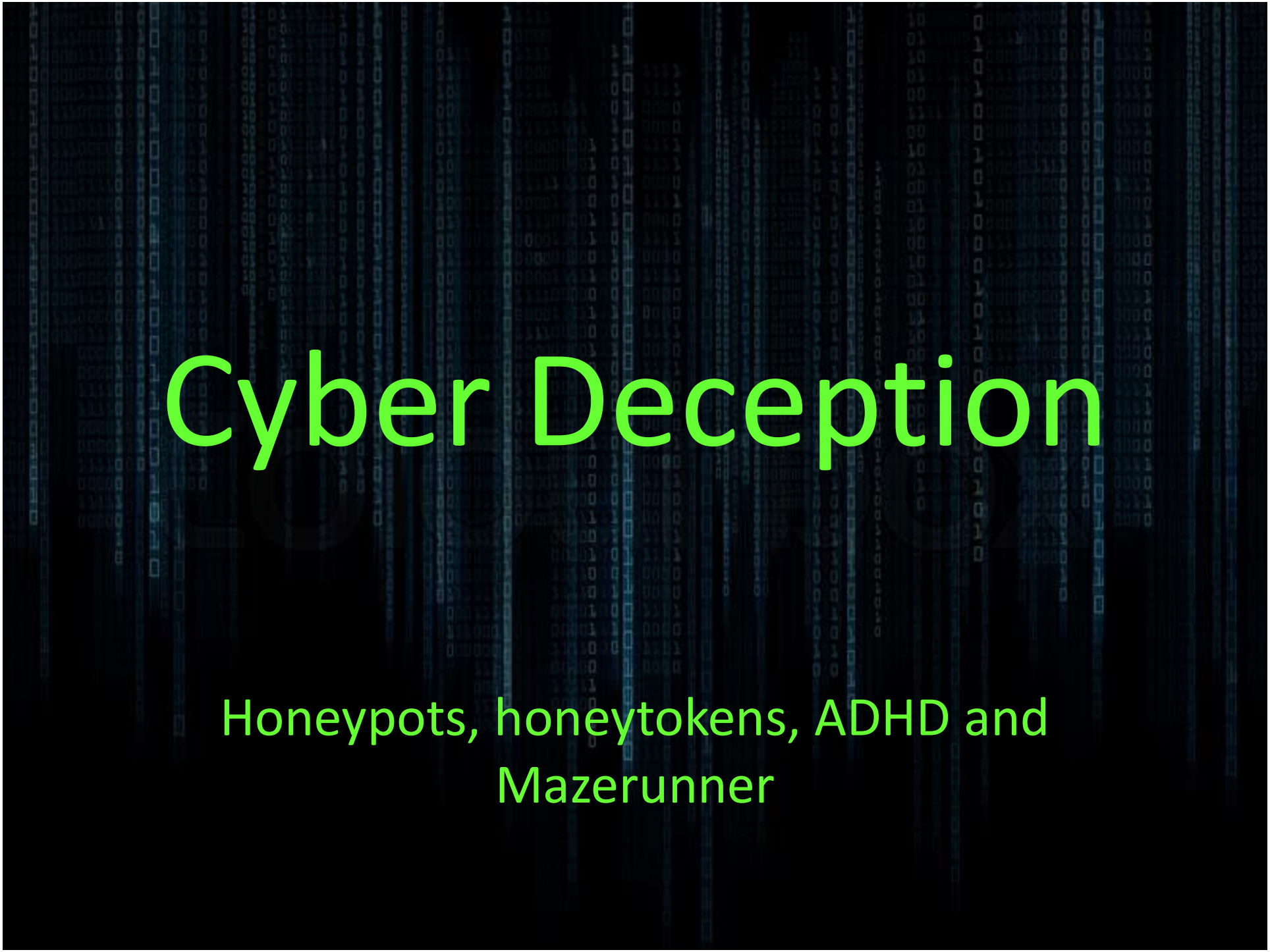

Cyber Deception
Honeypots, honeytokens, ADHD and Mazerunner

James Beal
Twitter: @chaoticneutr4l
Email: james.beal@caseys.com

- SOC Analyst at Casey's General Stores
- Legal disclaimer – all of this is my opinion and personal research, not representing work or any tools/techniques/procedures we use at CGS

