

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*



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.*

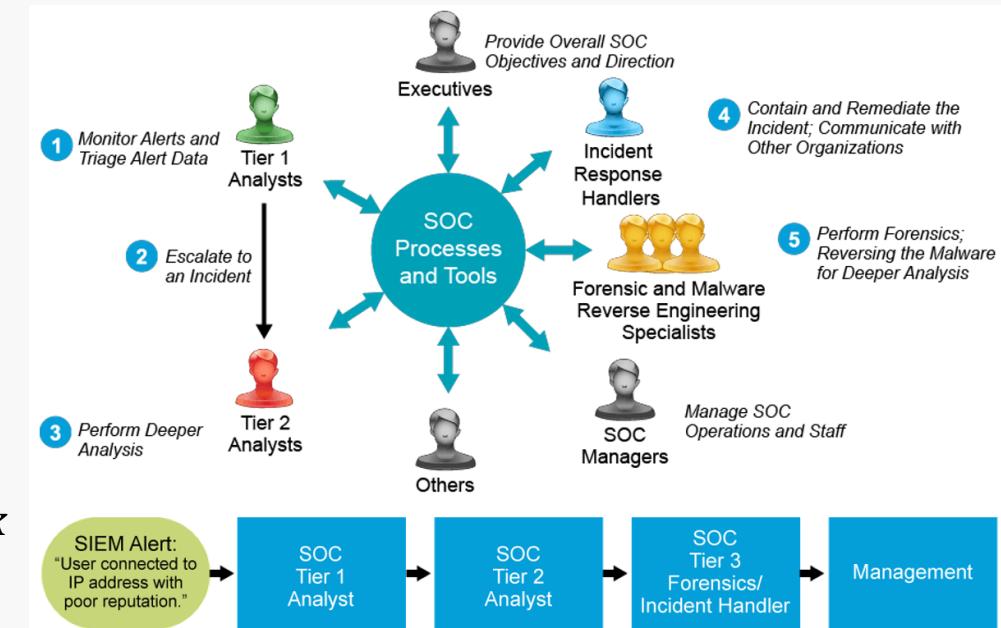
Security Operations Center (SOC)

- 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*



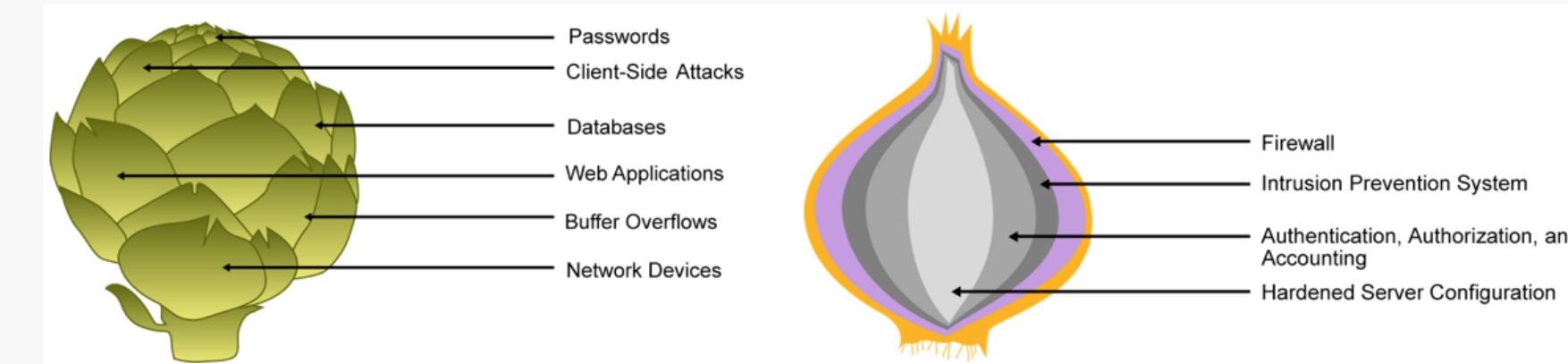
Roles in a SOC

- Tier 1
 - Continuously monitors the alert queue
 - Triage 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

The screenshot shows the FortiGate VM64 dashboard at 192.168.1.1/ng/system/dashboard/1. The left sidebar includes links for Status, Security, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, Log & Report, and Monitor. The main area displays:

- System Information:** Hostname: FortiGate-VM64, Serial Number: FGVMEVCRJDKQIM6D, Firmware: v6.2.1 build0932 (GA), Mode: NAT, System Time: 2019/08/27 12:52:54, Uptime: 00:00:27:39, WAN IP: Unknown.
- Licenses:** FortiCare Support, Firmware & General Updates, IPS, AntiVirus, Web Filtering.
- Virtual Machine:** Allocated vCPUs: 1/1 (100%), Allocated RAM: 1002 MIB / 1 GiB (98%).
- FortiGate Cloud:** Status: Not Supported.

pfSense

The screenshot shows the pfSense Status / Dashboard at 192.168.1.1/. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main area displays:

