RV CONNEX

ALPHAWOLF

CYBER INTELLIGENCE

ORACLE OF THE NEW ERA OF CYBER DEFENSE AND ITS DEPLOYMENT FOR AUDITORS

Supakorn Kungpisdan, Ph.D.

CISSP, CISA, CISM, PECB ISO 27001 PI, IRCA ISO27001 PA, PECB ISO 22301 PI, PECB ISO31000 RM, Security+, ITIL Foundation, C|CISO, E|CSA, C|EH, C|HFI, E|NSA, E|CES, C|EI, C|SCU, CCNA Instructor, CCNAS Instructor

Managing Director, Alpha Wolf

AGENDA

- R V CONNEX INTRODUCTION
- A HOLISTIC APPROACH FOR CYBER DEFENSE
- CYBER INTELLIGENCE

RVC CAPABILITIES

- SYSTEM INTEGRATION / SOFTWARE DEVELOPMENT
- UNMANNED AIRCRAFT SYSTEM: UAS
- AIRCRAFT AVIONIC SERVICES AND AIRCRAFT MODIFICATION SERVICE
- CYBER
- SATELLITES AND GROUND STATION

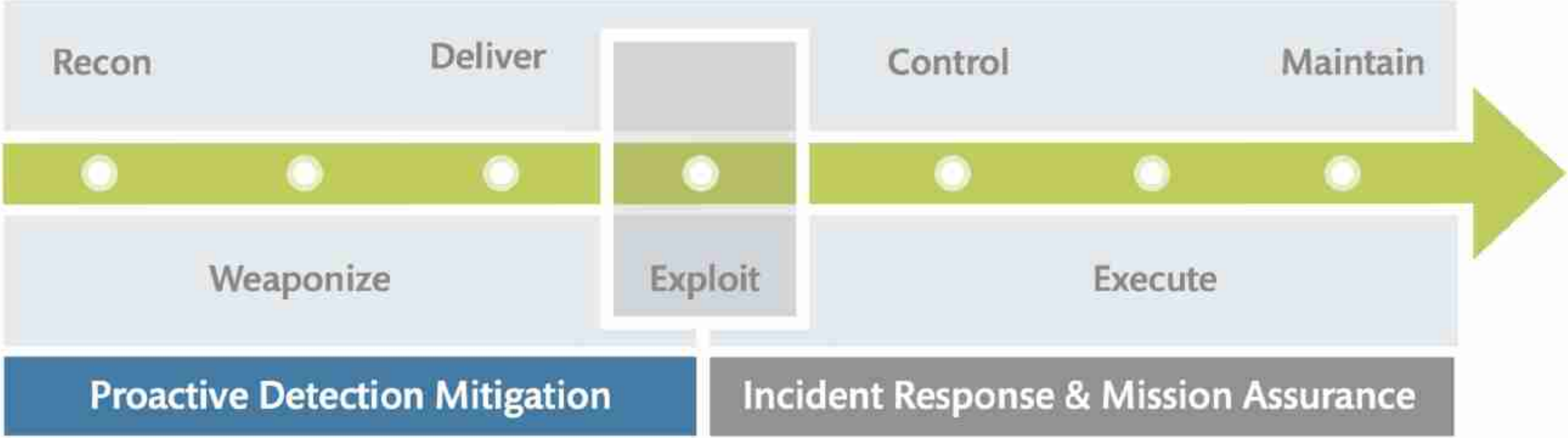
ALPHAWOLF R V CONNEX

A HOLISTIC APPROACH FOR CYBER DEFENSE

ALPHAWOLF

R V CONNEX

CYBER KILL CHAIN



Recon

Weaponize

Deliver

Exploit

Control

Execute

Maintain

Proactive Detection Mitigation

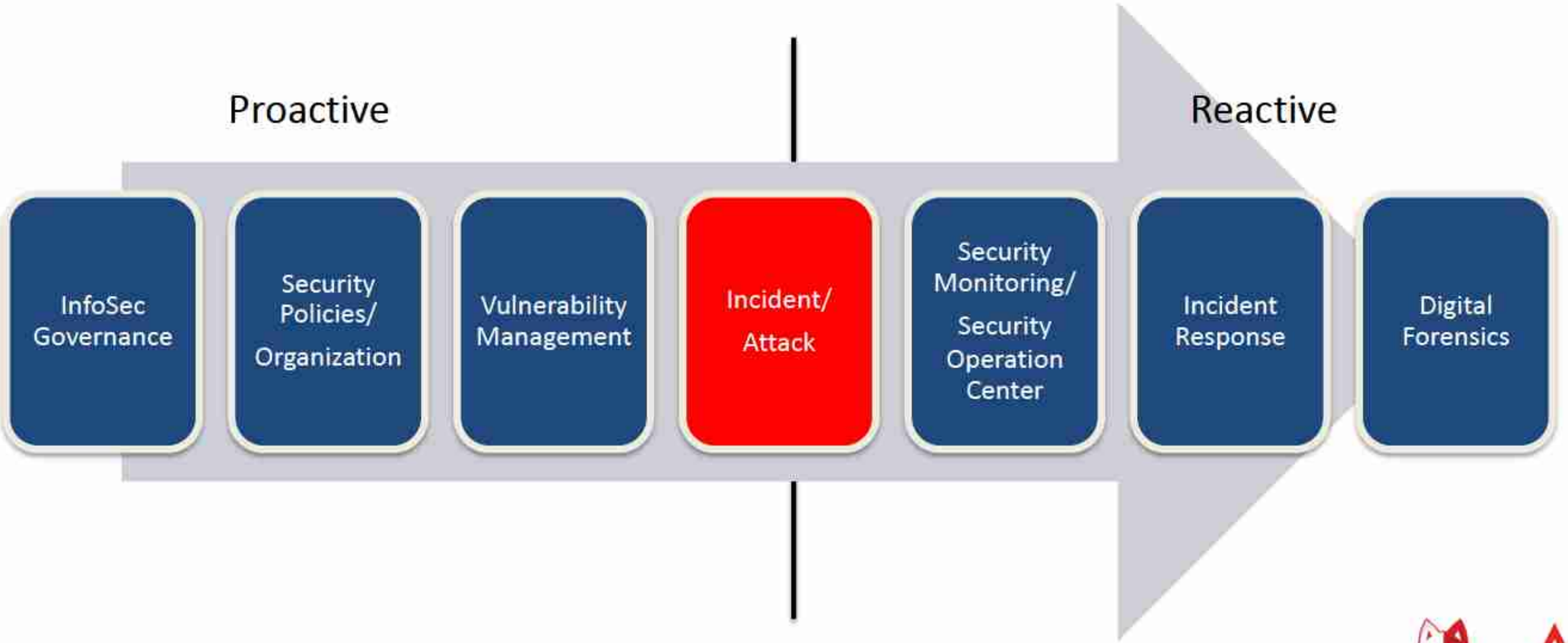
Incident Response & Mission Assurance

REF: https://www.mitre.org/sites/default/files/publications/active_defense_strategy.pdf

