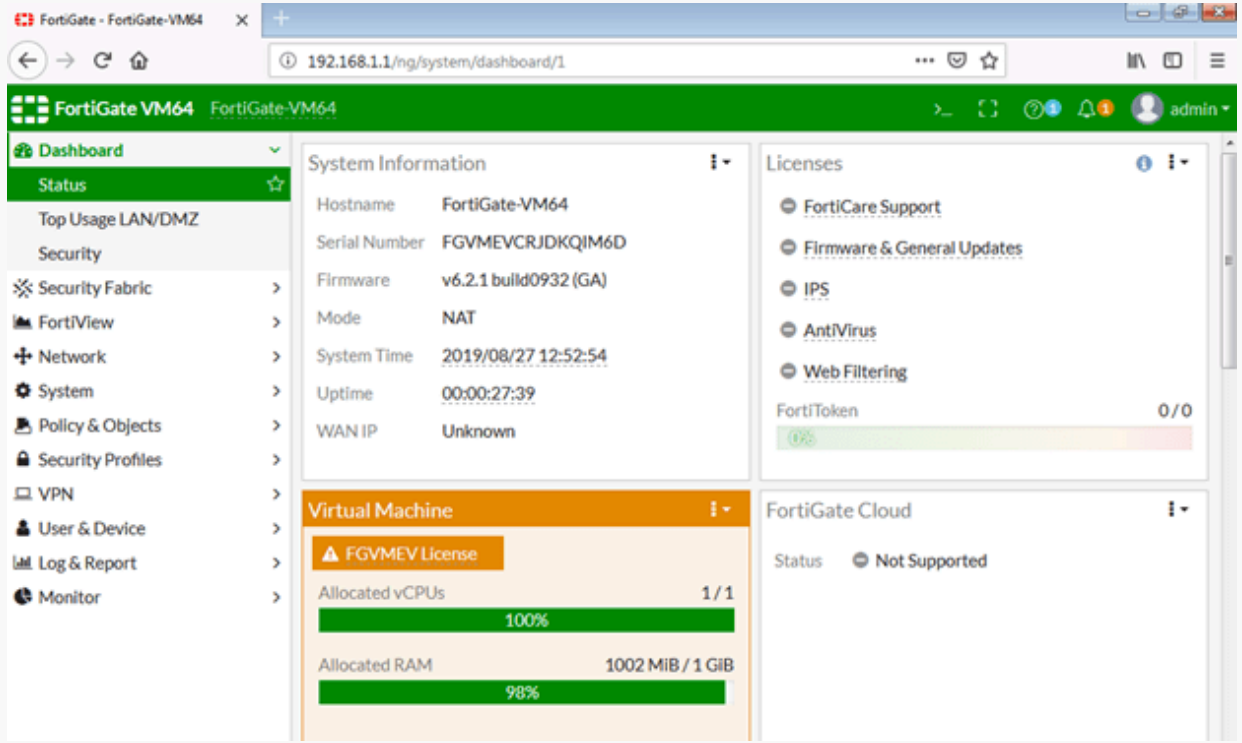
- Authentication, Authorization, and Accounting
- Identity and Access Management (IAM)
- **Stateful Firewalls**
- **Network Taps**
- **IDS/IPS**
- Email Content Security
- **Web Content Security**
- **DNS Security**
- NetFlow
- Network–Based Malware Protection
- **Next Generation Firewall**
- Cyber Threat Intelligence
- **Antivirus**
- **Endpoint Detection & Response (EDR)**
- **Malware Sandboxing**
- **Malware Reverse Engineering**
- **SIEM**
- **Case/Incident Management System**

Tool Comparison

- Router
  - *FortiGate vs. pfSense*
- IDS/IPS
  - *Cisco SourceFire vs. Suricata*
- Packet Capture
  - *Riverbed vs. Moloch*
- DNS Security
  - *Cisco Umbrella vs.* Quad9 DNS service
- Malware Sandboxing
  - *FortiSandbox vs. Cuckoo*
- Malware Reverse Engineering
  - *IDA Pro vs. Blackphenix*
- SIEM
  - *Splunk vs. ELK*
- Antivirus
  - *Symantec AV vs. ClamAV*
- EDR
  - *Carbon Black vs. osquery*