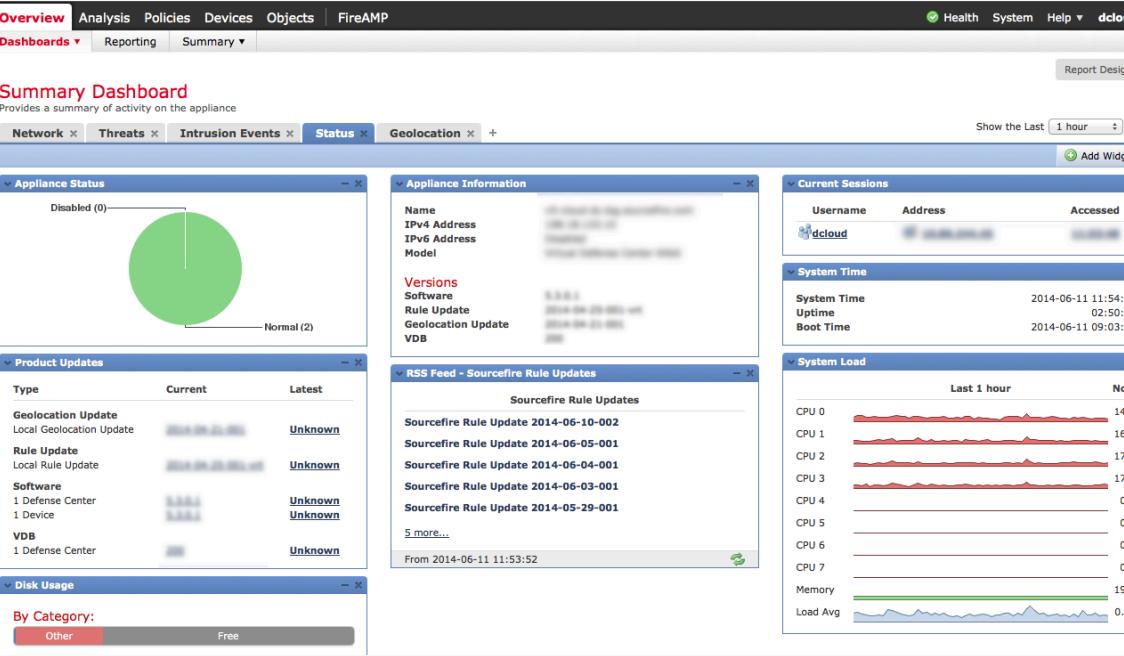
- System Information:** Name: pfSense.localdomain, System: Netgate SG-4860, Version: 2.3.3-DEVELOPMENT (amd64), Platform: pfSense, CPU Type: Intel(R) Atom(TM) CPU C2558 @ 2.40GHz, Hardware crypto: AES-CBC,AES-XTS,AES-GCM,AES-ICM, Uptime: 6 Days 17 Hours 23 Minutes 42 Seconds, Current date/time: Mon Oct 10 12:43:53 EDT 2016.
- Thermal Sensors:** Core 3: 39.0 °C, Core 2: 39.0 °C, Core 1: 38.0 °C, Core 0: 39.0 °C.
- Interfaces:** WAN, LAN, L1, L2, L3, L4, LAN3 (autoselect).
- Rss:** pfSense 2.3.2-p1 RELEASE Now Available!, pfSense 2.4 pre-alpha snapshots now available., pfSense 2.3.2-RELEASE Now Available!, pfSense moves to Apache License.
- Traffic Graphs:** wan (in: 0.0, out: 20k).
- Services Status:** Services listed include avahi, bsnmpd, dhcpcd, dplinger, ipsec, ntpd, sshd, unbound, all marked as running (green checkmark).

At the bottom, it says: pfSense is © 2004 - 2016 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license].