Honeypots

- Made “famous” by Lance Spitzner in early 2000’s with the Honeynet Project
  - https://www.honeynet.org
- It is a closed group, I have not yet attempted to apply for membership to their research mailing lists

Books

amazon Try Prime

Books honeypots

honeypots

Departments Your Amazon.com Today's Deals Gift Cards & Registry Sell Help

Books Advanced Search New Releases Best Sellers The New York Times® Best Sellers Children's Books Textbooks Textbook Rentals Sell Us Your Books Best Books of the Month Kindle eBooks

1-12 of 651 results for **Books** : **"honeypots"**

Show results for

Any Category

Books

- Security & Encryption (174)
- Internet, Groupware, & Telecommunications (53)
- Computers & Technology (223)
- Networking & Cloud Computing (170)
- Hacking (37)
- Privacy & Online Safety (34)
- Network Security (124)
- Software (21)
- Networks, Protocols & APIs (61)
- Mathematics (10)
- Romance (169)

+ See more

Refine by

Amazon Prime

Prime

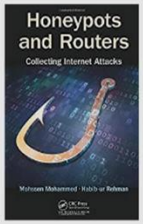
Eligible for Free Shipping

Free Shipping by Amazon

New Releases

Last 30 days (13)
Last 90 days (46)
Coming Soon (3)

Author



Honeypots and Routers: Collecting Internet Attacks Dec 1, 2015

by Mohssen Mohammed and Habib-ur Rehman

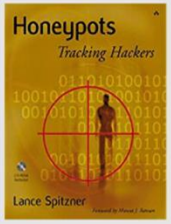
Hardcover
$62.04 ~~$69.95~~ Prime
Only 8 left in stock - order soon.

More Buying Choices
$56.61 used & new (23 offers)

Kindle Edition
$69.95
Auto-delivered wirelessly

FREE Shipping on eligible orders See Details

Excerpt
Front Cover : ... *Honeypots* and Routers Collecting Internet Attacks Mohssen Mohammed ... See a random page in this book.



Honeypots: Tracking Hackers Sep 20, 2002

by Lance Spitzner

Paperback
$33.96 ~~$44.99~~ Prime
Only 8 left in stock - order soon.

More Buying Choices
$4.98 used & new (52 offers)

★★★★½ 15

FREE Shipping on eligible orders See Details

Virtual Honeypots: From Botnet Tracking to Intrusion Detection Jul 26, 2007

by Niels Provos and Thorsten Holz

Paperback
$41.06 ~~$64.99~~ Prime
Only 3 left in stock - order soon.

More Buying Choices
$26.00 used & new (50 offers)

Kindle Edition
$28.07
Auto-delivered wirelessly

★★★★★ 13

Trade in yours for an Amazon Gift Card up to $3.90
FREE Shipping on eligible orders See Details

Honeypot Types
Low Interaction

- Simulate only the services frequently requested
- Consume relatively few resources
  - multiple virtual machines can easily be hosted on one physical system
  - short response time