Firewalls

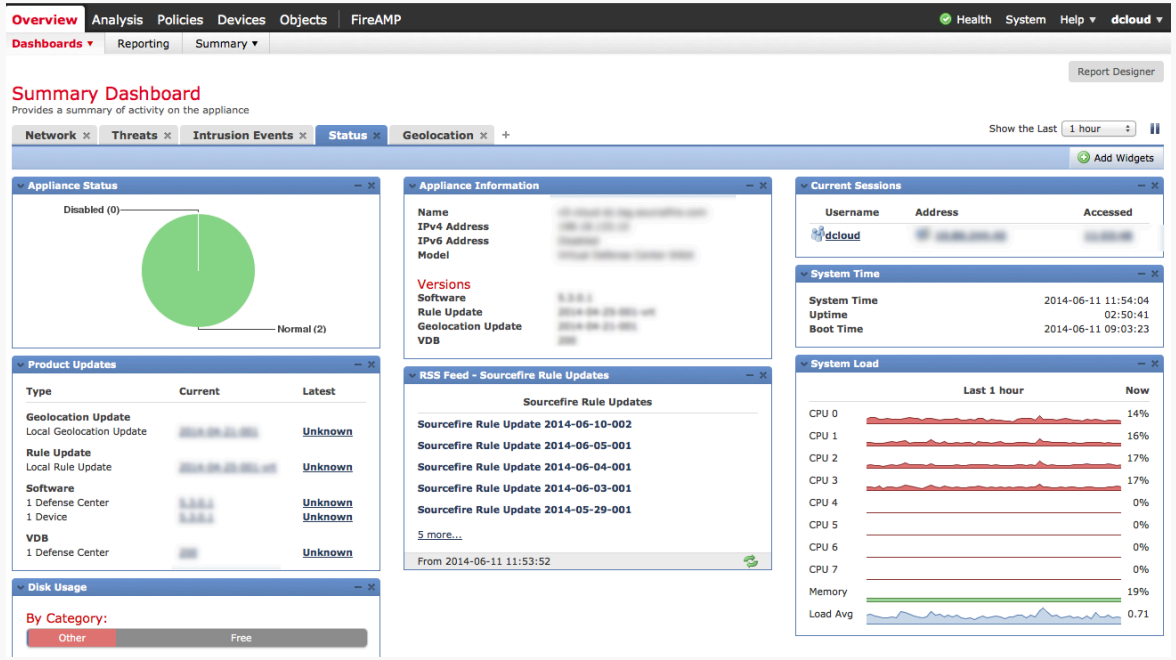
FortiGate



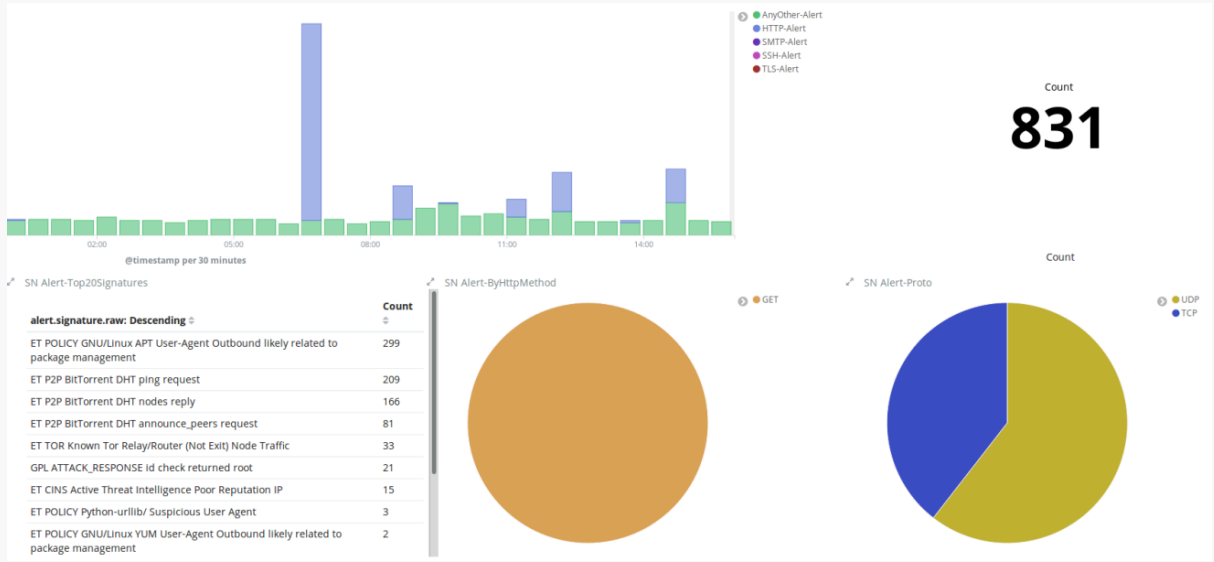
pfSense

IDS/IPS

Cisco Sourcefire

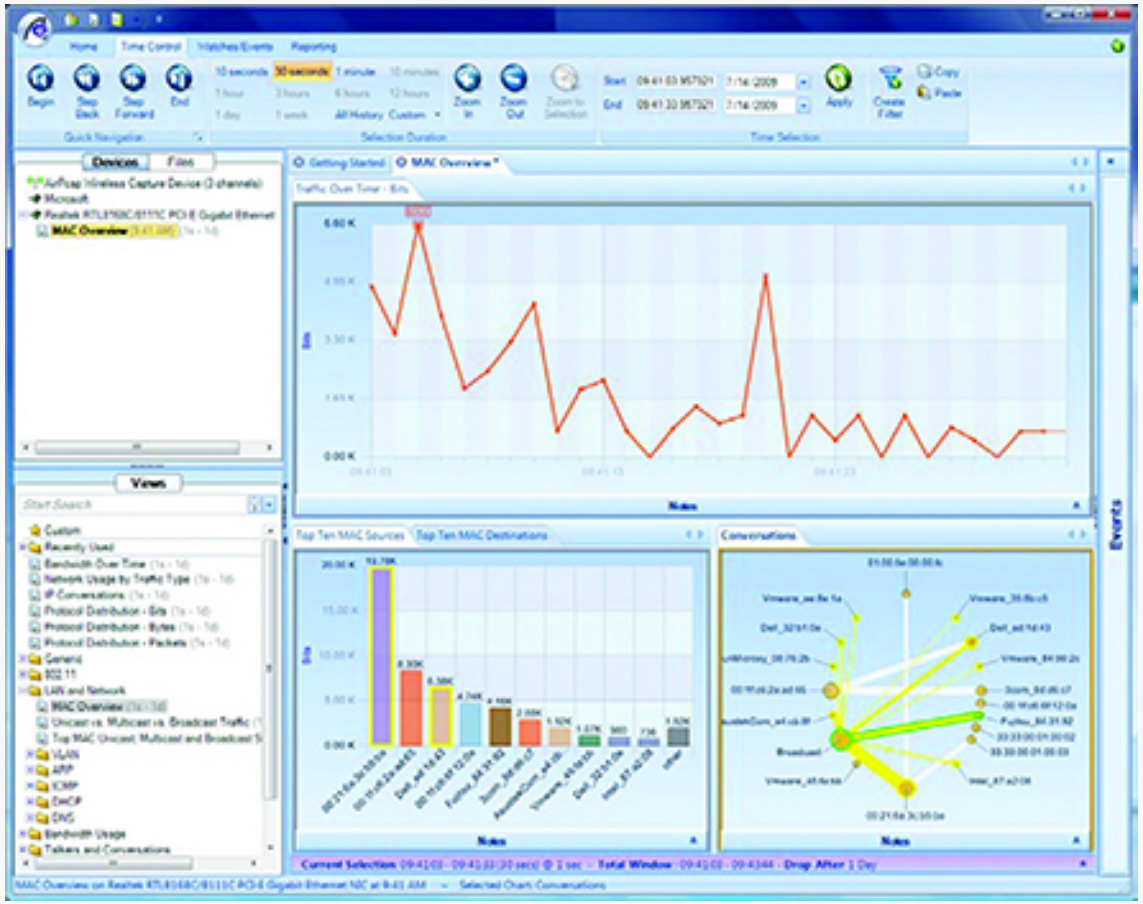


Suricata

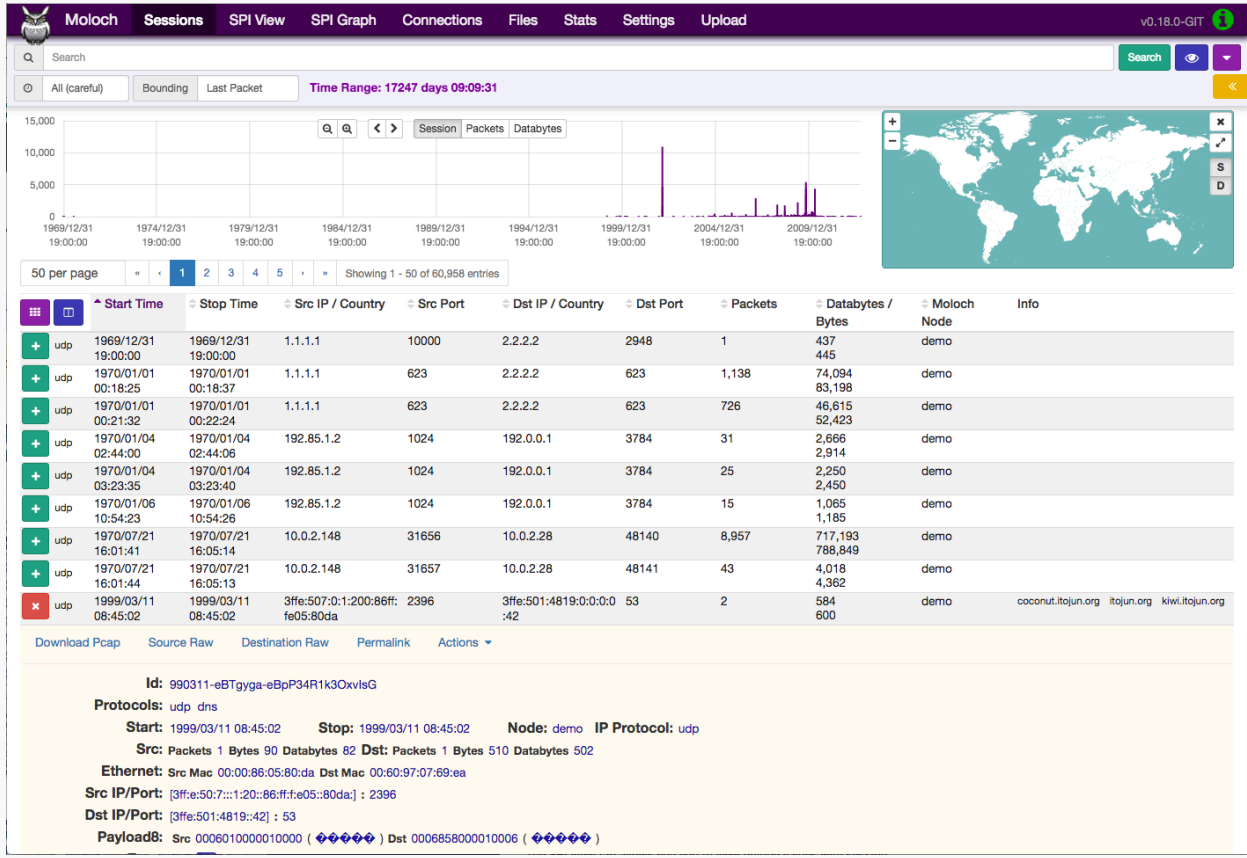


Packet Capture

Riverbed SteelCentral



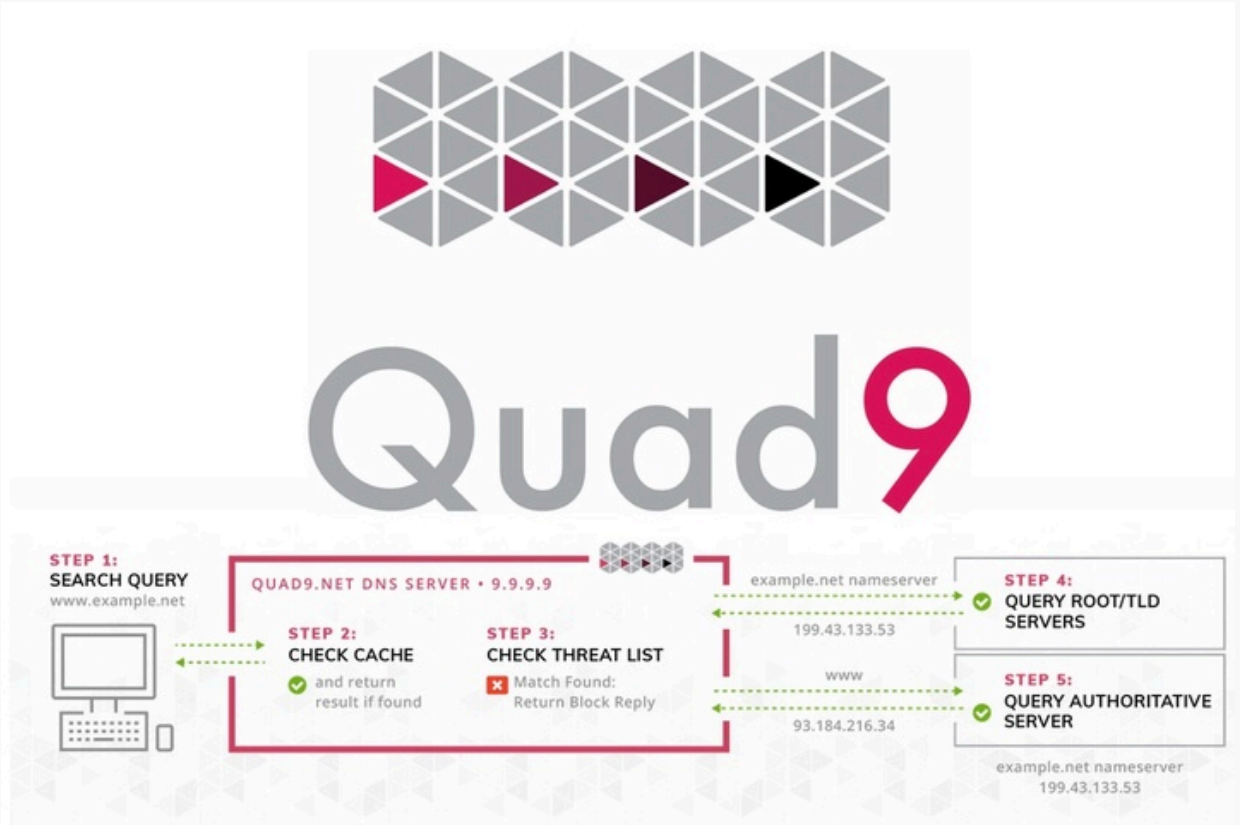
Moloch



DNS Security

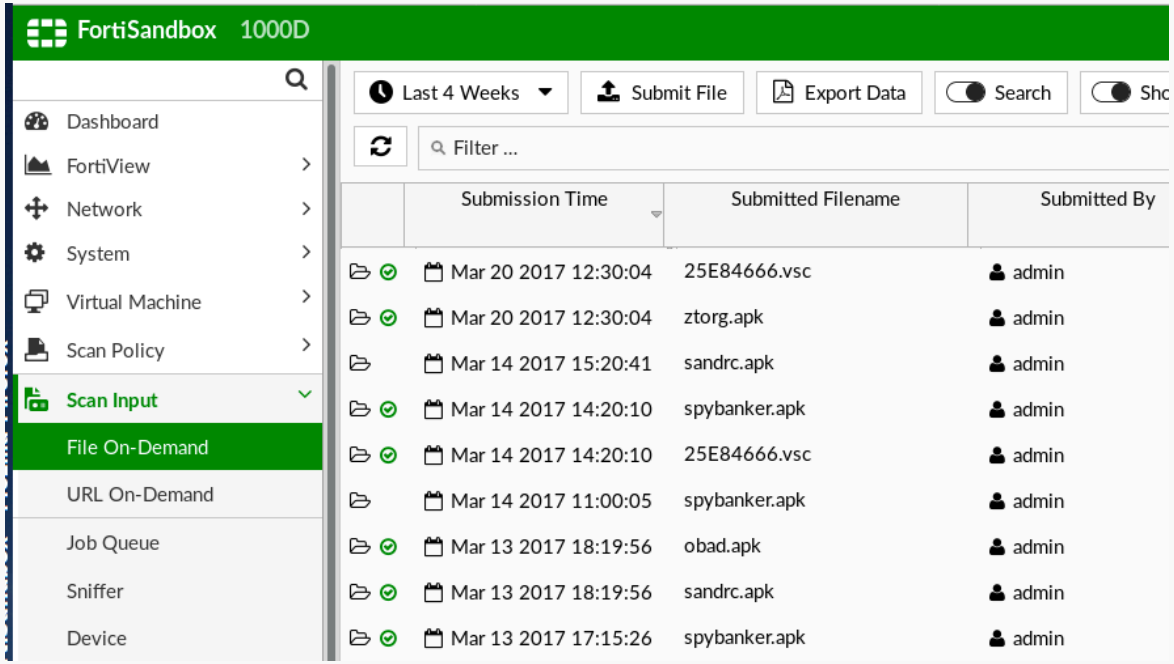
Cisco Umbrella

Quad9

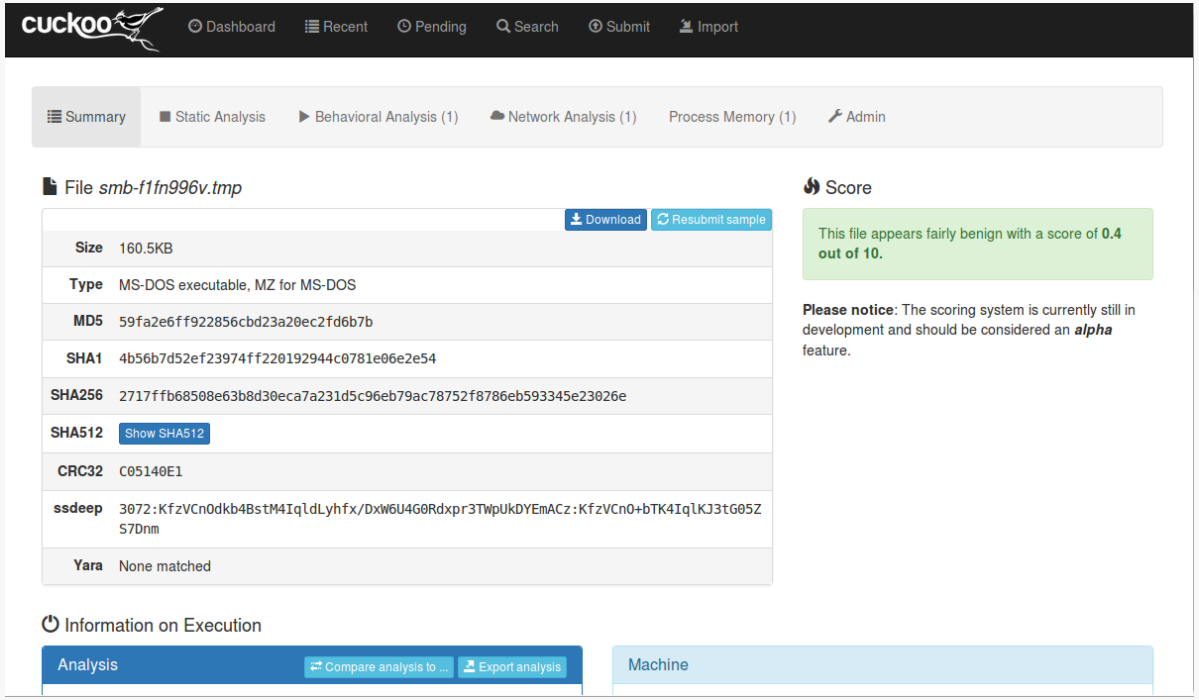


Malware Sandboxing

FortiSandbox

