Monitoring Intrusions with HONEYAPPS

Spenser Reinhardt

https://github.com/honeyappsproject/presentations

Celebrating a decade of guiding security professionals.

SECURE360 conference

Who am I?

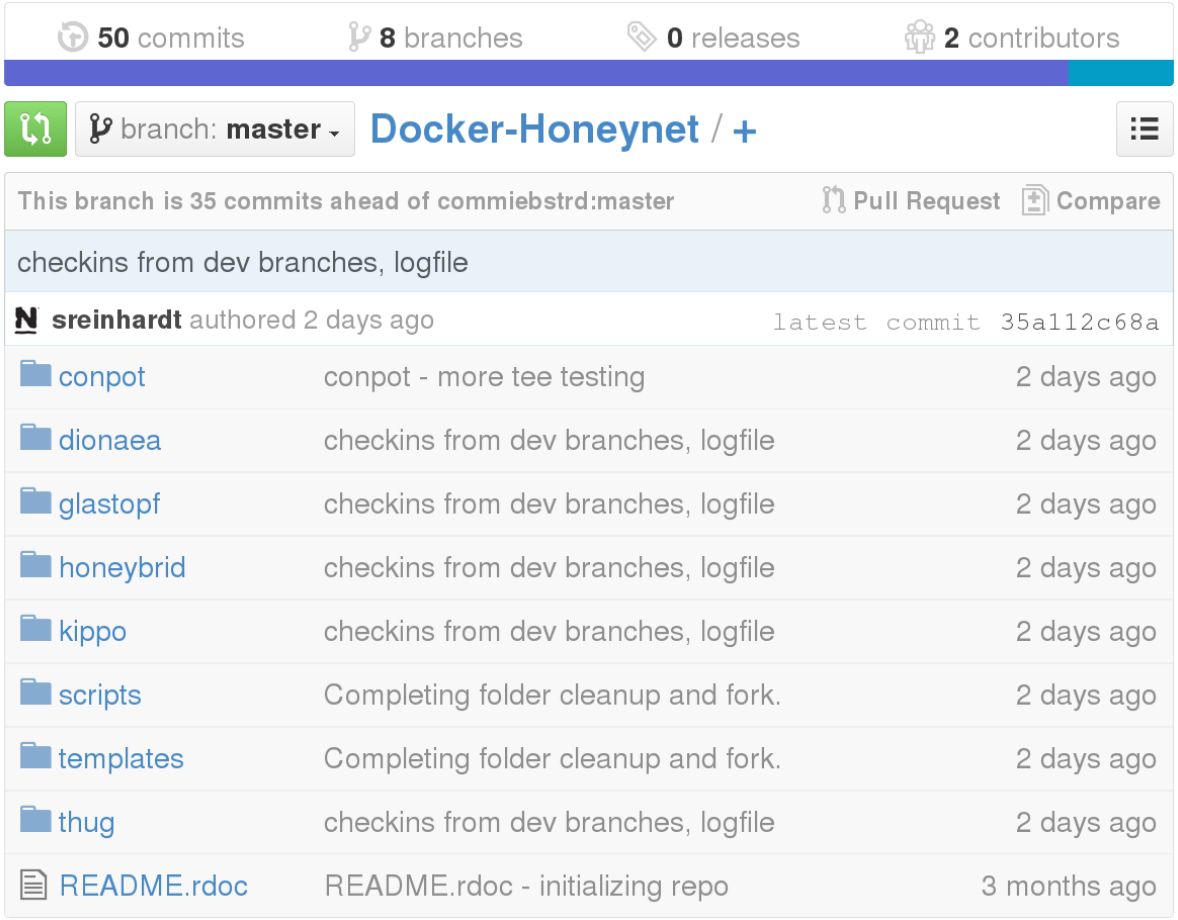
- Spenser Reinhardt (@c0mmiebstrd)
- Github: commiebstrd \ sreinhardt \ honeyappsproject
- Docker: commiebstrd \ sreinhardt \ honeyappsproject
- Co-Founder \ Lead Developer – Honeyapps
- Lead Developer \ Security Lead – Nagios-Plugins
- Def Con NOC Goon
- Capture the Flag Challenge Creator

Plan of Attack

- Terminology
- Where We've Been
- Where We're Going
- How Do Honeypots Help Improve Security Posture
- How Does HoneyApps Fit in My Org
- Videos

Terminology

Github – Code versioning system and storage



50 commits | 8 branches | 0 releases | 2 contributors

branch: master | Docker-Honeynet / +

This branch is 35 commits ahead of commiebstrd:master | Pull Request | Compare

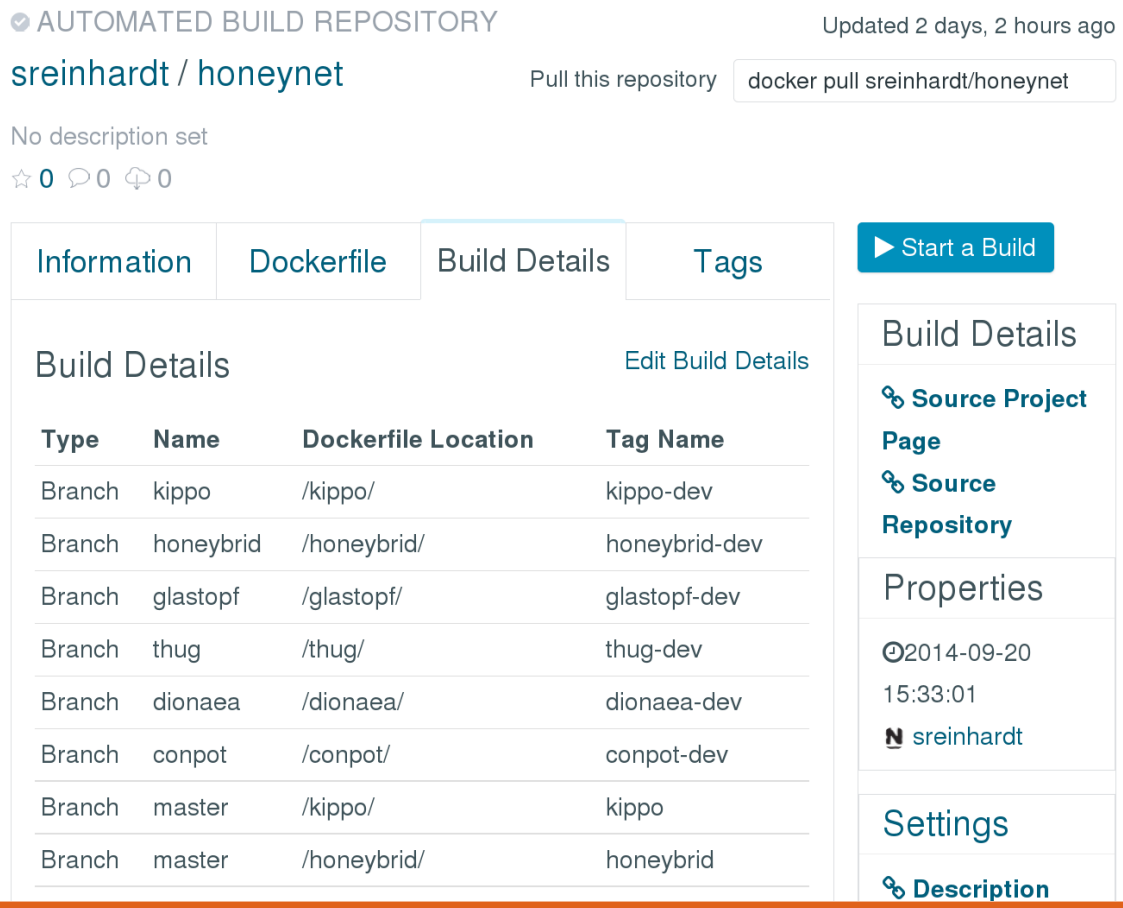
checkins from dev branches, logfile

sreinhardt authored 2 days ago — latest commit 35a112c68a

conpot	conpot - more tee testing	2 days ago
dionaea	checkins from dev branches, logfile	2 days ago
glastopf	checkins from dev branches, logfile	2 days ago
honeybrid	checkins from dev branches, logfile	2 days ago
kippo	checkins from dev branches, logfile	2 days ago
scripts	Completing folder cleanup and fork.	2 days ago
templates	Completing folder cleanup and fork.	2 days ago
thug	checkins from dev branches, logfile	2 days ago
README.rdoc	README.rdoc - initializing repo	3 months ago