ALPHAWOLF

R V CONNEX

CYBERSECURITY MANAGEMENT TIMELINE



Proactive

Reactive

InfoSec Governance

Security Policies/ Organization

Vulnerability Management

Incident/ Attack

Security Monitoring/ Security Operation Center

Incident Response

Digital Forensics

ALPHAWOLF R V CONNEX

TESTING YOUR SECURITY PERIMETER

BEFORE SOMEONE DO

- VULNERBILITY ASSESSMENT
- PENETRATION TESTING
- APPLICATION SECURITY TESTING

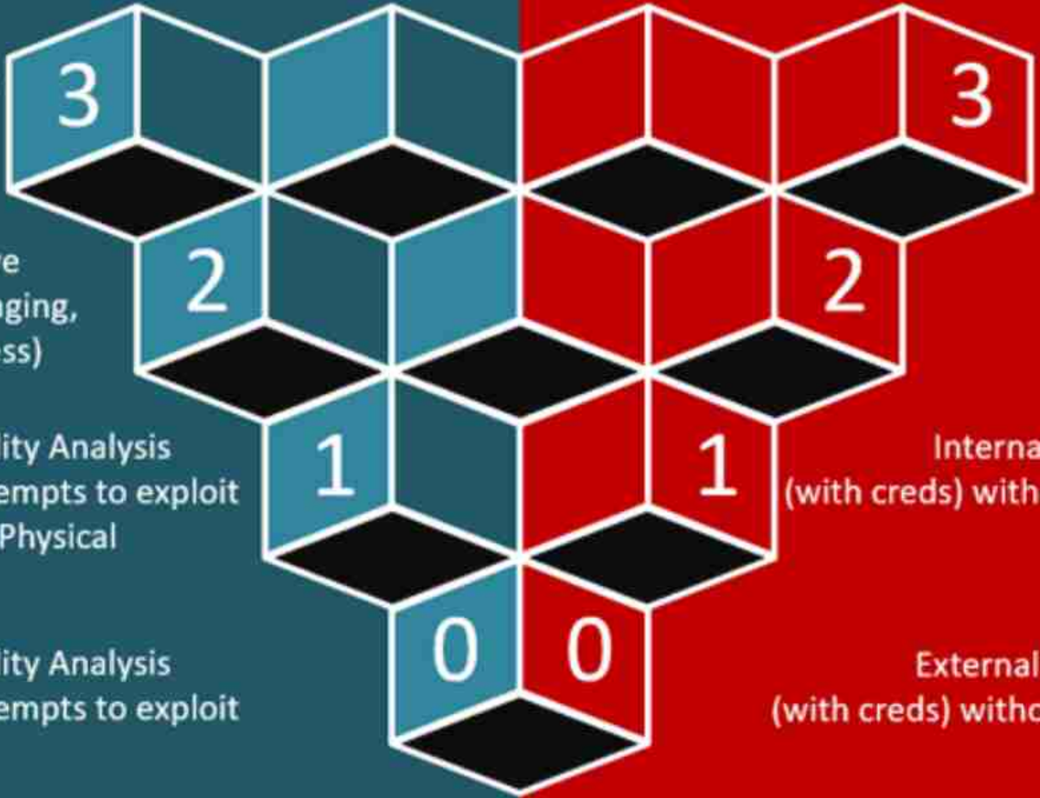
PENETRATION TESTING

3 “Oceans Eleven”
Active exploitation
Defined Objective
Web App Exploits

2 Phishing with Active content (not damaging, but persistent access)

1 External Vulnerability Analysis (no creds) with attempts to exploit
Phishing / OSINT / Physical

0 External Vulnerability Analysis (no creds) with attempts to exploit



VULNERABILITY SCANNING

Web Application Analysis 3

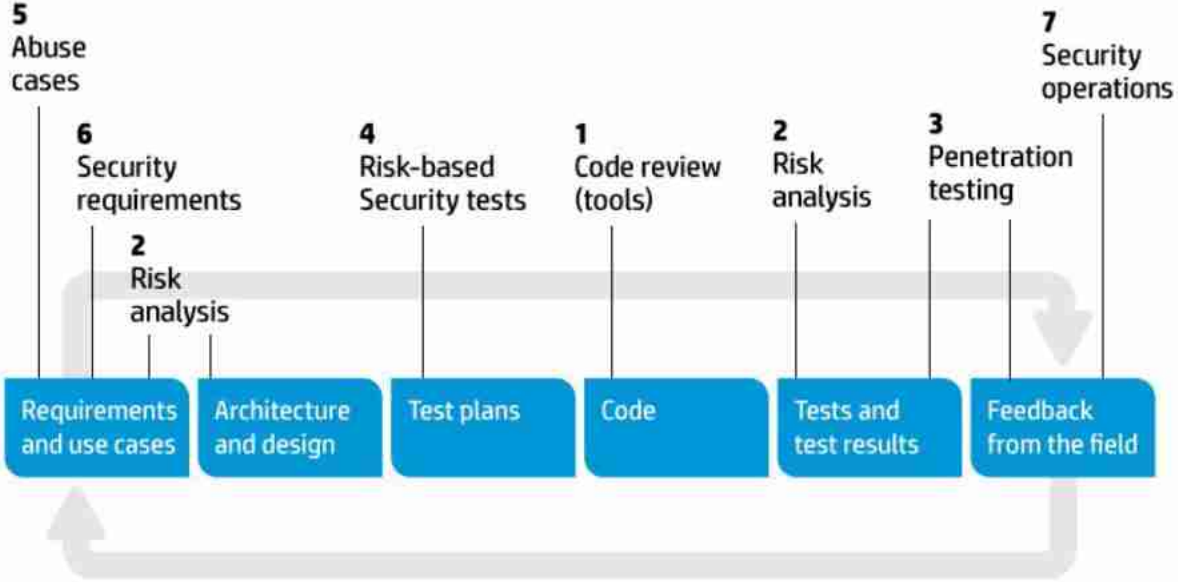
Wireless Vulnerability Scanning 2

Internal Vulnerability Analysis (with creds) without attempts to exploit 1

External Vulnerability Analysis (with creds) without attempts to exploit 0

REF: https://www.esentire.com/blog/cybersecurity-101-vulnerability-assessment-vs-penetration-testing/

7 touchpoints for software security



Gary McGraw's seven best-practice "touchpoints" for secure software development involve knowing and understanding common risks, designing for security, and subjecting all software artifacts to thorough, objective risk analyses and testing.