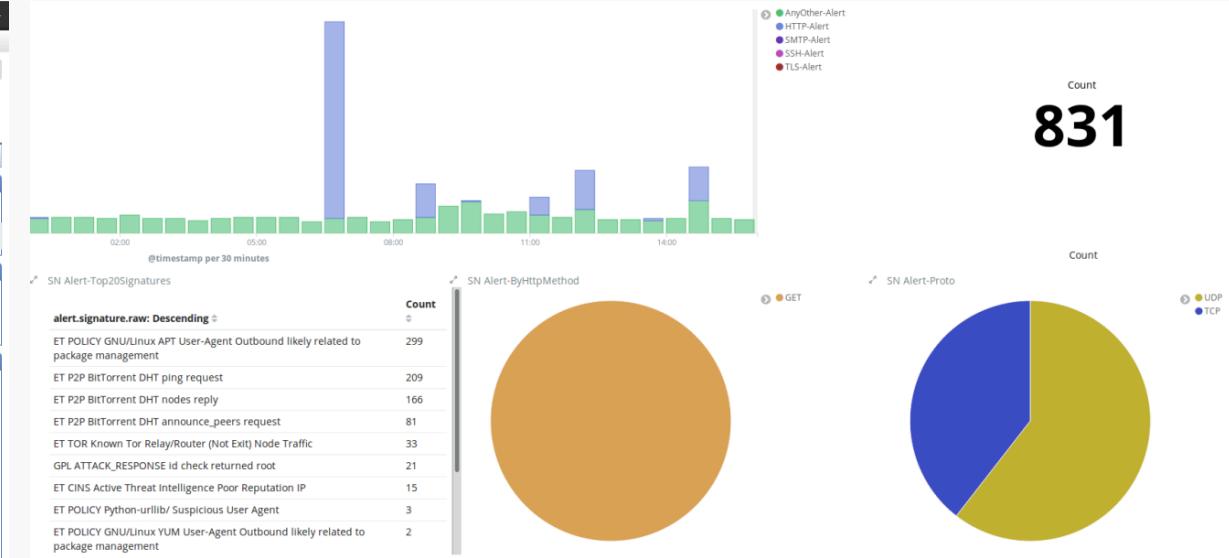


IDS/IPS

Cisco Sourcefire



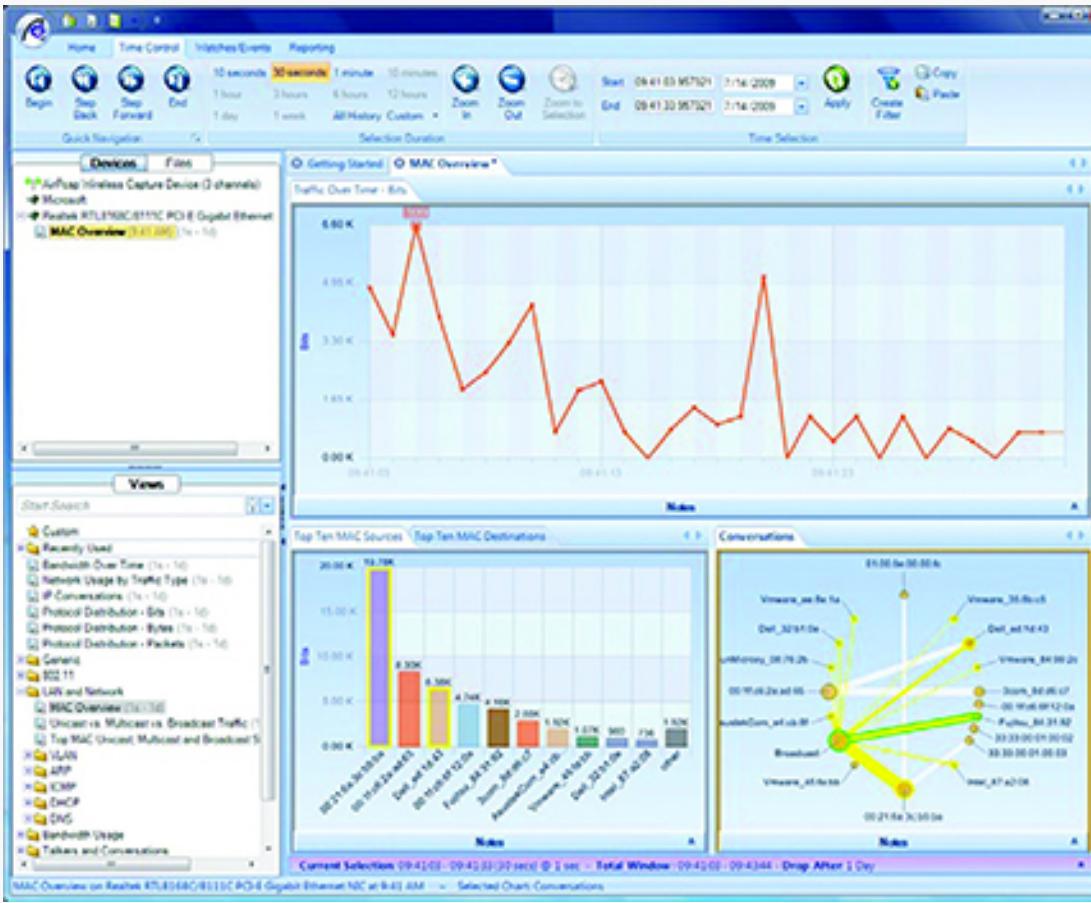
Suricata



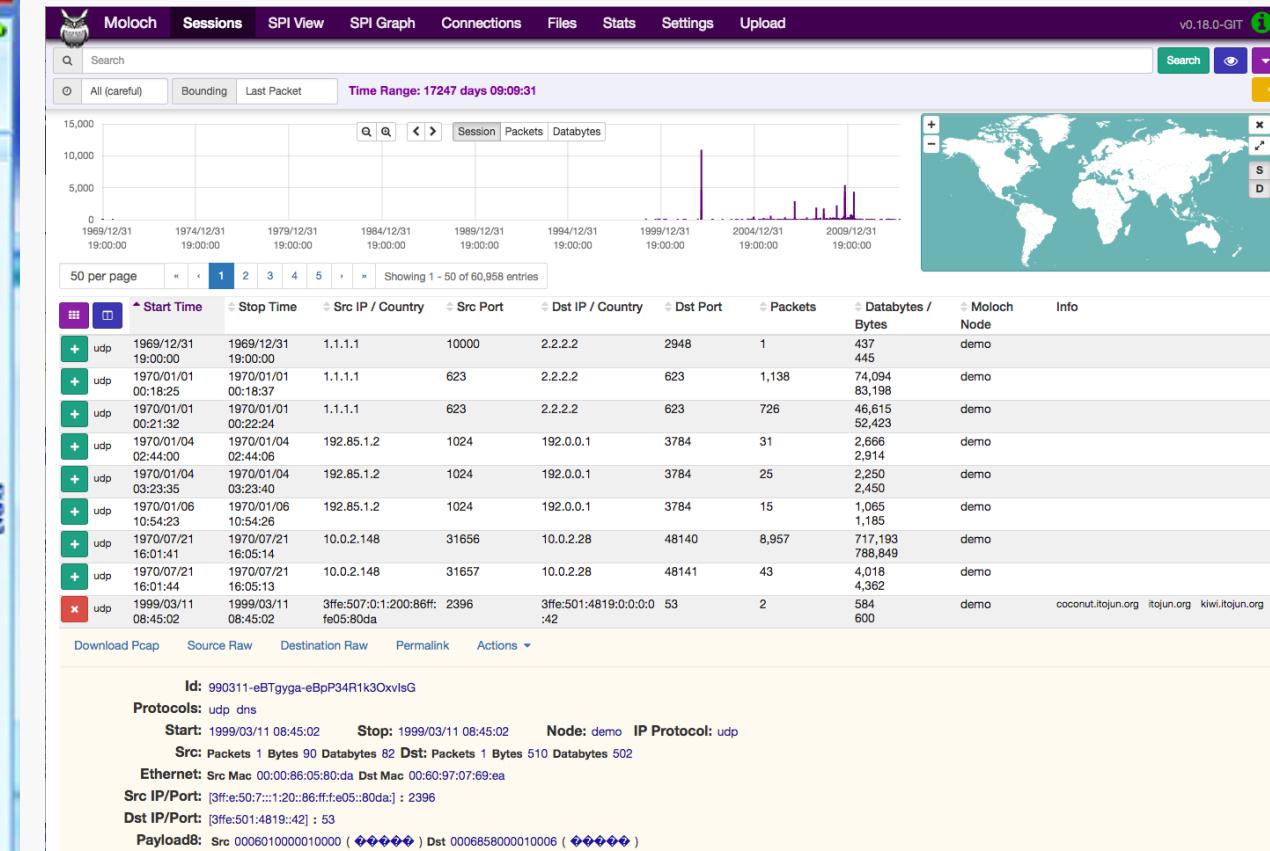


Packet Capture

Riverbed SteelCentral



Moloch





DNS Security

Cisco Umbrella



Quad9



Malware Sandboxing

FortiSandbox

The screenshot shows the FortiSandbox 1000D interface. At the top, there's a navigation bar with links for Dashboard, FortiView, Network, System, Virtual Machine, Scan Policy, Scan Input (which is currently selected), File On-Demand, URL On-Demand, Job Queue, Sniffer, and Device. Below the navigation bar is a search and filter section with dropdowns for 'Last 4 Weeks' and 'Search', and buttons for 'Submit File', 'Export Data', and 'Search'. A table lists submitted files with columns for Submission Time, Submitted Filename, and Submitted By. The table contains the following data:

| | Submission Time | Submitted Filename | Submitted By |
|---|----------------------|--------------------|--------------|
| 1 | Mar 20 2017 12:30:04 | 25E84666.vsc | admin |
| 2 | Mar 20 2017 12:30:04 | ztorg.apk | admin |
| 3 | Mar 14 2017 15:20:41 | sandrc.apk | admin |
| 4 | Mar 14 2017 14:20:10 | spybanker.apk | admin |
| 5 | Mar 14 2017 14:20:10 | 25E84666.vsc | admin |
| 6 | Mar 14 2017 11:00:05 | spybanker.apk | admin |
| 7 | Mar 13 2017 18:19:56 | obad.apk | admin |
| 8 | Mar 13 2017 18:19:56 | sandrc.apk | admin |
| 9 | Mar 13 2017 17:15:26 | spybanker.apk | admin |