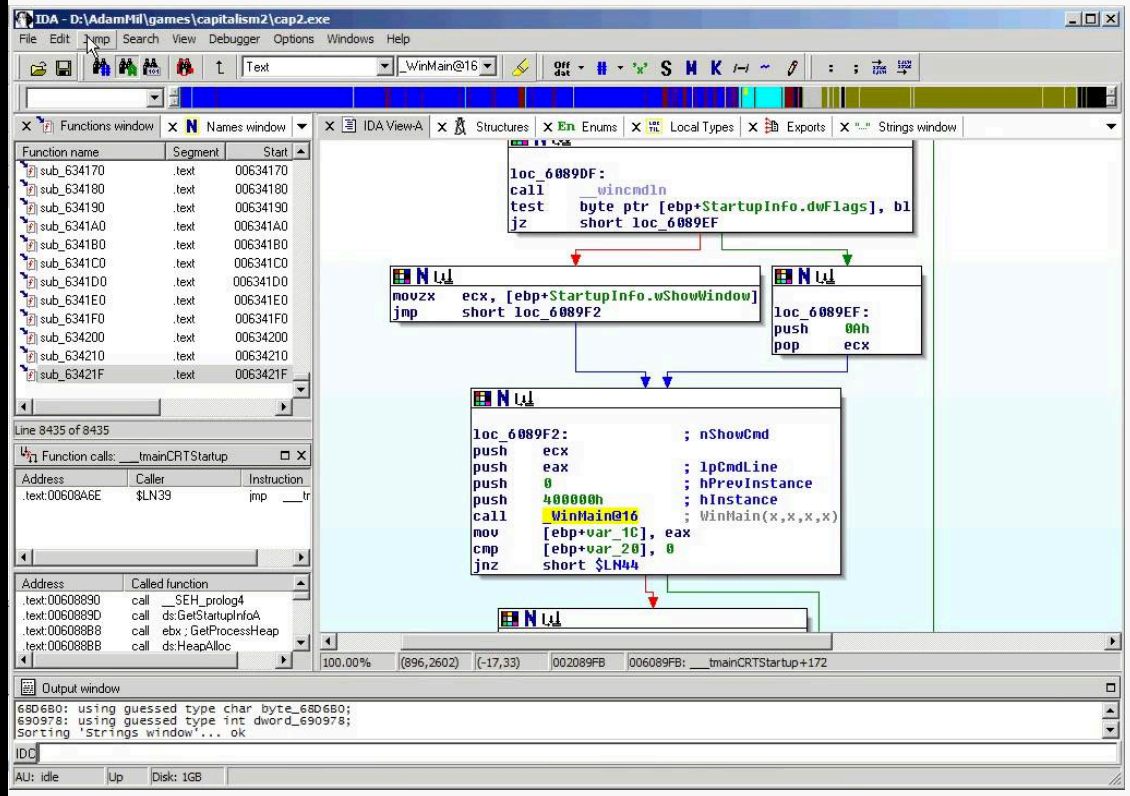


Cuckoo Sandbox

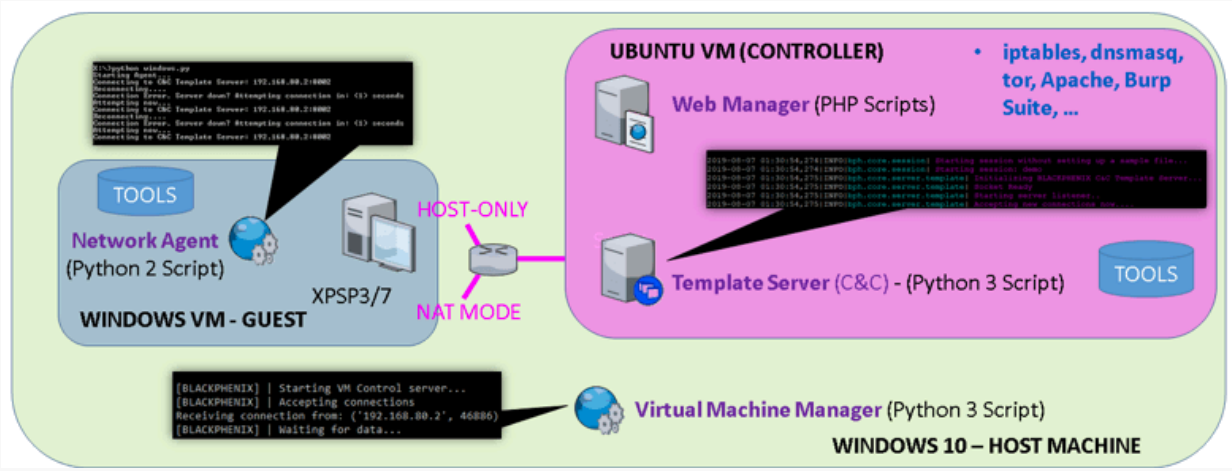


Malware Reverse Engineering

IDA Pro

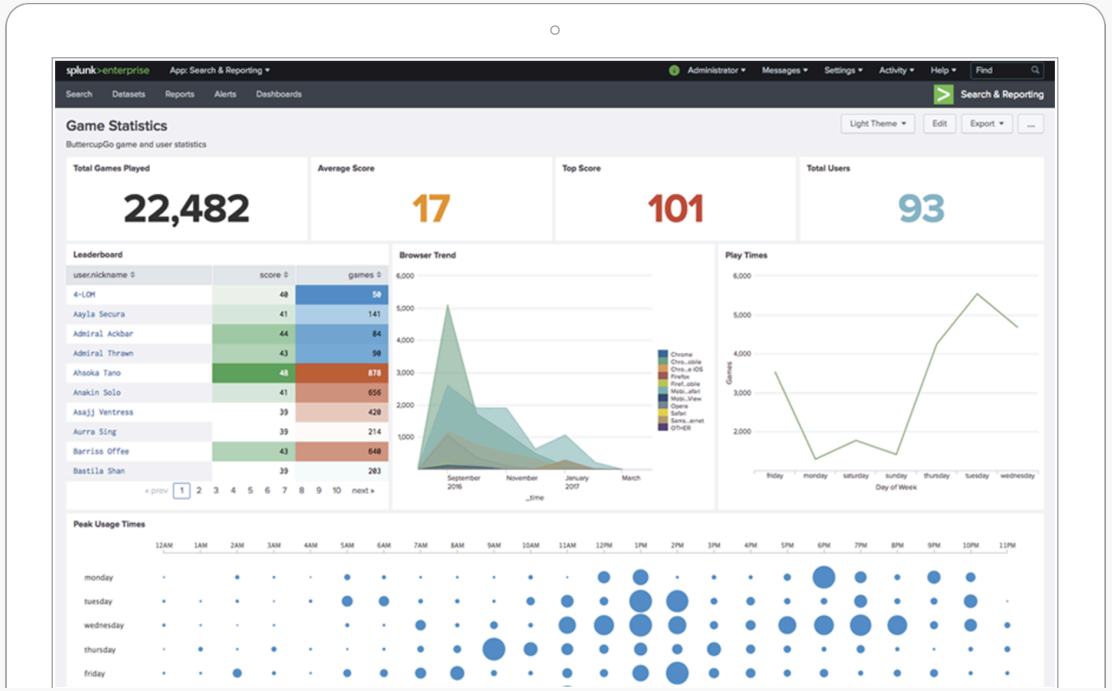


Blackphenix

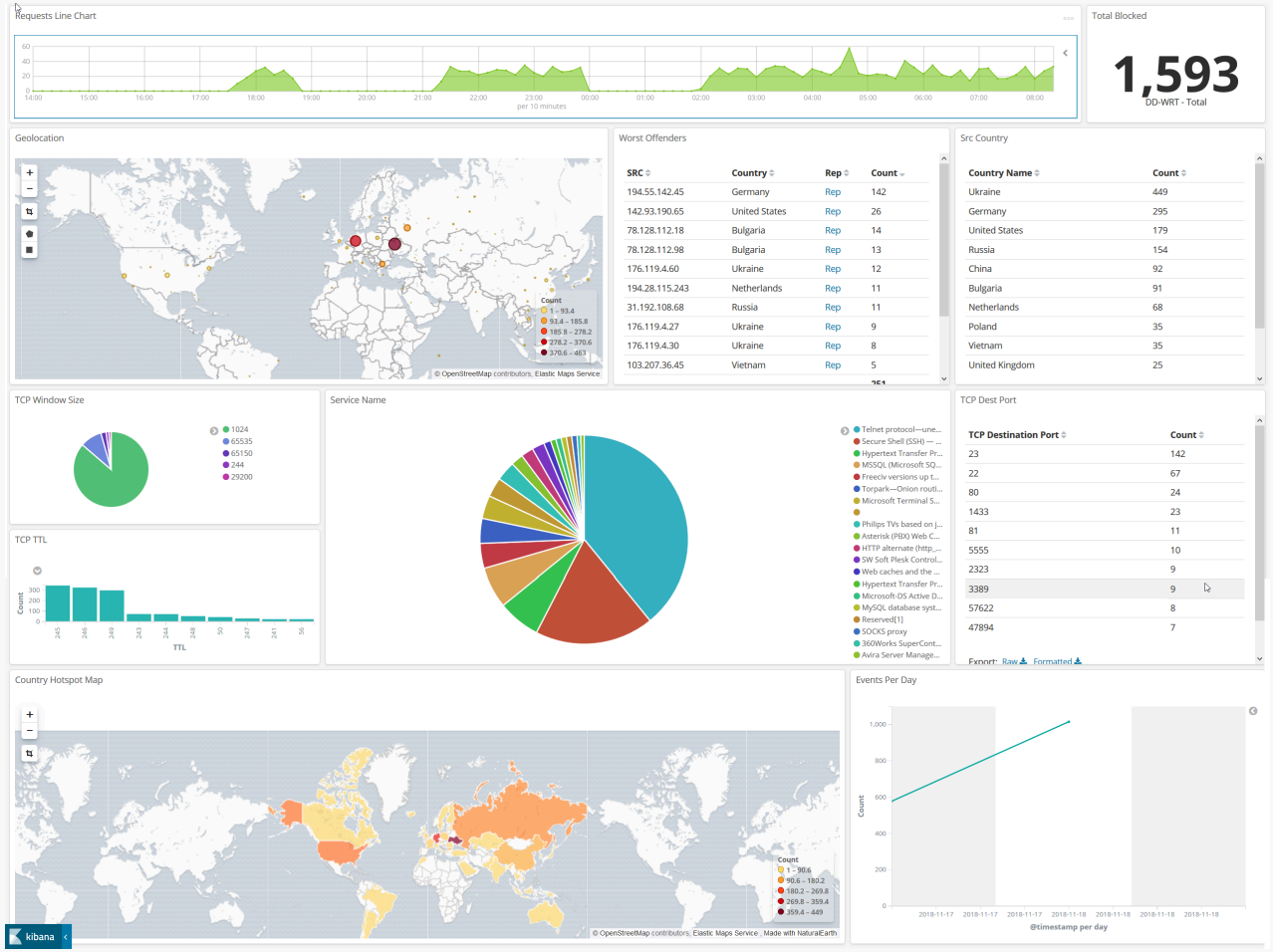


SIEM

Splunk

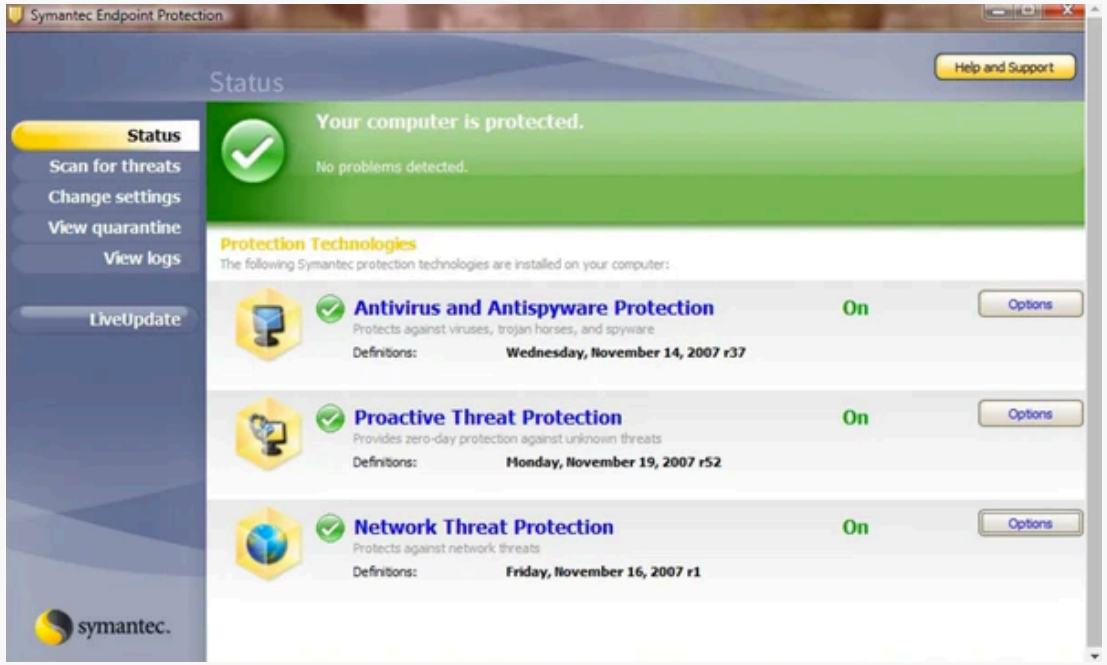


ELK（Elastic+Logstash+Kibana）

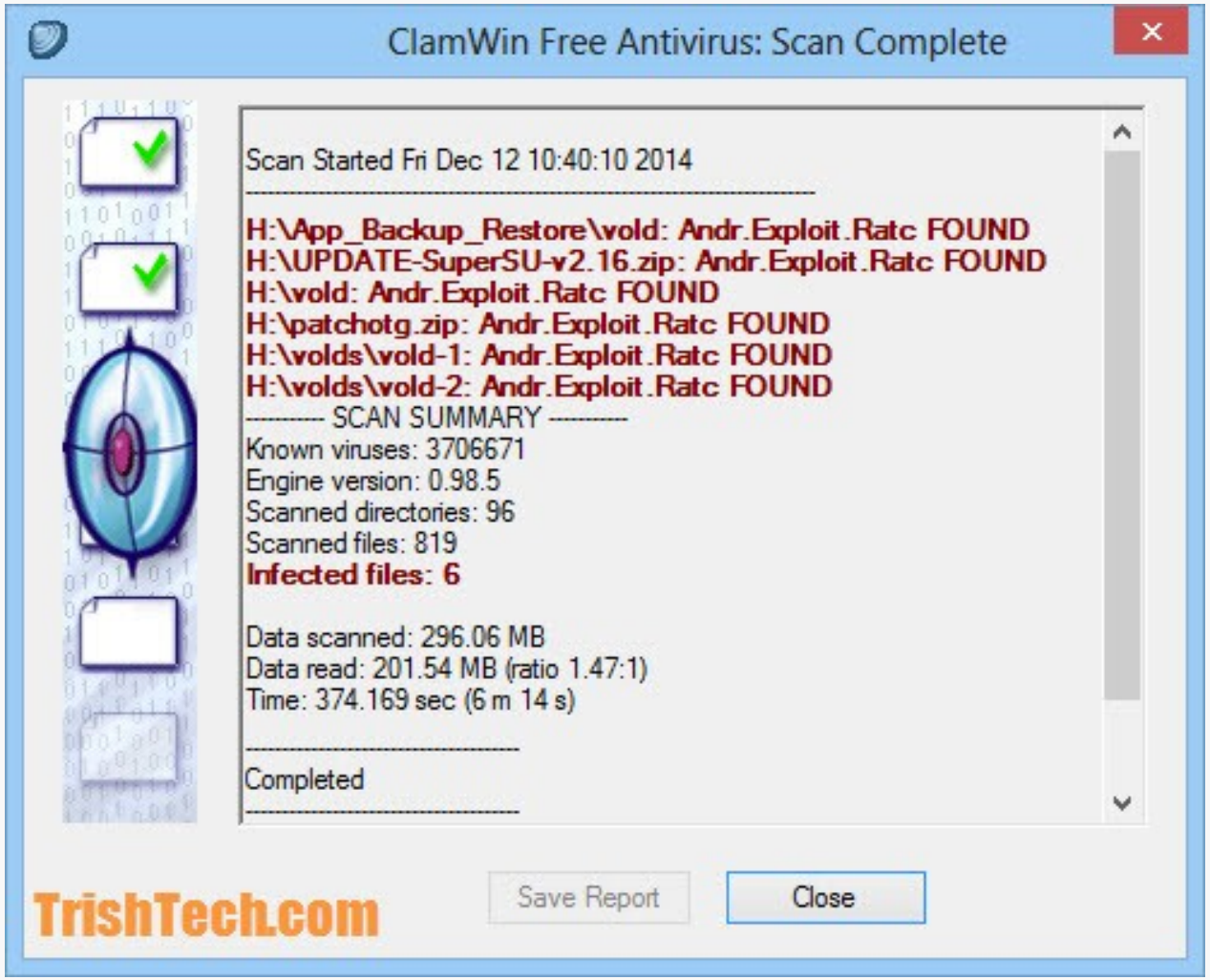


Antivirus

Symantec AV

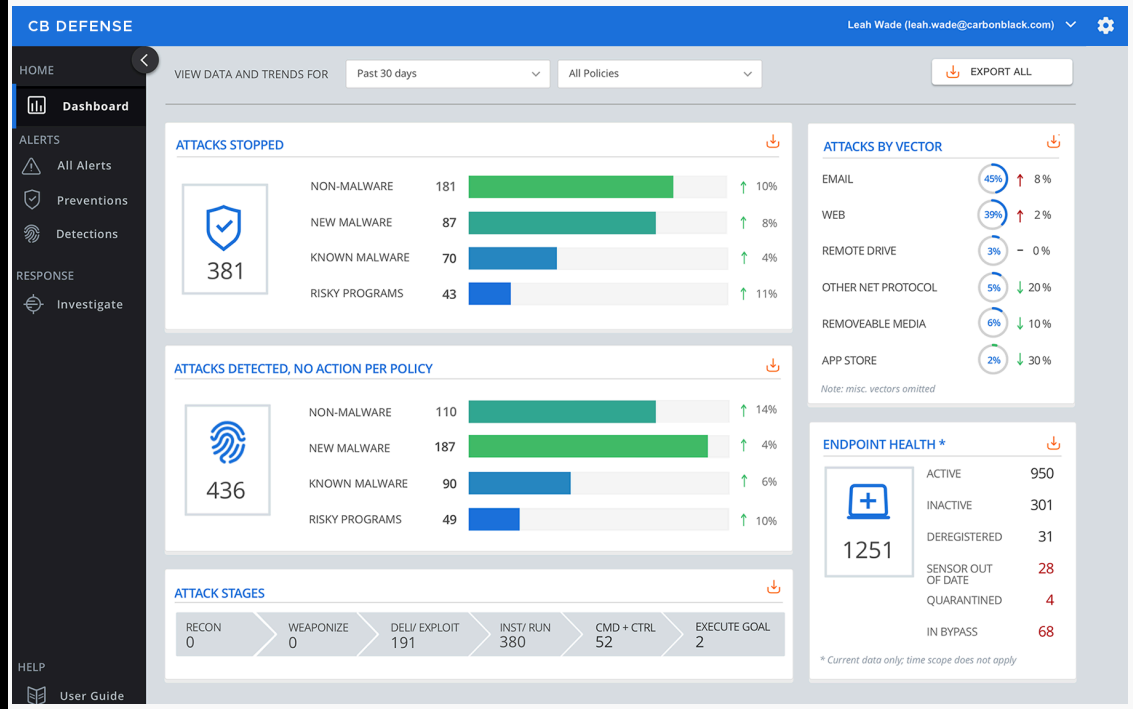


ClamAV

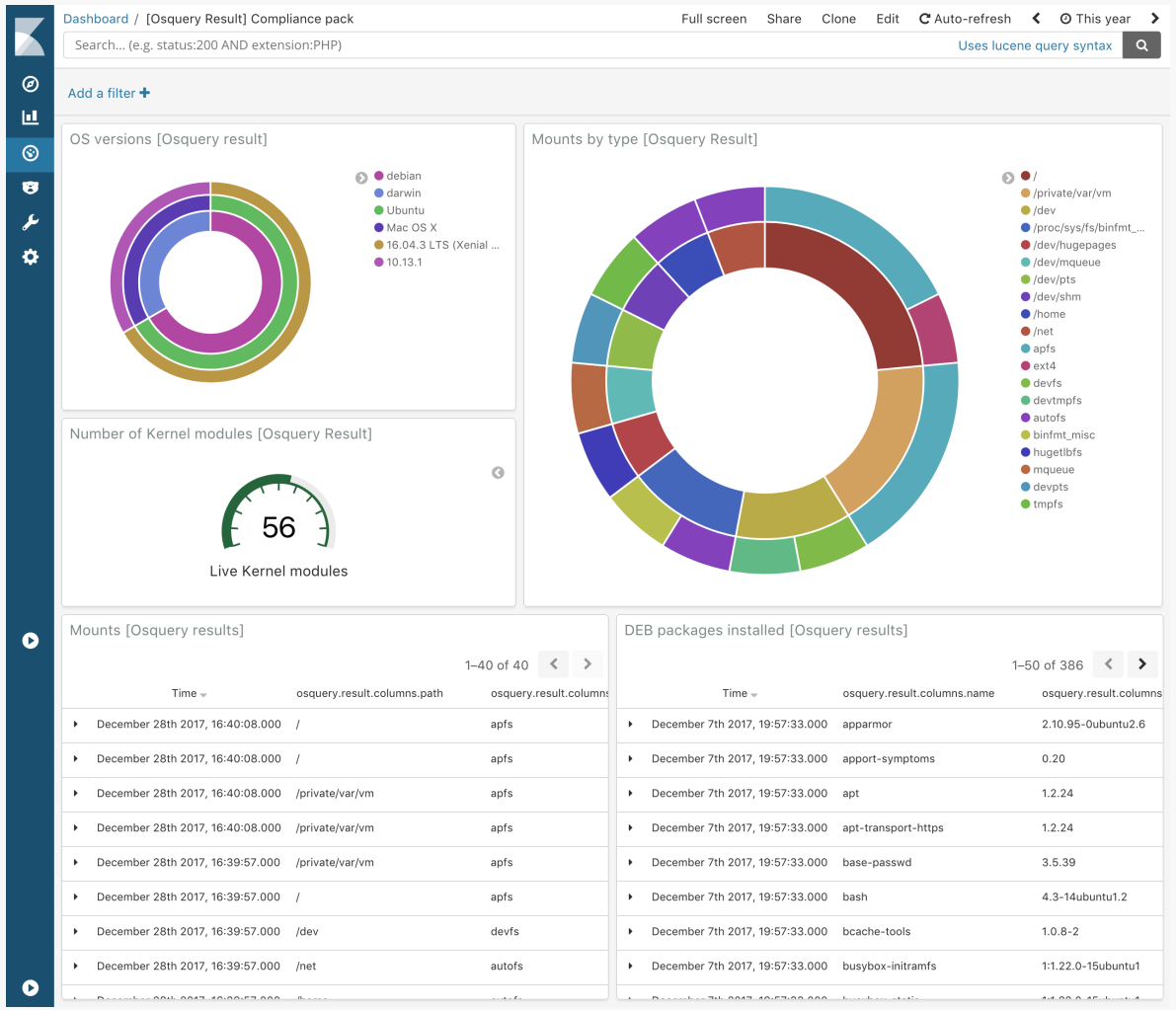