Terminology

Docker – Containerized application build and deployment



Terminology

Rust

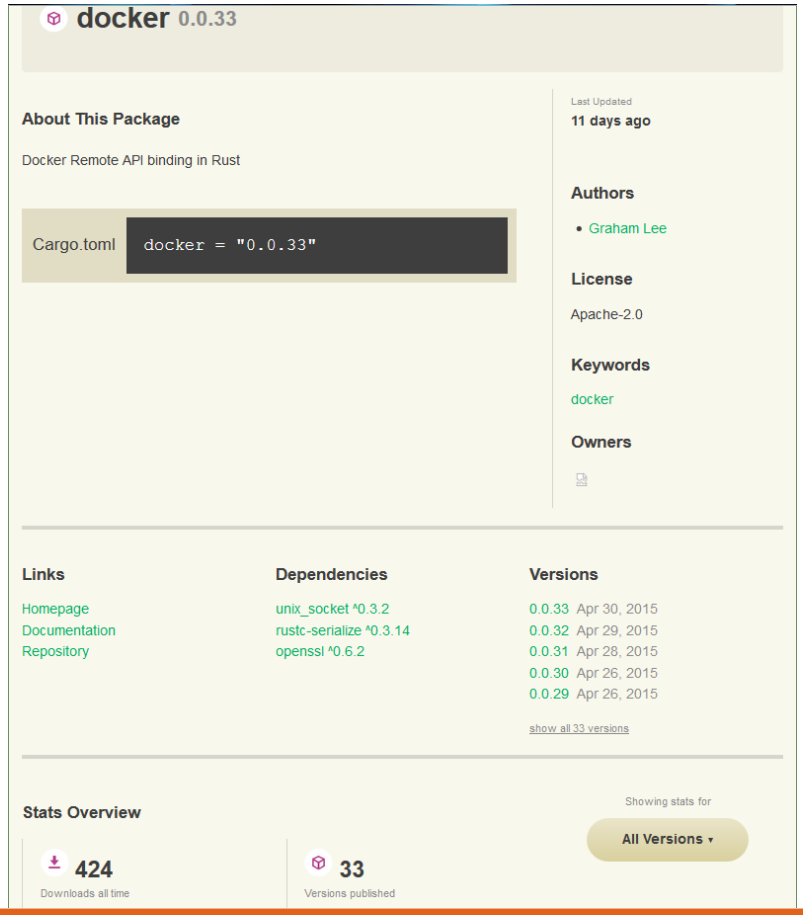
- Modern C\C++ replacement
- Memory safety without garbage collection
- Implicit immutability, explicit mutability
- Rich Typesystem
- Strong functional programming influence

"Rust is a systems programming language that runs blazingly fast, prevents almost all crashes*, and eliminates data races."

* In theory. Rust is a work-in-progress and may do anything it likes up to and including eating your laundry. Control / Performance Safety C C++ Rust Go Java ML Haskell

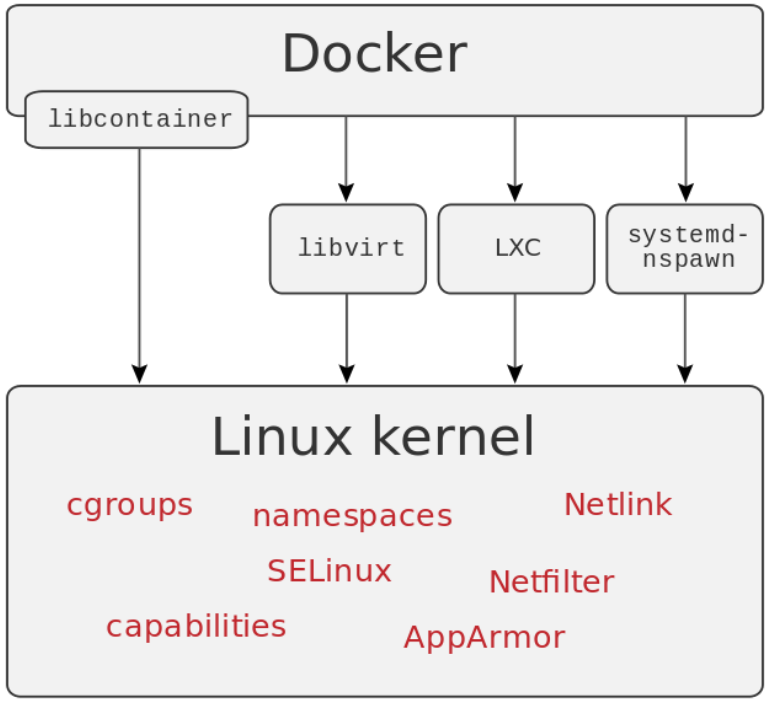
Terminology

Cargo – Automated build and dependency tracker for Rust



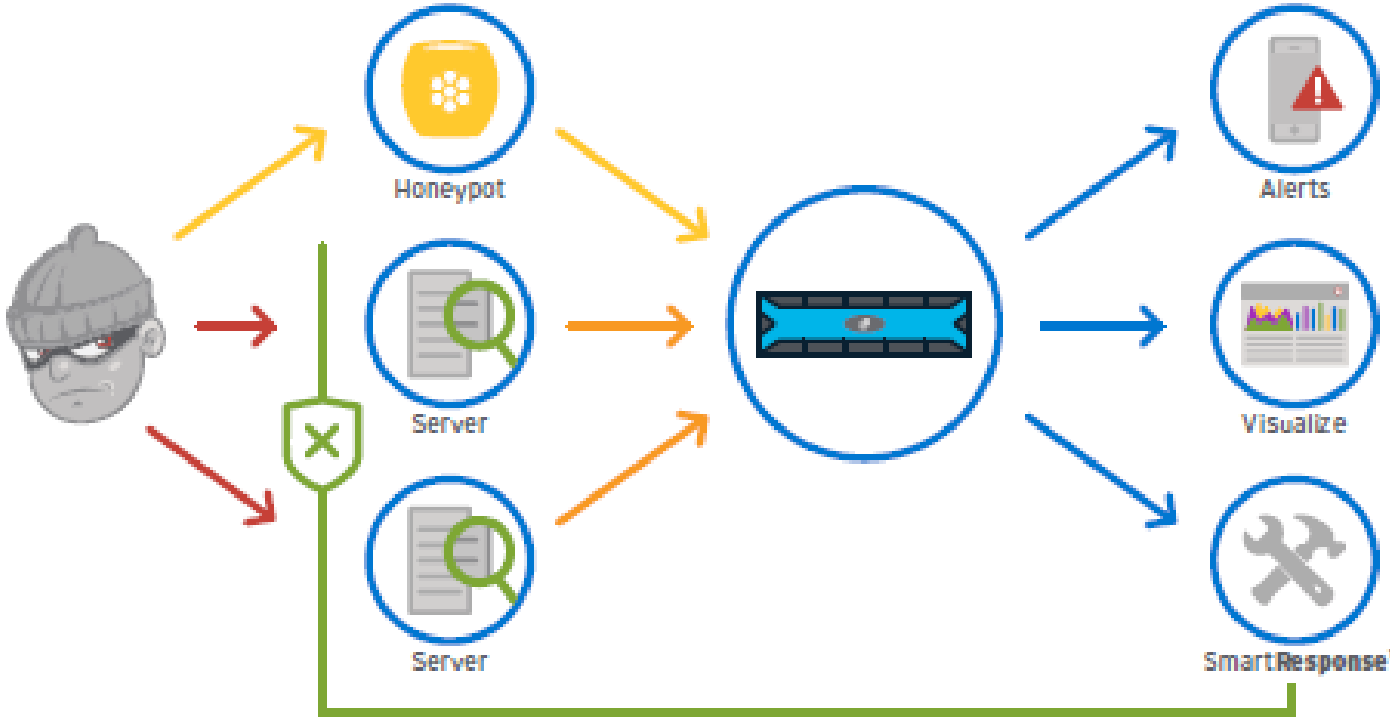
Terminology

Containers – OS level virtualization and isolation method for deploying applications.