Cuckoo Sandbox

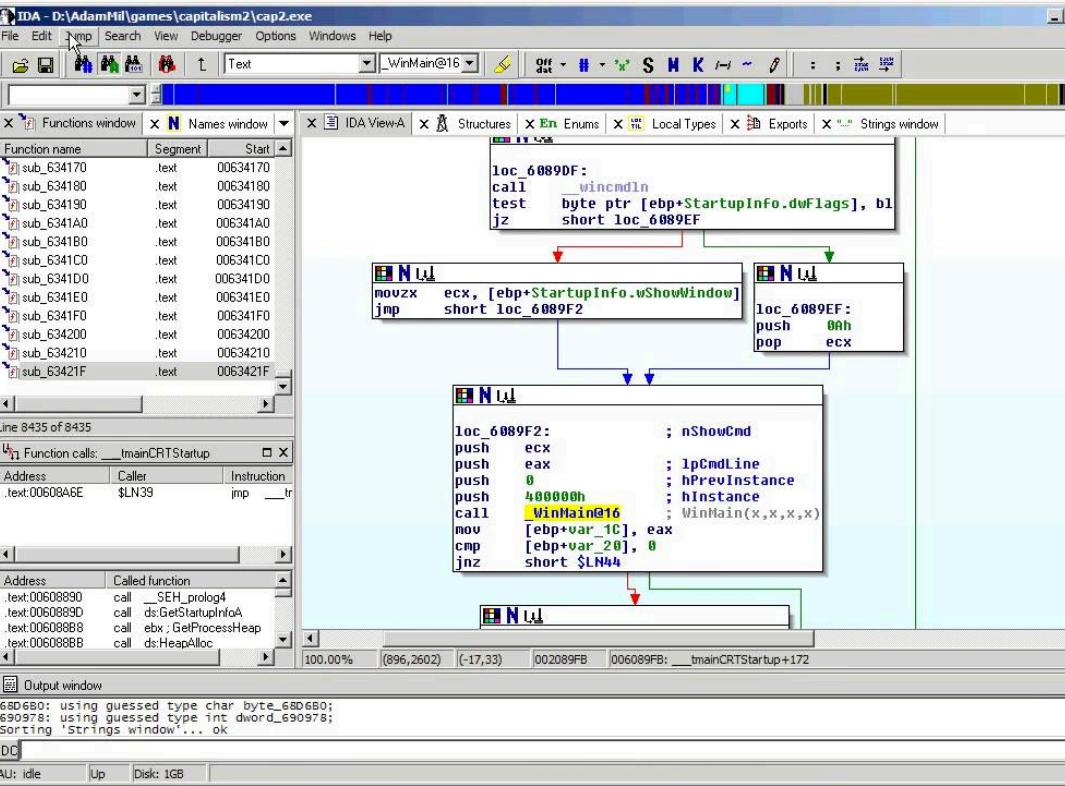
The screenshot shows the Cuckoo Sandbox interface. At the top, there's a navigation bar with links for Dashboard, Recent, Pending, Search, Submit, and Import. Below the navigation bar is a summary bar with tabs for Summary, Static Analysis, Behavioral Analysis (1), Network Analysis (1), Process Memory (1), and Admin. The main area displays analysis results for a file named 'File smb-f1fn996v.tmp'. The summary table includes the following data:

| Size | 160.5KB |
|--------|--|
| Type | MS-DOS executable, MZ for MS-DOS |
| MD5 | 59fa2e6ff922856cbd23a20ec2fd6b7b |
| SHA1 | 4b56b7d52ef23974ff220192944c0781e06e2e54 |
| SHA256 | 2717ffb68508e63b8d30eca7a231d5c96eb79ac78752f8786eb593345e23026e |
| SHA512 | Show SHA512 |
| CRC32 | C05140E1 |
| ssdeep | 3072:KfzVCn0dkb4BstM4IqlLyhfx/DxW6U4G0Rdxpr3TwplKDYEmACz:KfzVCn0+bTK4IqlKJ3tG05Z S7Dnm |
| Yara | None matched |

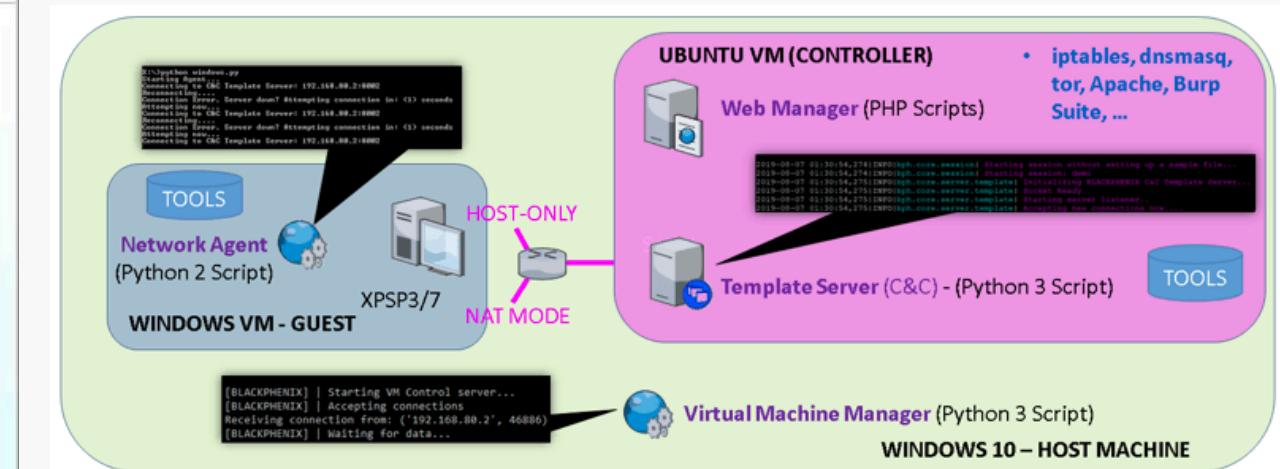
To the right of the analysis table is a 'Score' section with a green box stating: "This file appears fairly benign with a score of 0.4 out of 10." Below the analysis table is a section titled "Information on Execution" with tabs for Analysis (selected), Compare analysis to..., Export analysis, and Machine.