EDR – Endpoint Detection & Response

Carbon Black



osquery

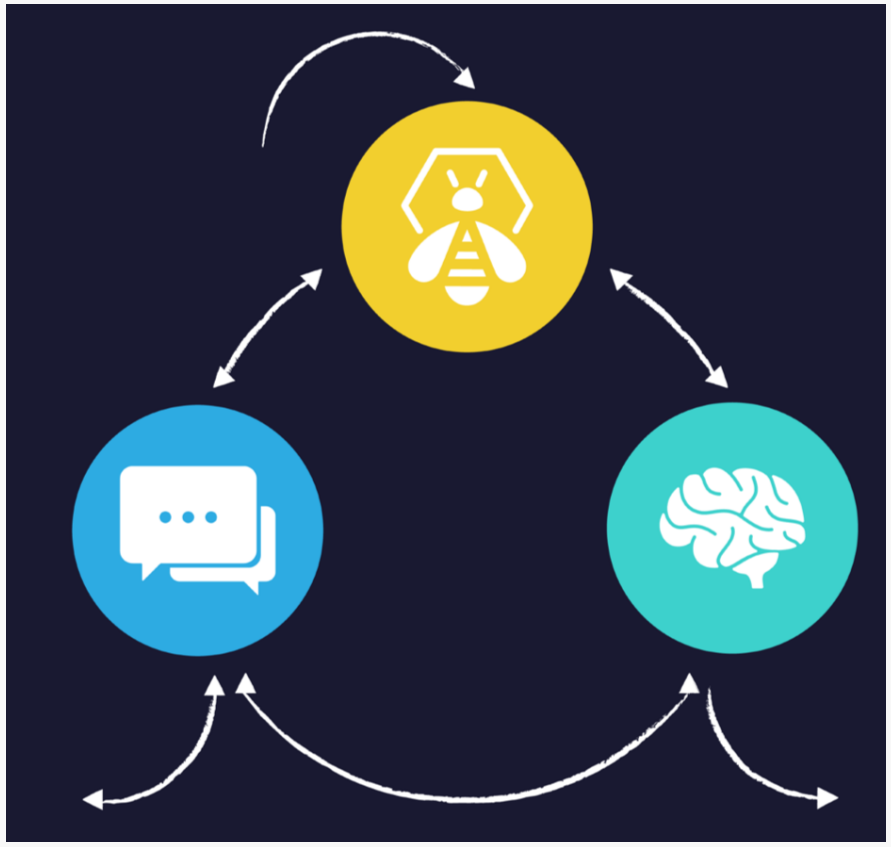


Case/Incident Management System

- Not a ticketing system
- Specific for Security Operations
- Tagging
- Classification
- Compliance Requirement

TheHive Project

- A 4–IN–1 SECURITY INCIDENT RESPONSE PLATFORM
- A scalable, open source and free Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly.



TheHive

- Collaborate in real-time