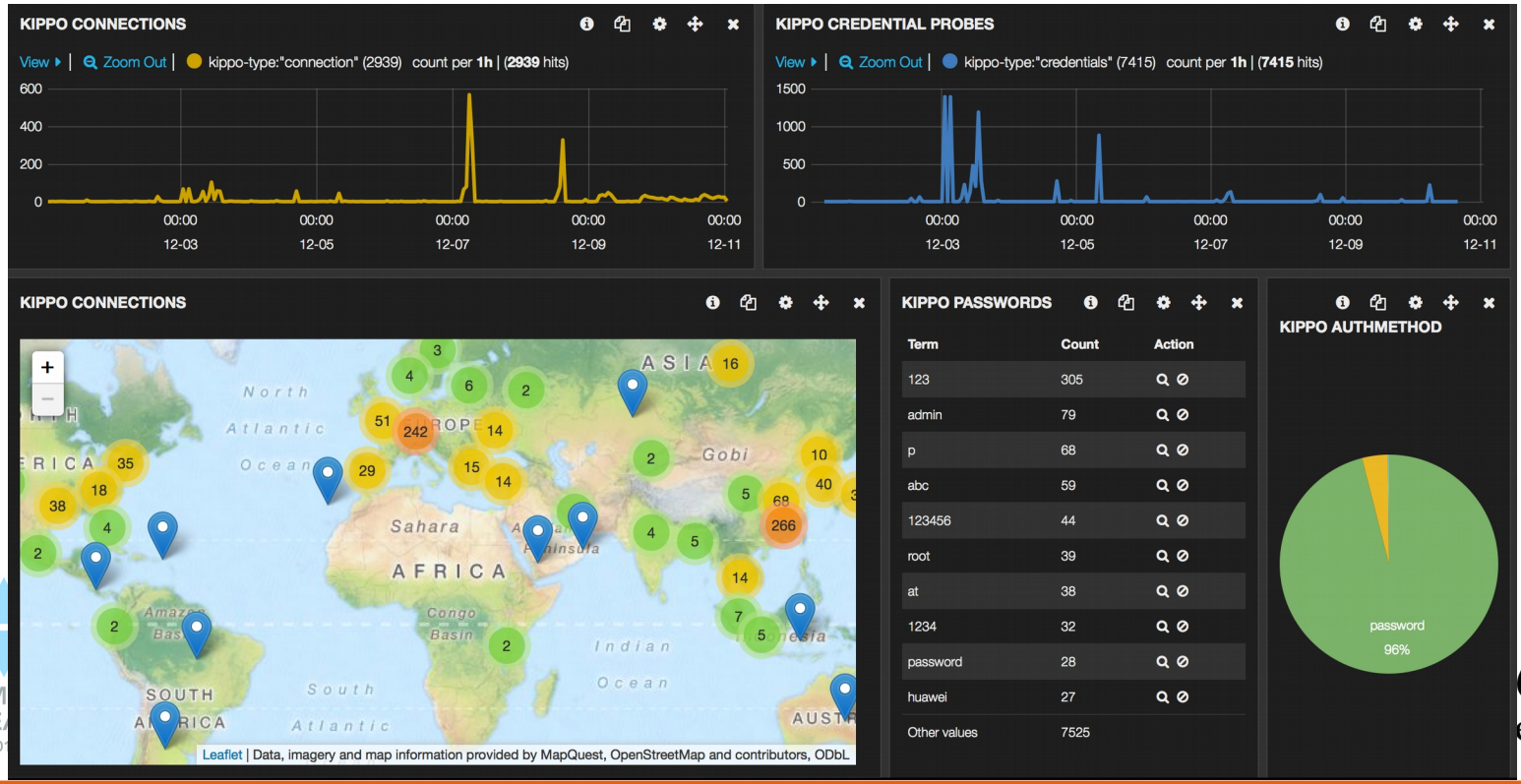
Terminology

Honeypot - System designed to attract and detect malicious actions and actors.



Terminology

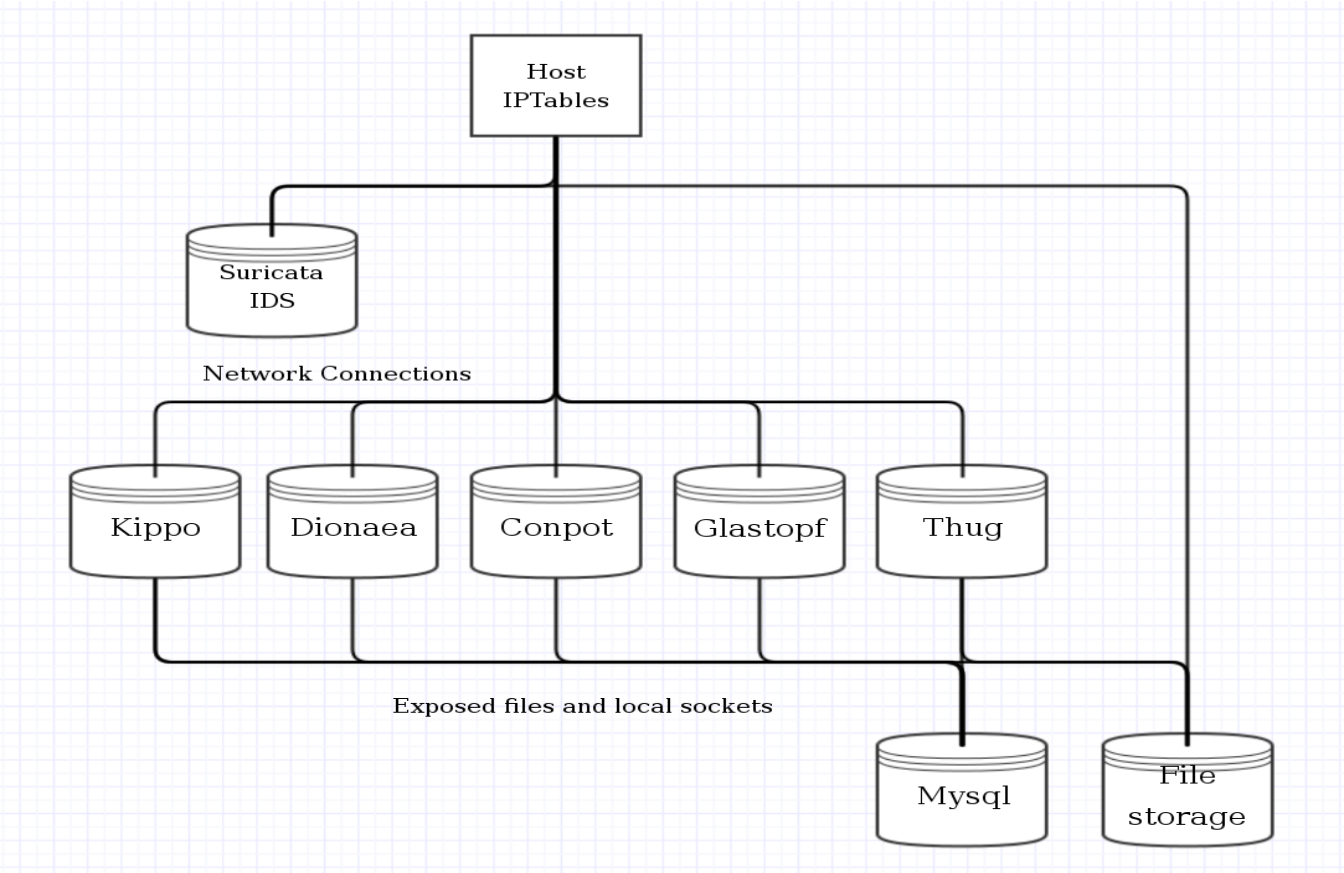
Elk Stack – Centralized log collection and parsing, deep search, and data analytics and visualizations.