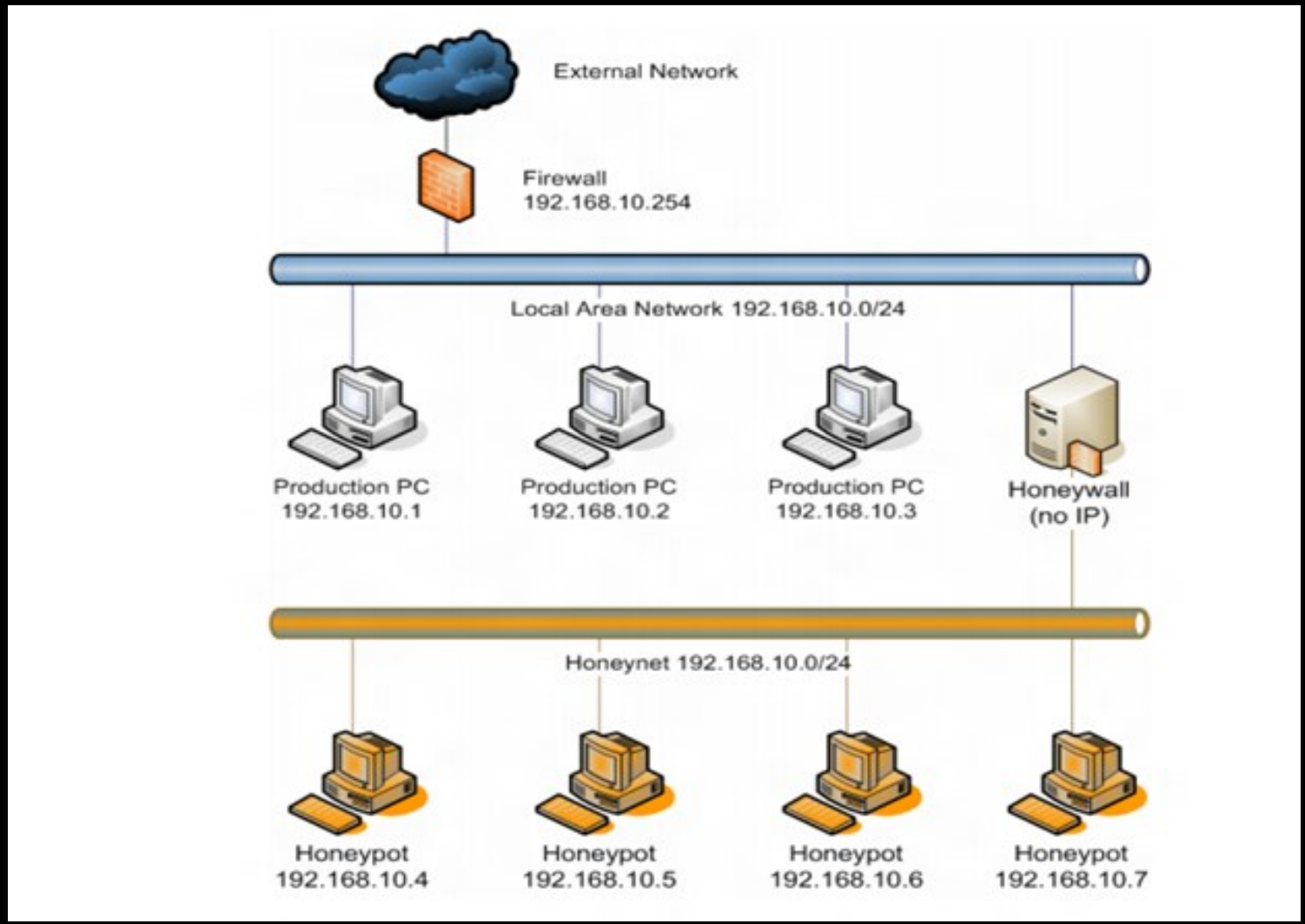
High Interaction

- imitate the activities of the production systems
- host a variety of services
- an attacker may be allowed a lot of services to waste his time.
- Using VMs - multiple honeypots can be hosted on a single physical machine – also easy rebuilds
- expensive to maintain - if you go physical

“Medium” Interaction

- More than low, which is essentially just a couple running services
- Not full machines like a High would be
- Easier to config/setup

Basic Architecture



Config

- Depending on which type you configure, the install process is a pain
- Usually a matter of build your own management systems/architecture/GUI
- LOGGING!!!