  - *SOAR (Security Orchestration, Automation, and Response)*
- Handle & respond to incidents
- Perform forensics analysis
- Organize, structure and archive incidents Corelate & merge incidents
- Gather & share IOCs with communities (using the native MISP integration)
- Custom case templates: incident workflows
- Augment your processes with metrics & custom fields
- Generate fully customizable dashboards: track activity, follow KPIs…
- Feeders: get alerts from MISP, CTI providers, SIEM, emails, …
- Triage & merge alerts
- Find similarities across cases & alerts
- Define observables as IOCs and/or sighted
- Audit trails
- REST API
- Webhook support

Cortex

- Observable analysis & active response engine
- Analyze using the Web UI or through the REST API
- Respond & take action
  - ***120+ Analyzers***
  - ***Responders***
- Use Python (or other languages supported by Linux) to write your own
- TheHive can leverage multiple Cortex instances Use MISP for additional analysis possibilities
- Multi-tenancy: Manage users and groups (organizations) Adjust TLP & PAP (Permissible Actions Protocol)
- Jobs history
- Cache jobs & reports
- Custom rate limiting for each analyzer
- Can use Docker to run analyzers and responders

Analyzers

- Programs for processing observables and delivering reports
- Input: observable + metadata
- Output:
  - *Summary report*
  - *Long report*
  - *Observables (optional)*
- Ex: get the VirusTotal report for a given hash/file