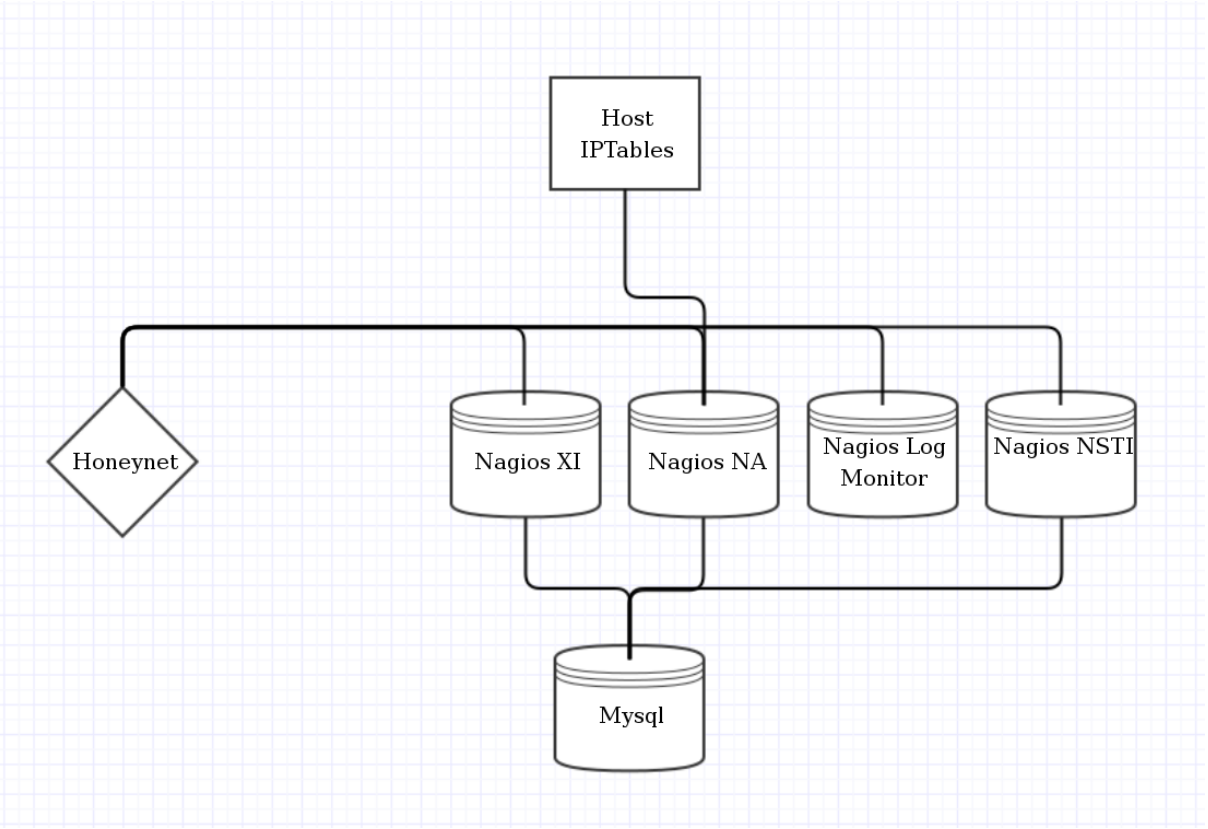
Where We've Been

- Nagios Core – Maintain honeypots, execute remote scripts.
- Nagios Log Server – Retain and visualize attack and log data.
- Nagios Network Analyzer – Capture netflow traffic.
- Docker – Honeypot containment and execution.
- Suricata – Signature based detection of attacks.
- Honeynet Project – Various honeypots.