Malware Reverse Engineering

IDA Pro



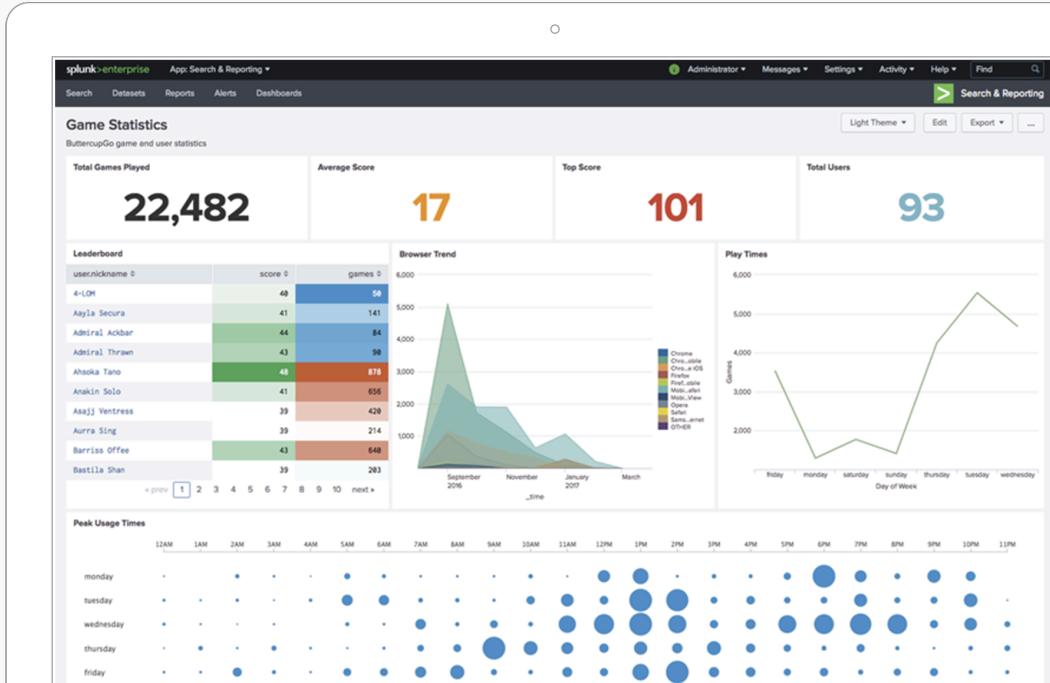
Blackphenix



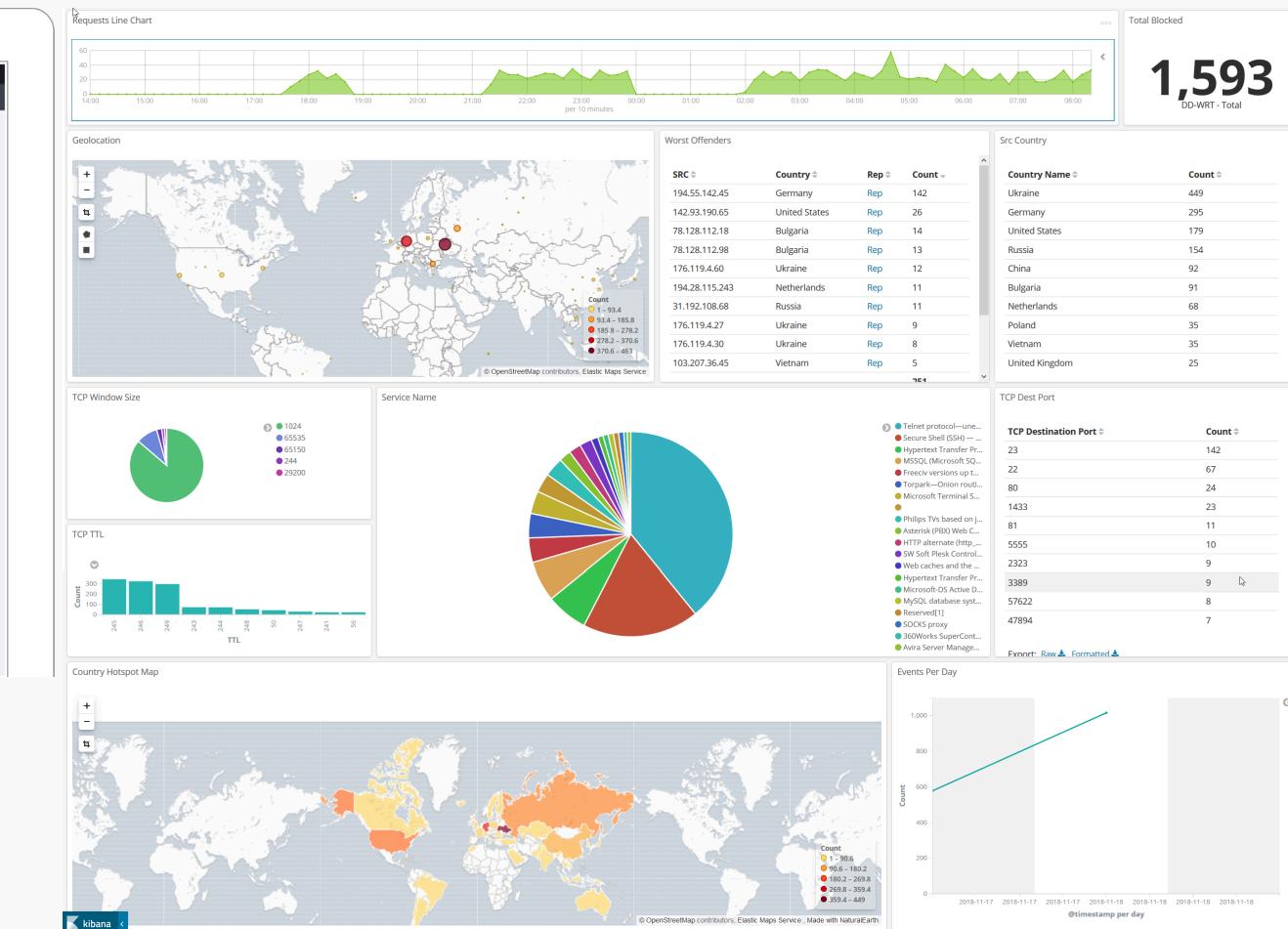


SIEM

Splunk



ELK (Elastic+Logstash+Kibana)