Current/Future

- That was the past
- Research just stopped for years
- Finally several new companies have taken the basic concepts and run with them into functional software tools/suites
- Thinkst(Canaries), BHIS(ADHD) and Cymmetria(Mazerunner)

Thinkst

- Main product is called Canary
- Idea is no management config necessary
- setup in 2-3 minutes and their software auto configures
- Multiple protocols supported out-of-the-box
- hosted console gives you effortless monitoring and notifications

ADHD

- Linux distro based on Ubuntu LTS
- Tools aimed at active defense preinstalled and configured
- Purpose of this distribution is to aid defenders by giving them tools to “strike back” at the bad guys.

- Interfering with the attackers’ reconnaissance
- Compromising the attackers’ systems
- Defense mechanisms triggered by malicious activity such as network scanning or connecting to restricted services.
- Look up John Strand’s YouTube account for vids

ADHD Tools

Annoyance

Artillery

Bear Trap

Cryptolocked

DenyHosts

Honey Ports

Invisiport

Kippo

OsChameleon

PHP-HTTP-Tarpit

Portspoof

PSAD

Rubberglue

Spidertrap

TcpRooter

Weblabyrinth

Wordpot

ADHD Tools

- Artillary - purpose of Artillery is to provide a combination of honeypot, file-system monitoring, system hardening, real-time threat intelligence feed, and overall health of a server monitoring-tool
- Cryptolocked - file system integrity failsafe, monitors your file system for unauthorized modification
- Spidertrap - Trap web crawlers and spiders in an infinite set of dynamically generated webpages.

ADHD Tools

Attribution

Decloak - Used to identify the real IP address of a web user, regardless of proxy settings, using a combination of client-side technologies and custom services

Docz.py

Honeybadger - Used to identify the physical location of a web user with a combination of geolocation techniques using a browser's share location feature, the visible WiFi networks, and the IP address

Jar-Combiner

Sqlite Bug Server

Web Bug Server

ADHD Tools

Absolution

Human.py - Human.py (Aka human pie) is a script made for the sole purpose of detecting human usage of service accounts.

Lockdown

OpenBAC

Simple-Pivot-Detect

Sweeper

TALOS - TALOS is an evolution in the democratization of Active Defense technologies and methodologies. It is an Active Defense Framework; allowing for the quick training and deployment of computer network defenders

ADHD Tools

Attack

Beef - The Browser Exploitation Framework Project is a tool for the pwnage of one of the underexplored frontiers in information security, the web browser

Gcat

Ghostwriting.sh - method of anti-virus bypass utilizing binary deconstruction, insertion of arbitrary assembly code, and reconstruction

Java-Web-Attack

Pushpin

Recon-ng – passive recon

SET(SocEng Toolkit) - open source tool implemented in python which focuses on penetration testing through social engineering

ADHD Tools

HoneyDrive

- Over 10 pre-installed and pre-configured honeypot software packages such as Kippo SSH honeypot, Dionaea and Amun malware honeypots, Honeyd low-interaction honeypot, Glastopf web honeypot and Wordpot, Conpot SCADA/ICS honeypot, Thug and PhoneyC honeyclients

Windows

Kansa - modular incident response framework in Powershell

OsFuscate

Powercat - PowerShell module offers all the functionality of netcat with a few added features

Software Restriction Policies - restrict which types of files from the Windows and Program Files directories are allowed to run and where they are allowed to run from

Mazerunner – Community Edition

- Platform for creating effective deception stories
- Attackers making lateral movement will first collect info on their next target
- Breadcrumbs deployed by MazeRunner that point to decoys
- Reveal their attack tools and methods, which defenders are then able to document and analyze
- Setup to export threat information to create attack signatures