Where We've Been



Where We've Been

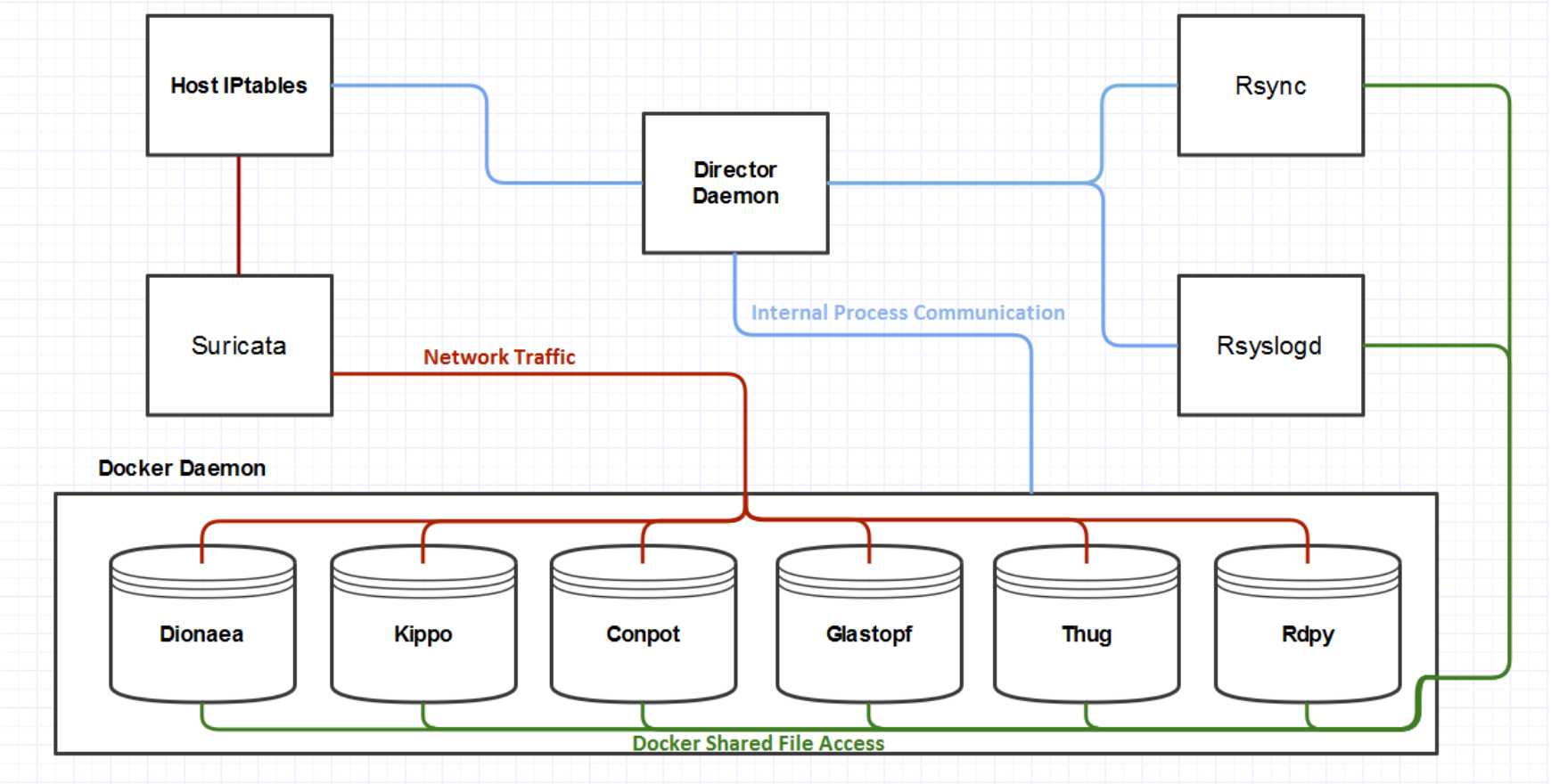


Where We're Going

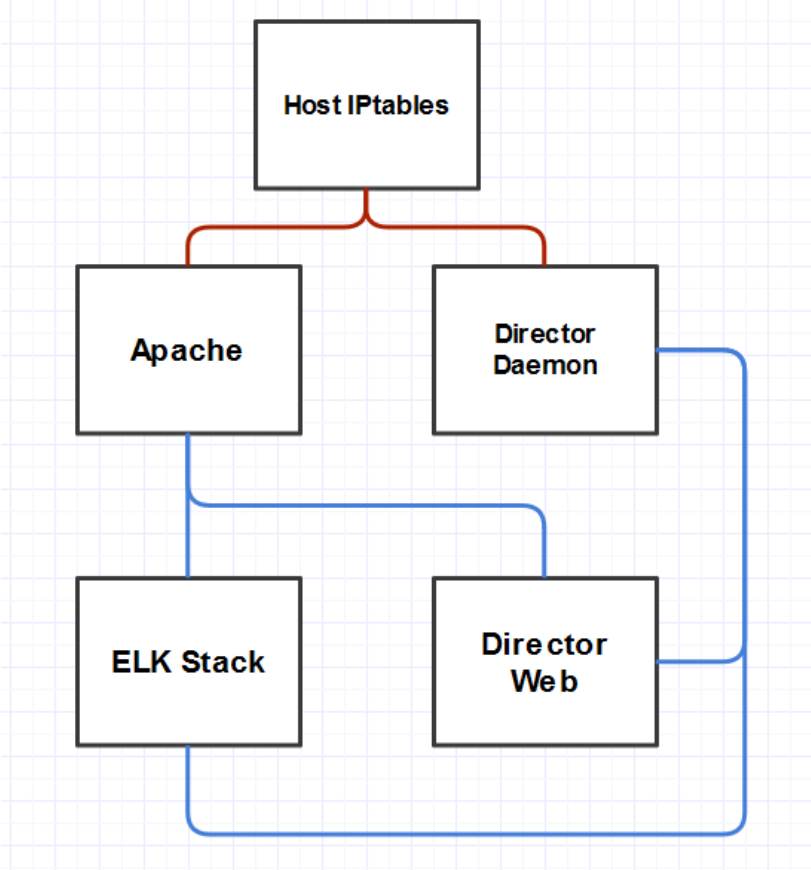
- HoneyApps Director
  - Centralized management interface
  - Control, logging, honeypot daemon isolation.
  - Simple flat file and web interface configuration.
  - Memory and thread safe build language.
  - Repeatable build and test environments, publicly available.

- Overall Project
  - Revert on crash honeypots.
  - Fast deployment with automatic configuration pushes.
  - Deployment via Docker containers and VMware images.
  - HPfeeds\HPfriends integration via native rust implementation
  - Integration and correlation with third-party tools. (import & export)
  - Enterprise supported open-source project

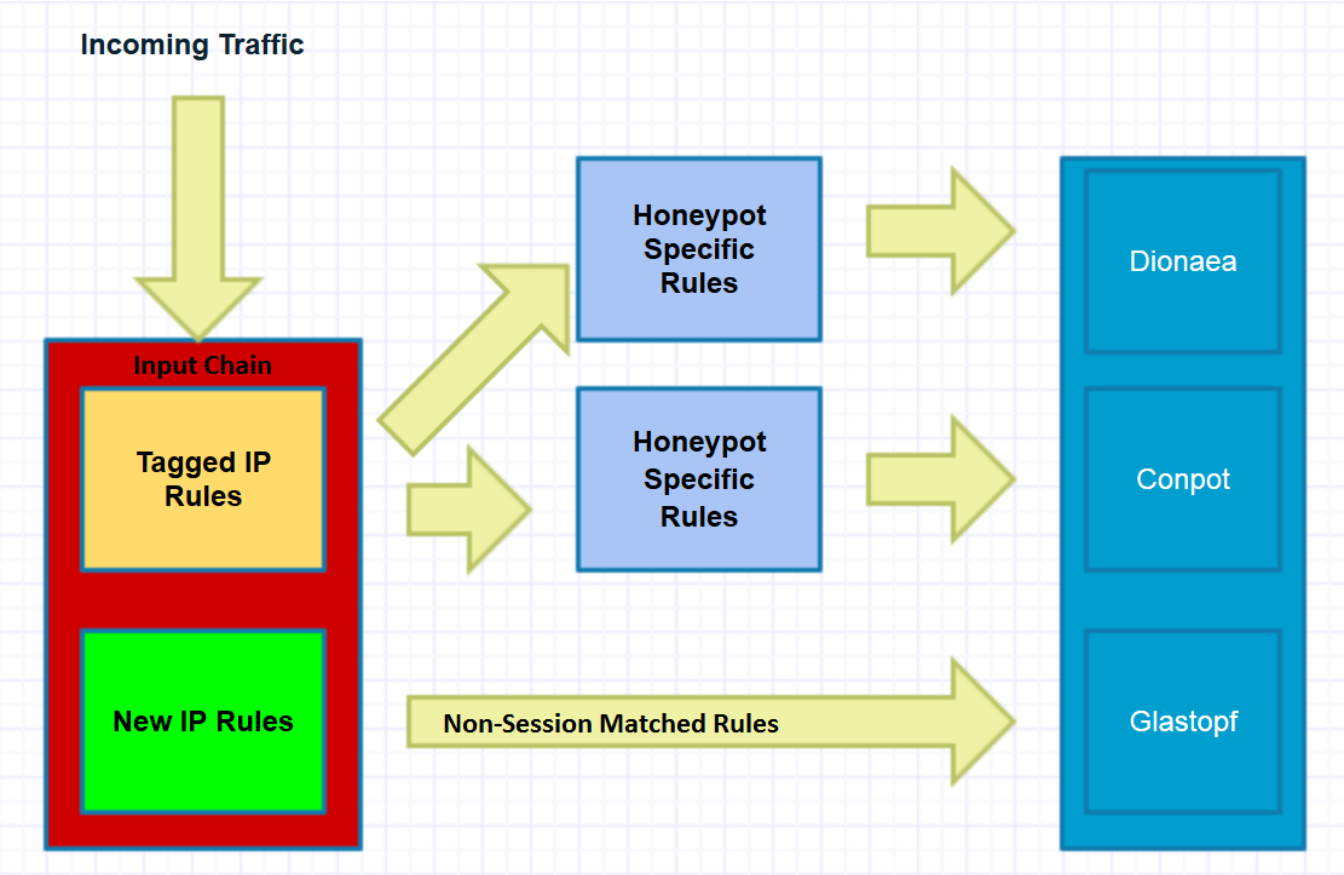
Director Worker



Director Primary



Dynamic IPtables Rules



Why It's Important To You

Perimeter Security? Intrusion Detection\Prevention Systems?
Honeypots!