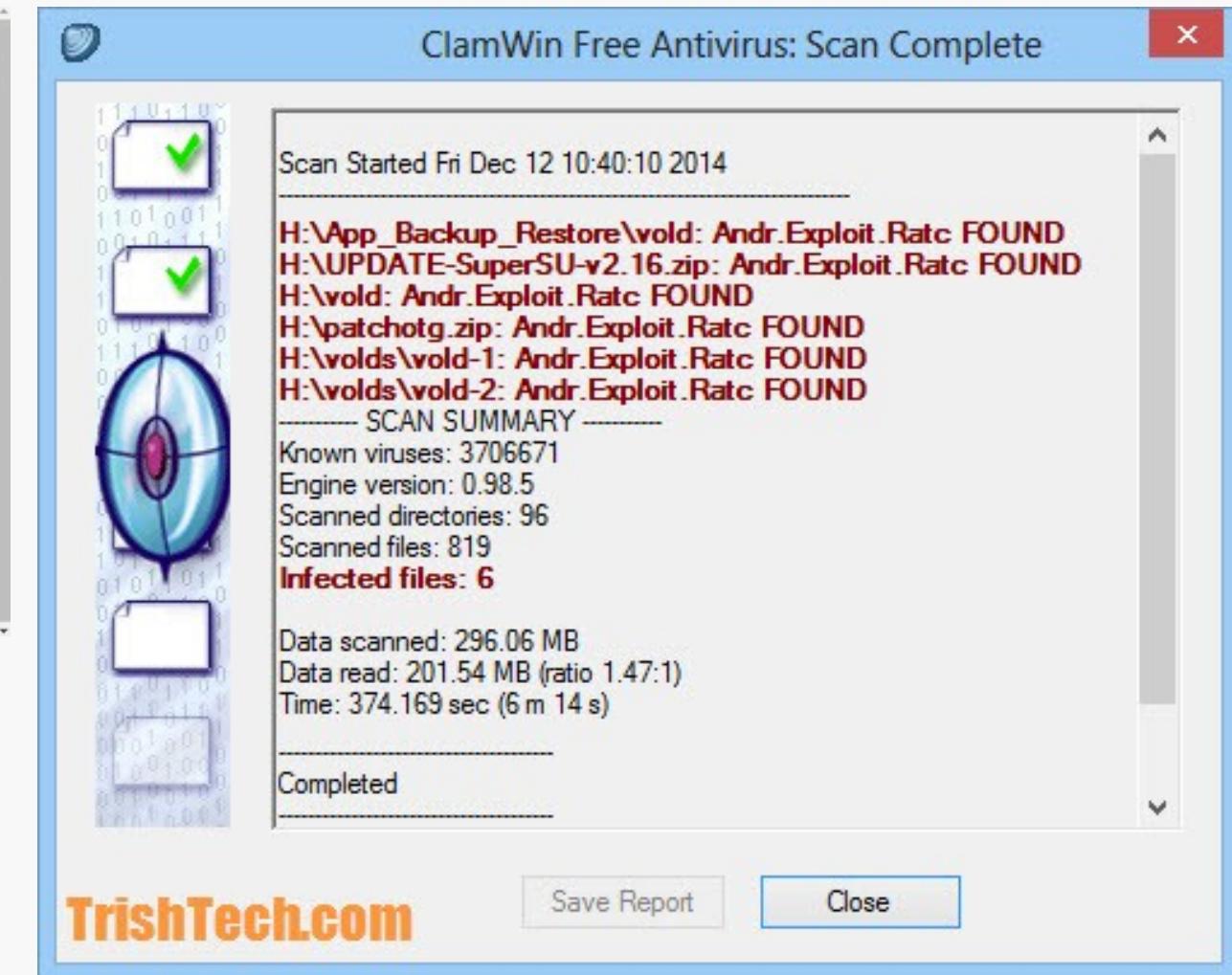


Antivirus

Symantec AV

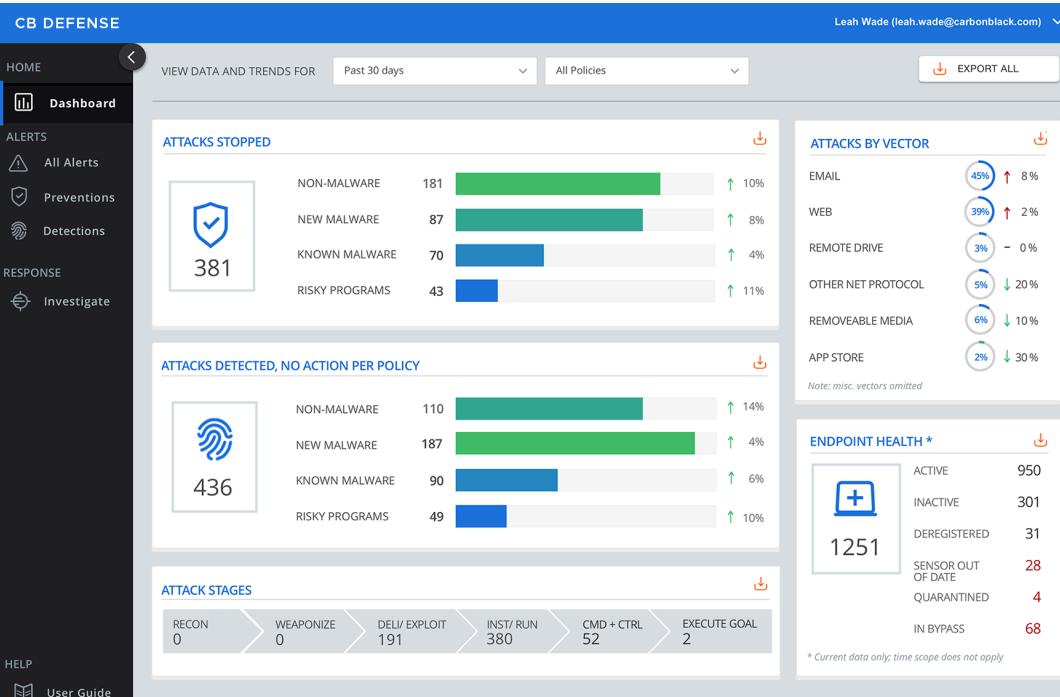


ClamAV

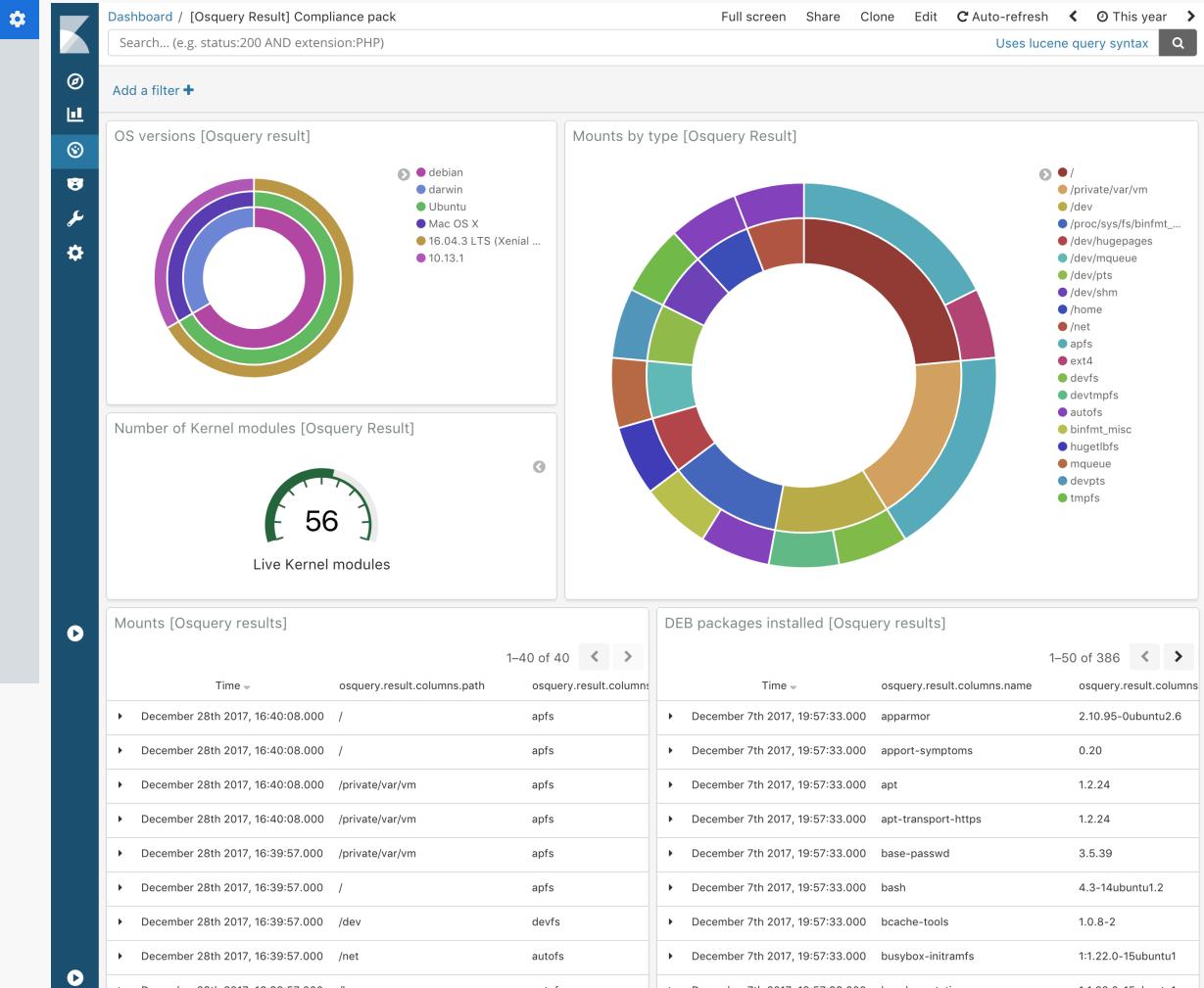


EDR – Endpoint Detection & Response

Carbon Black



osquery



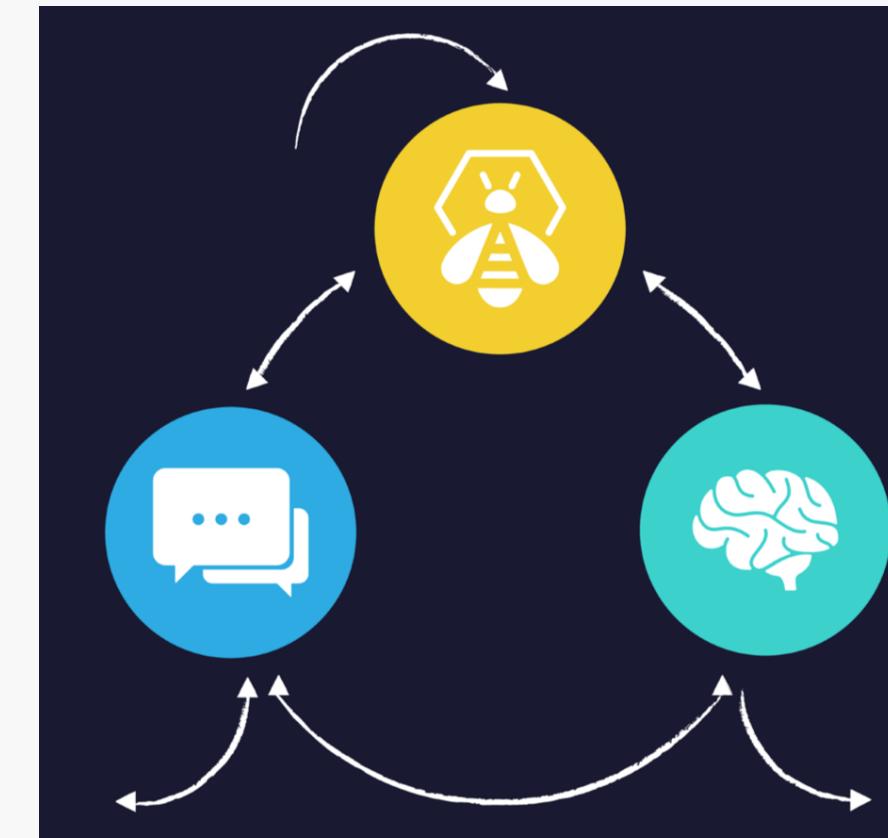
Case/Incident Management System