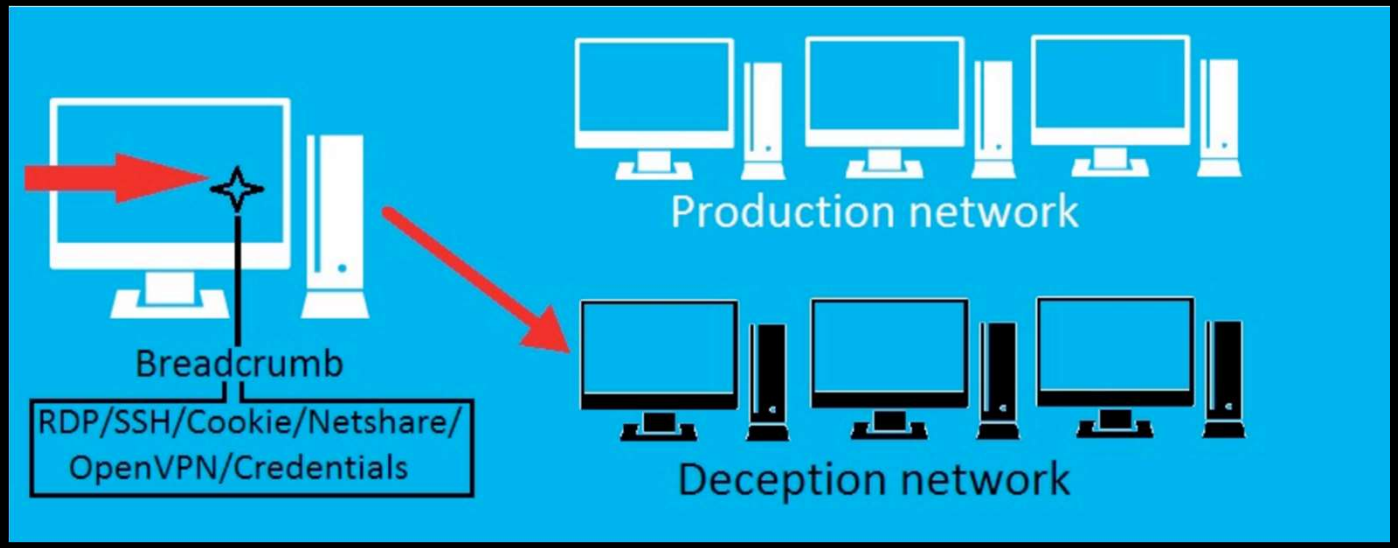
Mazerunner – Community Edition

- Community edition comes as a preconfigured OVA/QCOW2 file – two open VM formats
- Easy to setup in VMWare Player/Wkstn, ESXi and KVM
- Currently NOT supported for VirtualBox
- System req's:
  - 150GB minimum storage, 500GB recommended
  - 2GB of RAM (add 2GB for each additional nested decoy)
  - 1 x CPU @ 2 GHz (add another CPU core for each additional nested decoy)
  - VMware hypervisor (Player 7 or higher; Workstation 11 or higher; ESXi server 5.1 or higher) or KVM hypervisor, with nested virtualization enabled