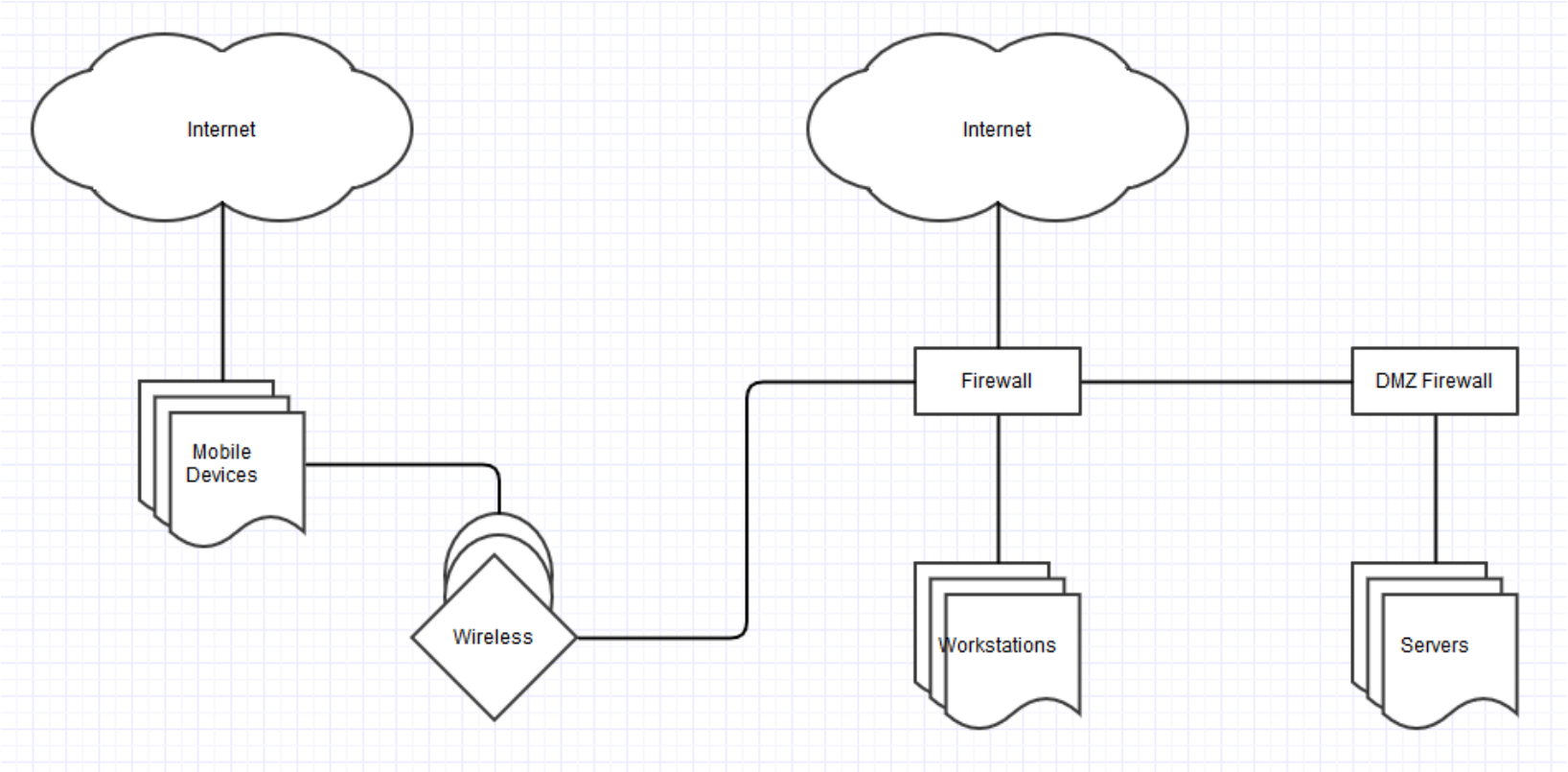
DIAMOND YEAR —2015—

Celebrating a decade of guiding security professionals.

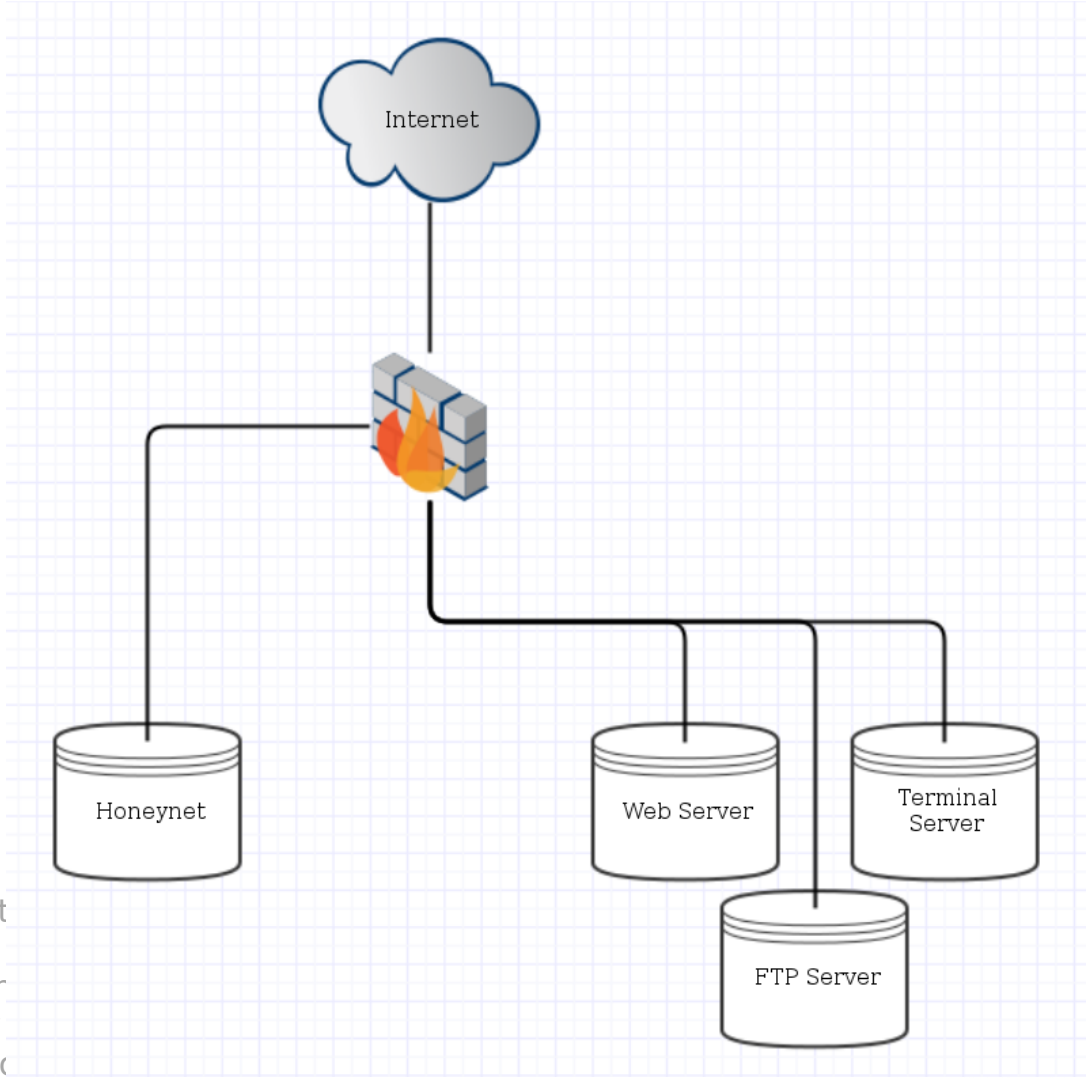
Where the Science is Taking Us in Cybersecurity