- 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

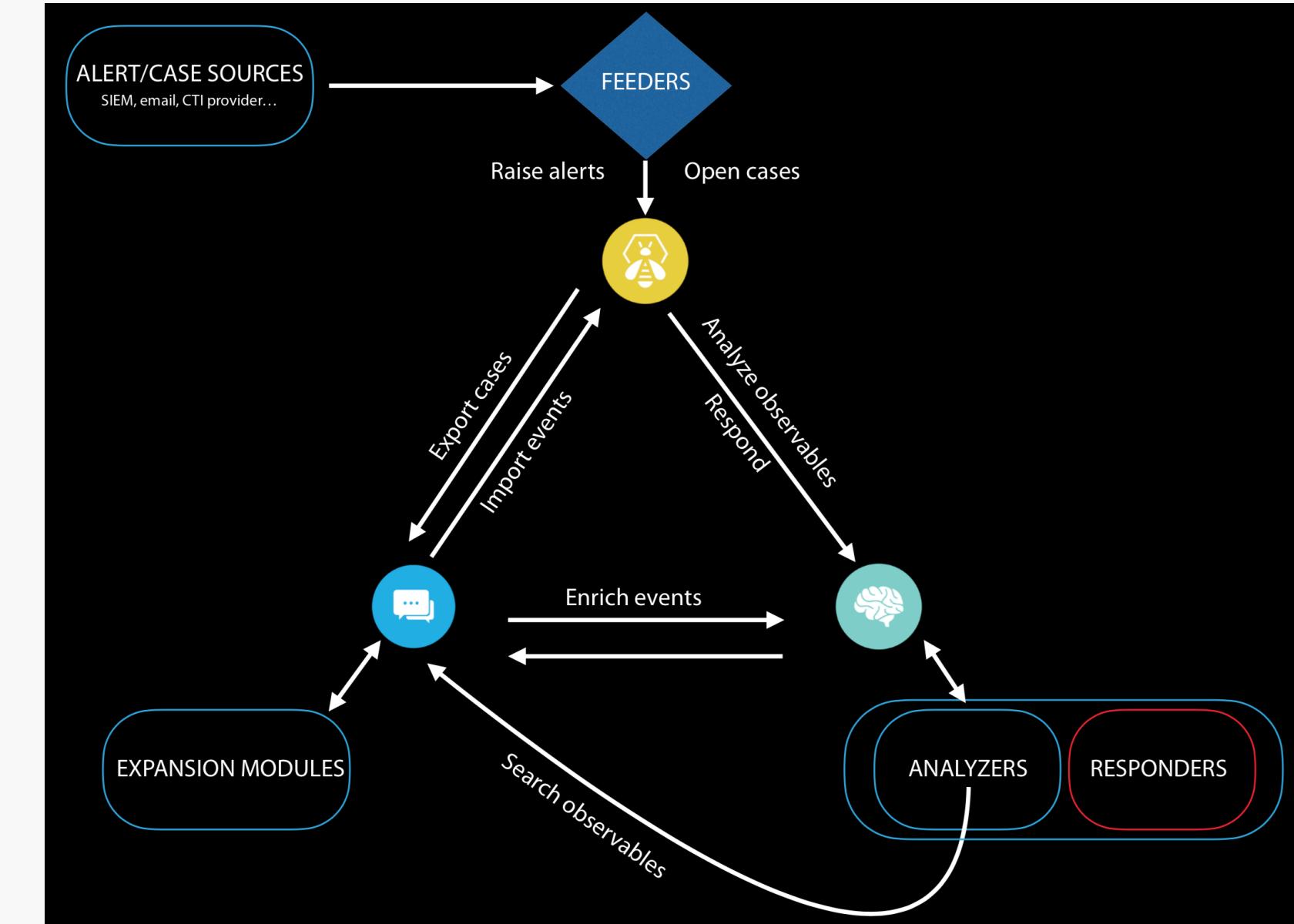
- Programs to take action at the Alert, Case, Task, Log or Observable level
- Input: data and metadata
- Output: Success Failute
 - *Operations : ex: “Add tag in case”, “Add tag in Observables”*