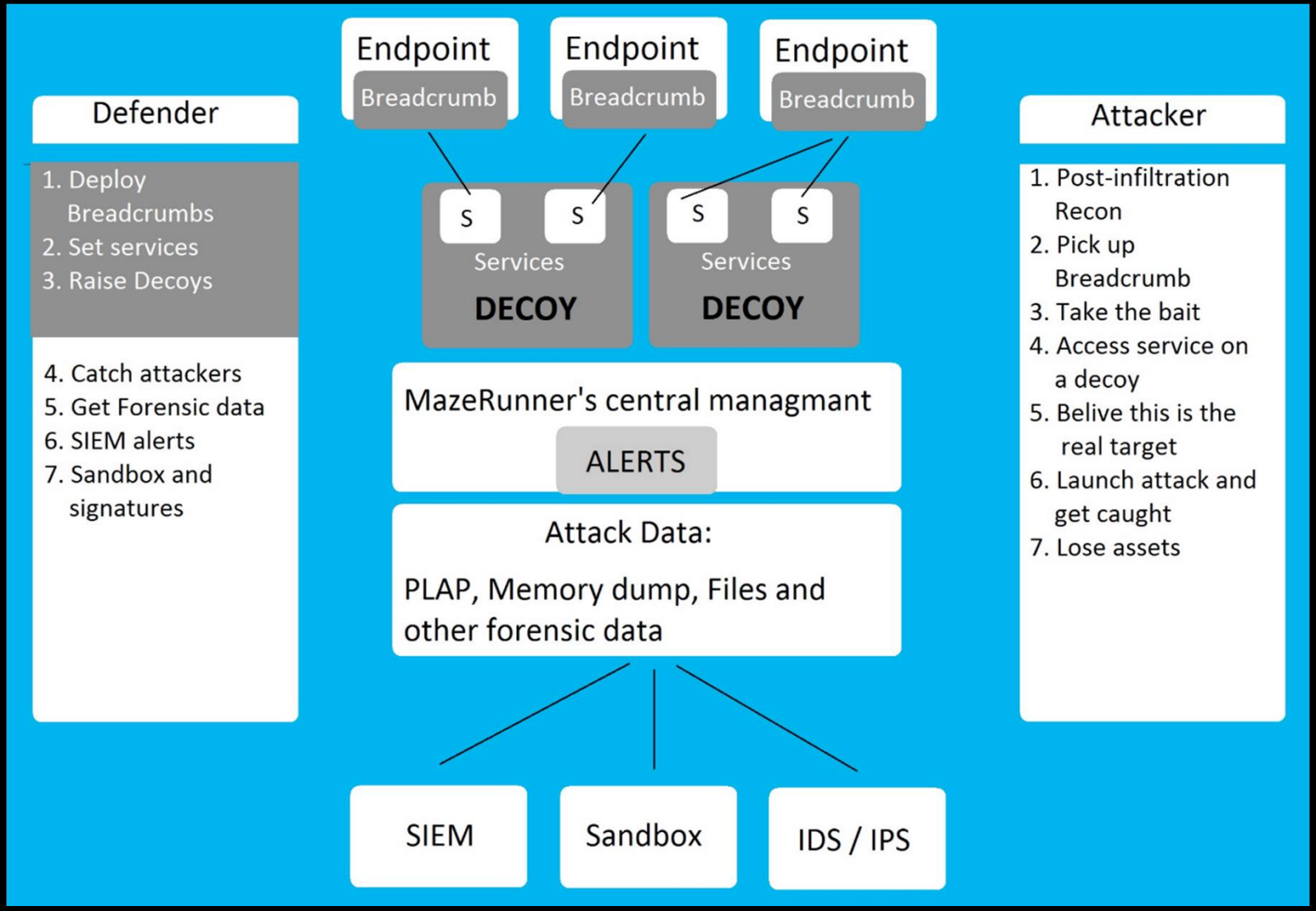
Mazerunner – Community Edition

- Dashboard – Your deception battle map, where you control and review your campaigns
- Campaign screen – Here you create the different components of your deception campaign
- Endpoints screen – This screen shows the endpoints on which you have placed breadcrumbs
- Investigation screen – Used for viewing your campaign's events and alerts. Here you can see every move an attacker has made

Mazerunner – Community Edition
Basic Architecture



Mazerunner – Community Edition Detailed Architecture



Deception campaign:

Decoys

- Virtual machines (servers or other devices) running Windows or Linux systems
- Look and act like production machines
- Reached by following a breadcrumb found on an endpoint

Deception campaign:

Services

- Each decoy server runs live services (e.g., SMB, SSH, OpenVPN servers, etc.)
- Each breadcrumb leads to a specific service on a decoy machine

Breadcrumbs

- Passive elements of data
- placed on endpoints to be found by attackers during the reconnaissance phase
- placed in a natural manner that is compatible with a user's habits

Deception campaign:

Demo’s

Honeyports vid:

https://www.youtube.com/watch?v=0YZjNdbTnoc

Mazerunner vid:

https://www.youtube.com/watch?v=E-dj4CtAdcE