SECURE360 conference

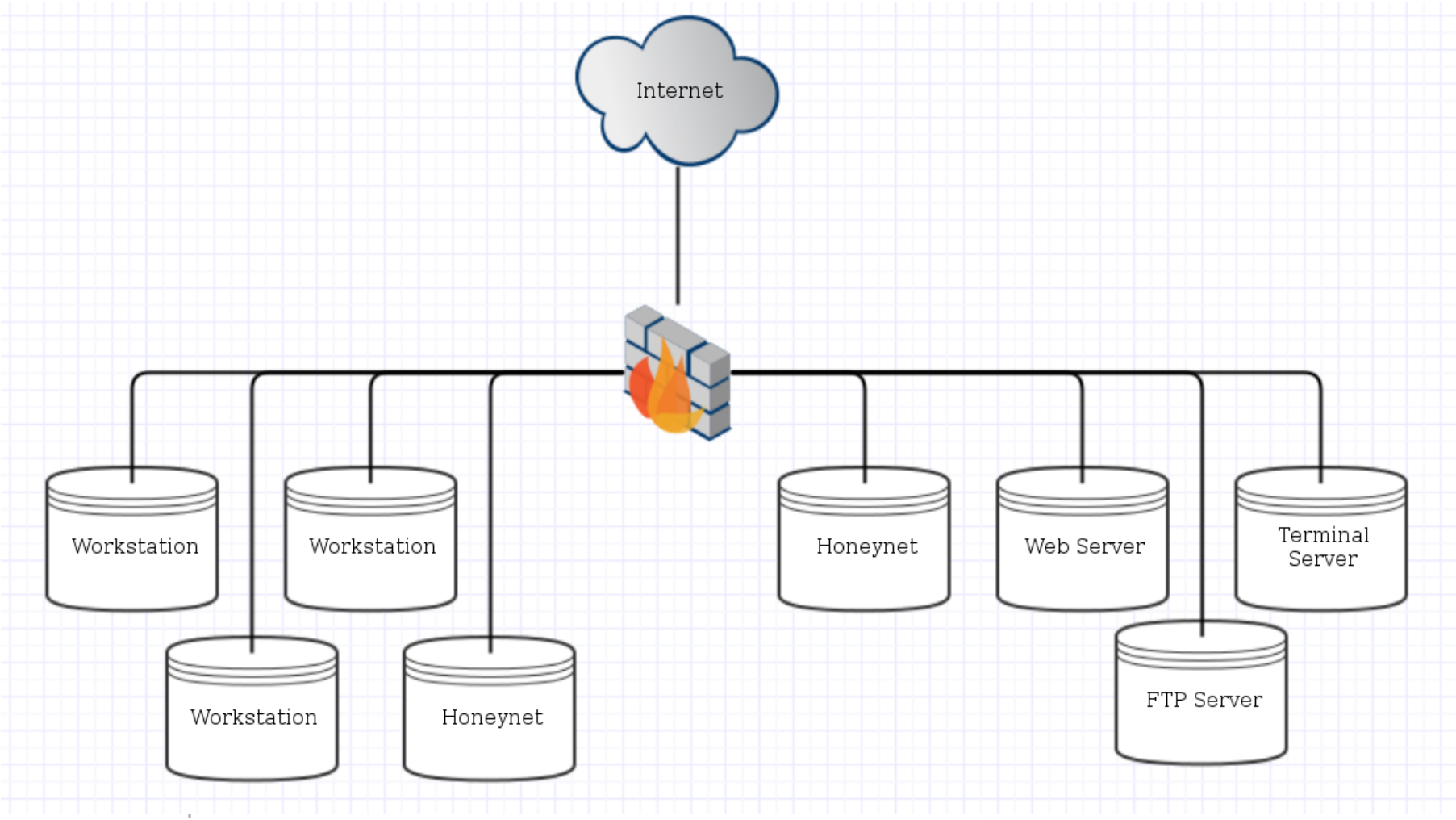
Modern Network Layouts



Server Honeypot Layout



Workstation Honeypot Layout



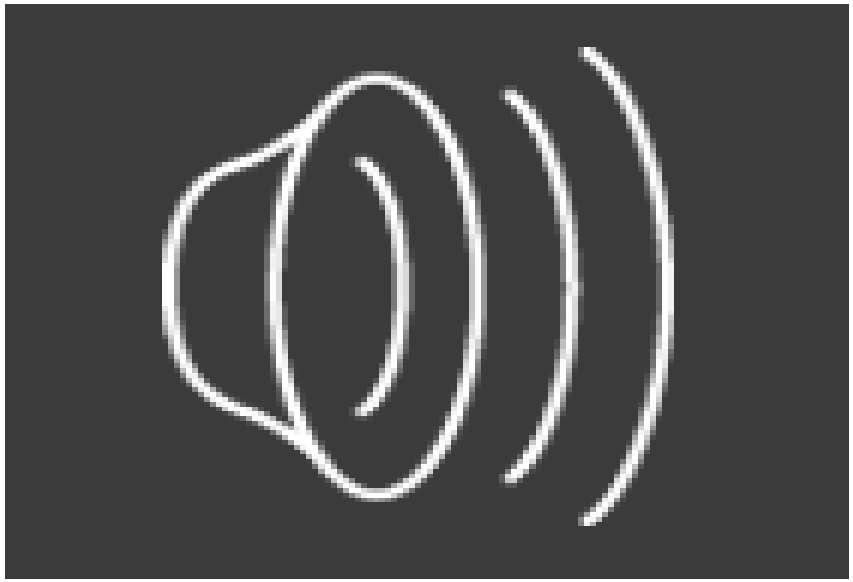
Plan of Attack

- ~~Terminology~~
- ~~Where We've Been~~
- ~~Where We're Going~~
- ~~How Do Honeypots Help Improve Security Posture~~
- ~~How Does HoneyApps Fit in My Org~~
- Videos

Dionaea Honeypot

- General purpose honeypot
- Expandable through plugins and modules
- Full shellcode emulation
- Detects attacks on ports:
  - 21(ftp)
  - 69(tftp)
  - 135(emap)
  - 445(smb)
  - 1443(mssql)
  - 3306(mysql)
  - 5060-5061(sip)
  - 63001-64000(ftp)
- Automated control and deployment with Director

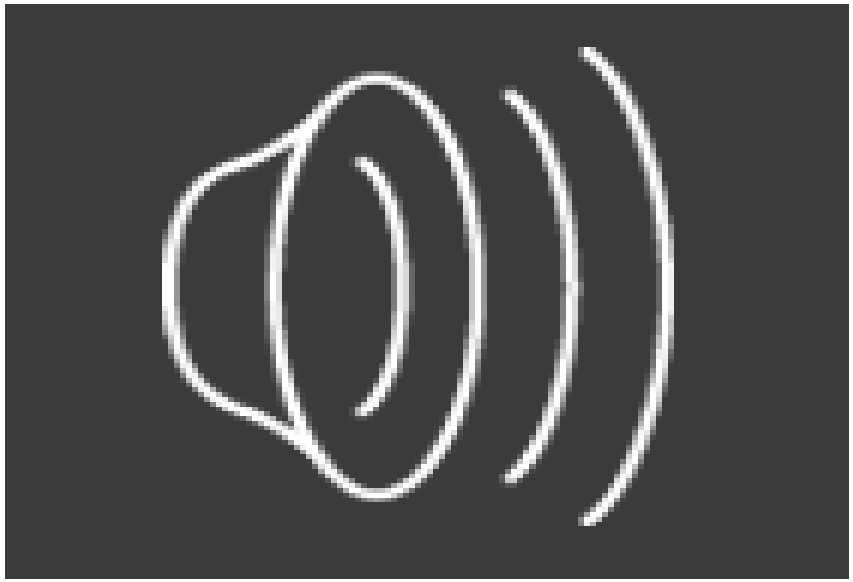
Dionaea Attacks



Glastopf Honeypot

- Web application specific honeypot
- Detects attacks on ports:
  - 80 (http)
  - 443 (https)
- Full PHP emulated virtual environment
- Emulated sql backend
- Automated control and deployment with Director