- Mostly customer-specific
- Ex.
 - *Block a set of malicious URLs*
 - *Reply to a user notification*

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.

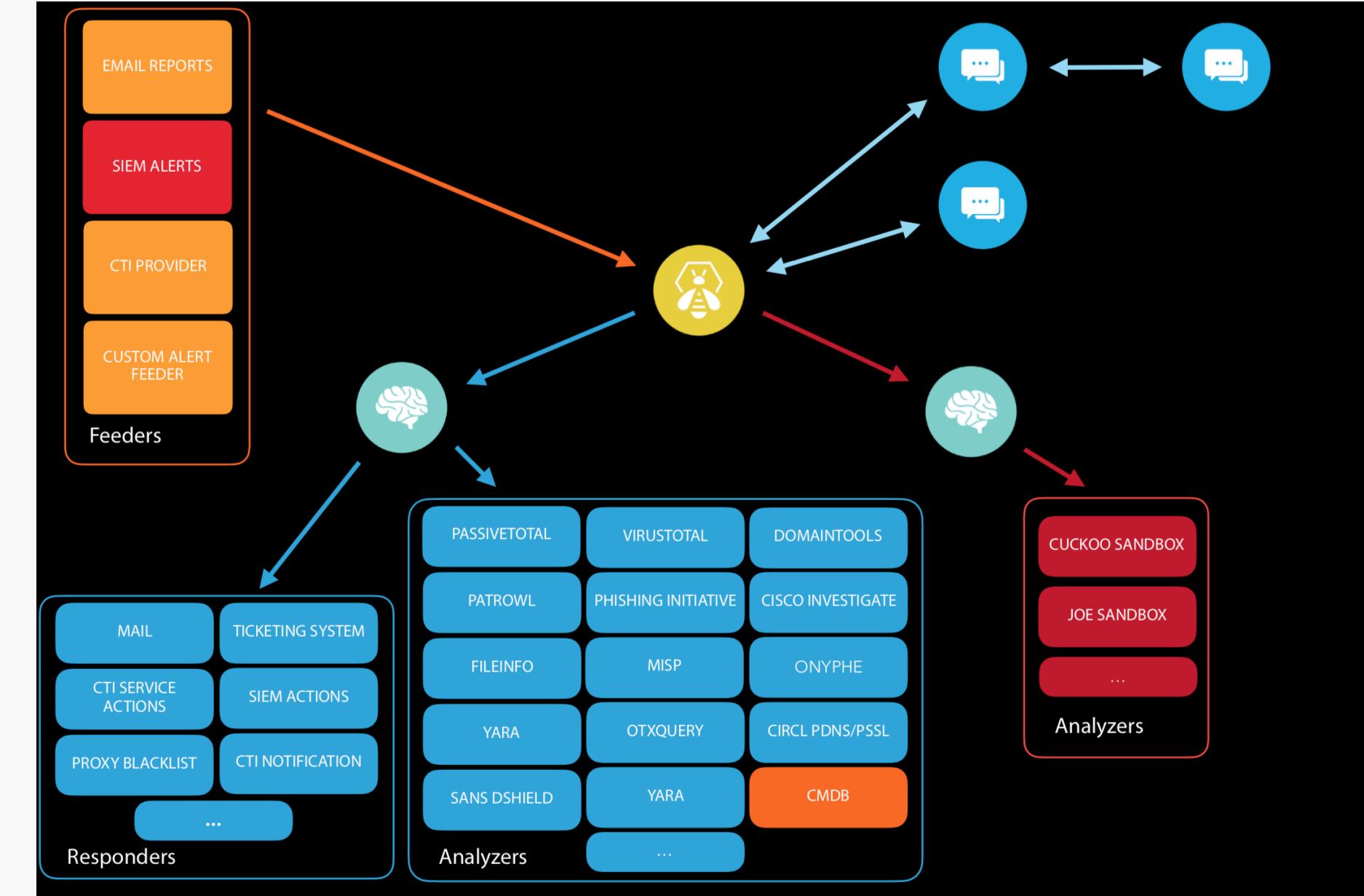


Typical Integration





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