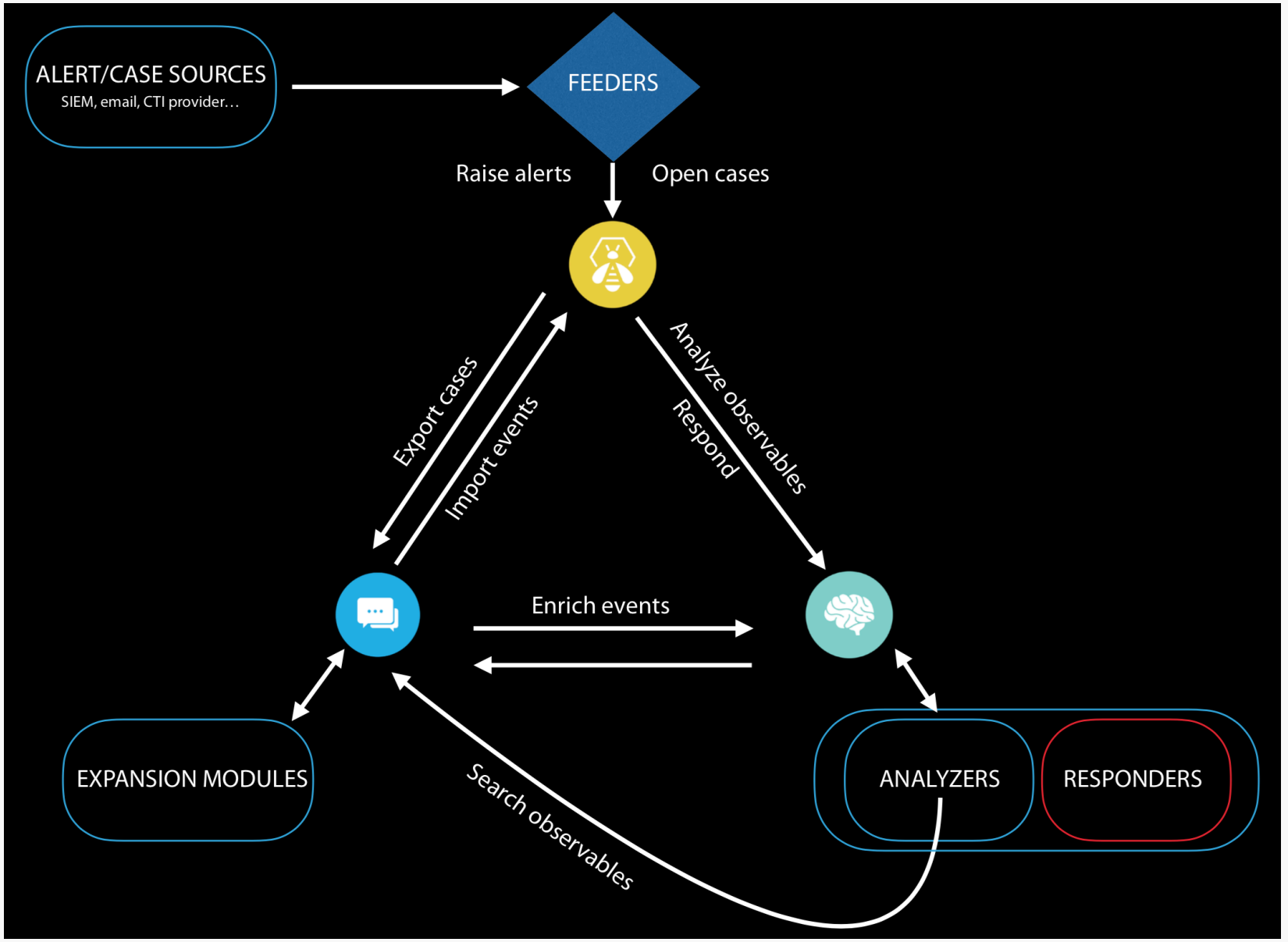
Responders

- Programs to take action at the Alert, Case, Task, Log or Observable level
- Input: data and metadata
- Output: Success Failute
  - *Operations : ex: "Add tag in case", "Add tag in Observables"*
- Mostly customer–specific
- Ex.
  - *Block a set of malicious URLs*
  - *Reply to a user notification*

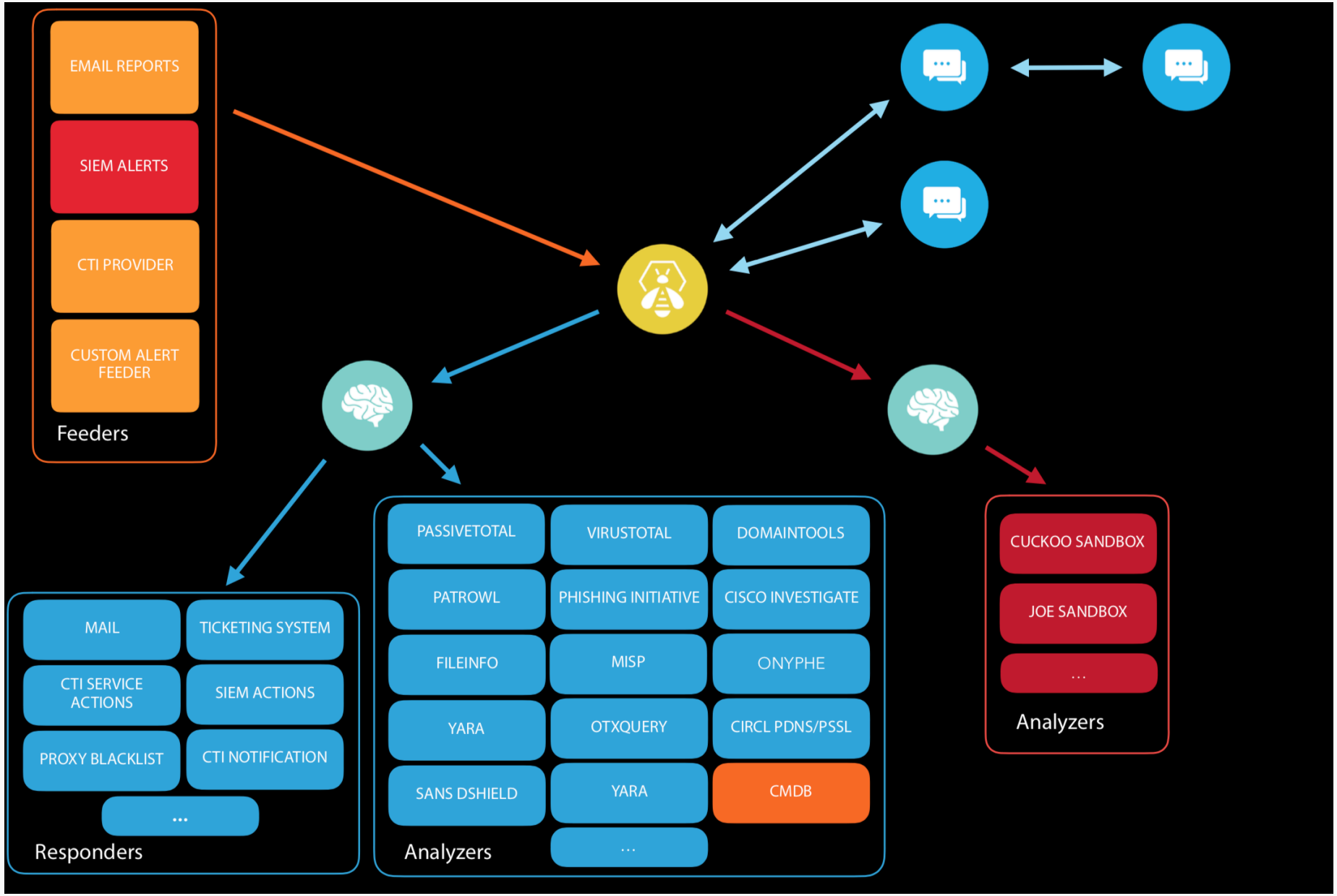
MISP (Malware Information Sharing Platform)

- MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing
- The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators.
- A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter–terrorism information.

Typical Integration



Real-World Example



Demo

Pros vs. Cons – Open–Source in the Enterprise

Advantages

- Better Access to Innovation
- Scalable
- At times Free
- Can be tailored/customize to the company
- No Vendor lock–in
  - *No need to waste time with sales, TACs, etc.*
- Higher Quality Software
- Attract better talent
- Greater Security
- Better Security

Disadvantages

- Hire the right individuals
- You must have many CTI Subscriptions
- Not easy to setup
- Need equipment
- In–house support (nightmare)
- No User Friendly
- No Easy to use
- Lots of Bugs
- Cost
  - *Equipment*
  - *Maintenance*
  - *Employees*
  - *Training*

Contribute!!!! Don’t be a Fool

- If you use it, contribute to the project
- If you don’t know how to contribute, ask!!!
- If you are using the tool for commercial use, don’t expect full support and fast resolution
  - *Tool owners have a life, family, etc.*
- Donate!!!!!!

References

- https://opensource.com/resources/what-open-source
- https://en.wikipedia.org/wiki/Open_source
- https://en.wikipedia.org/wiki/Open-source_license
- https://www.fortinet.com/products/next-generation-firewall.html
- https://www.pfsense.org/
- https://www.cisco.com/c/dam/global/th_th/assets/docs/seminar/Sourcefire_Next_Generation_IPS_Datasheet.pdf
- https://suricata-ids.org/
- https://www.riverbed.com/products/steelcentral/network-performance-management/packet-capture-solutions.html
- https://molo.ch/
- https://umbrella.cisco.com/
- https://www.quad9.net/
- https://www.fortinet.com/products/sandbox/fortisandbox.html
- https://cuckoosandbox.org/
- https://www.hex-rays.com/products/ida/
- https://www.fortinet.com/blog/threat-research/blackhat-black-phenix-framework.html
- https://www.splunk.com/
- https://www.elastic.co/
- Symantec Endpoint Security | Symantec
- https://www.symantec.com › products › endpoint
- https://www.clamav.net/
- https://www.carbonblack.com/products/cb-response/
- https://osquery.io/
- https://www.computerworld.com/article/3412269/what-are-the-advantages-of-open-source-software-in-the-enterprise-.html#slide8
- https://thehive-project.org/
- https://www.misp-project.org/index.html

Questions???

THANK YOU!!!!

Marco Palacios

Twitter: @MPalacios__Cyber

marco.palacios.cyber@gmail.com

LinkedIn: /in/marcopalacios

Slack: Margraf