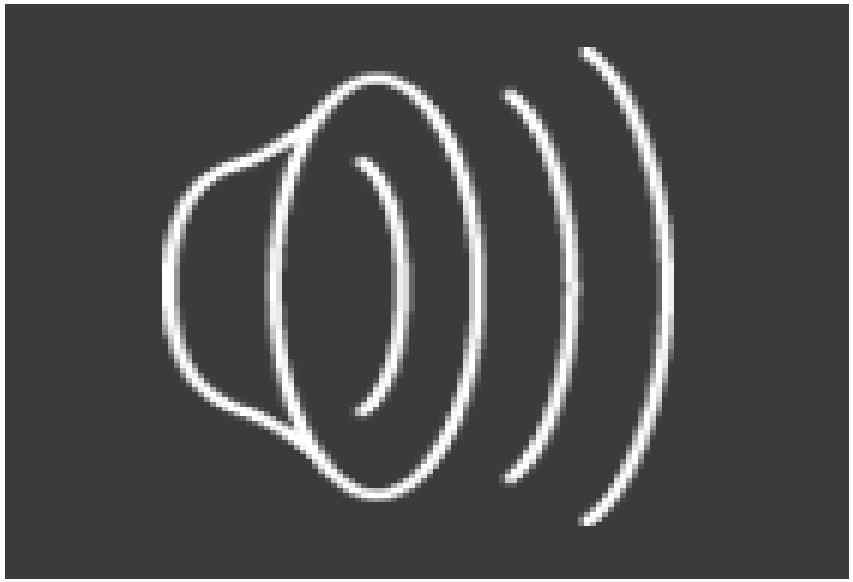
Glastopf Attacks



Conpot Honeypot

- Industrial Control Systems(ICS) Supervisory Control and Data Acquisition (SCADA)
- Defaults to building device control system
- Full Shellcode emulation
- Detects attacks on ports:
  - 80 (http)
  - 161 (snmp)
  - 503 (modbus)
- Automated control and deployment with Director

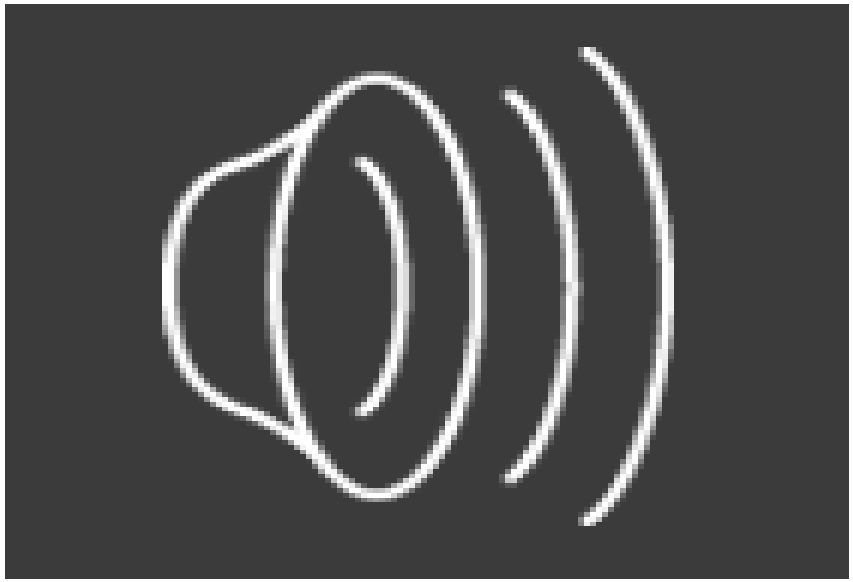
Conpot Attacks



Kippo Honeypot

- SSH specific honeypot
- Full virtual shell emulation
- Daemon attack emulation
- Detects attacks on port:
  - 22 (ssh)
- Automated control and deployment with Director

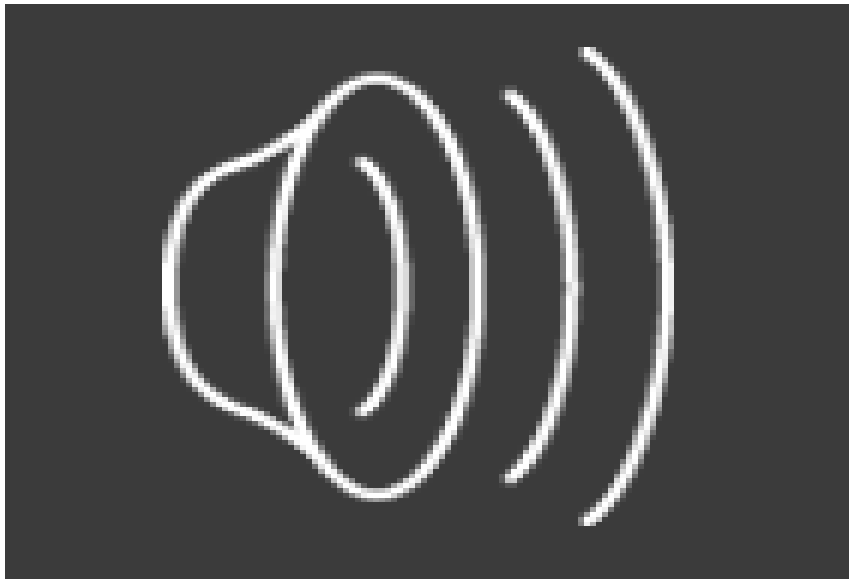
Kippo Attacks



RDPy Honeypot

- Remote Desktop Protocol honeypot and mitm
- Record & replay screen, mouse interaction, and keys
- Man-in-the-middle to live Windows hosts
- Detects attacks on port:
  - 3389 (ms-rdp)
- Automated control and deployment with Director

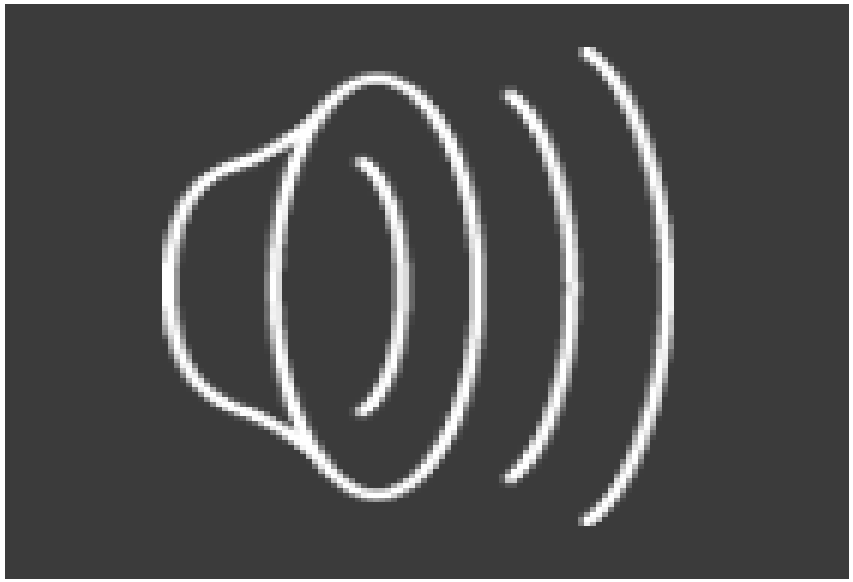
RDPy Attacks



Thug Honeypot

- Low interaction honeyclient
- W3C DOM compliant
- Google V8 Javascript Engine
- Libemu\Pylibemu shellcode emulation
- 8 IE, 15 Chrome, 3 Firefox, & 5 Safari user-agents and personalities
- No active ports, is feed uri's to connect and analyze
- Automated control and deployment with Director

Thug Attacks



Conclusion & Questions

Personal:

- @c0mmiebstrd
- Docker.com/u/sreinhardt – Docker.com/u/commiebstrd
- Github.com/commiebstrd – github.com/commiebstrd

HoneyApps:

- @honeyappsproj
- Docker.com/u/honeyappsproject
- Github.com/honeyappsproject
- www.honeyapps.net

HONEYAPPS