Source: "Software Security: Building Security In," by Gary McGraw

ALPHAWOLF R V CONNEX

TYPES OF CYBER ATTACKS

- BRUTEFORCE
- DDOS
- MALWARE
- RANSOMWARE
- WEBPAGE DEFACEMENT
- SQL INJECTION
- CROSS-SITE SCRIPT (XSS)
- SPAM
- PHISHING

ALPHAWOLF R V CONNEX

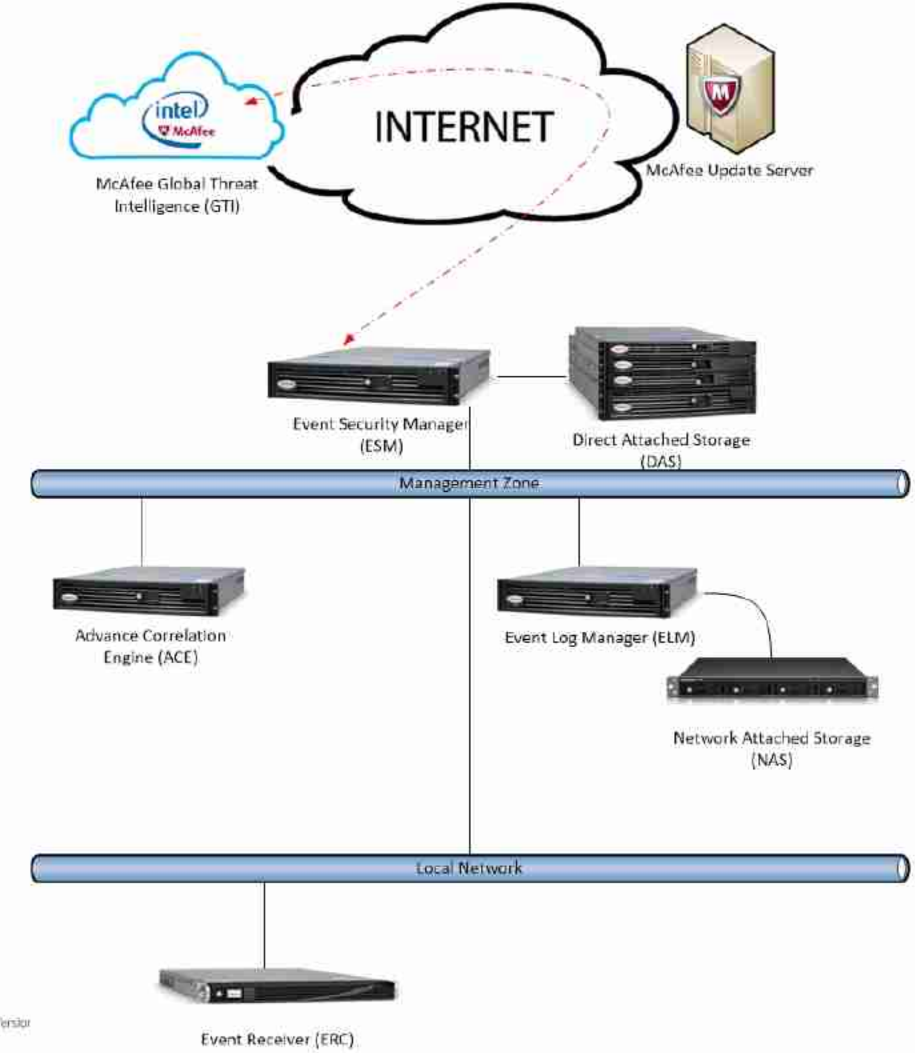
DETECTING CYBER ATTACKS

- LOG ANALYSIS
- FILE INTEGRITY MONITORING
- INTRUSION DETECTION/PREVENTION
- MALWARE DETECTION
- NETWORK MONITORING
- NETWORK FORENSICS
- DATA LOSS PREVENTION
- DDOS DETECTION
- EMAIL SECURITY GATEWAY
- AUTHENTICATION GATEWAY
- NETWORK ACCESS CONTROL

ALPHAWOLF

R V CONNEX

CYBERSECURITY OPERATION CENTER


intel
McAfee
McAfee Global Threat Intelligence (GTI)
INTERNET
McAfee Update Server
Event Security Manager (ESM)
Direct Attached Storage (DAS)
Management Zone
Advance Correlation Engine (ACE)
Event Log Manager (ELM)
Network Attached Storage (NAS)
Local Network
Event Receiver (ERC)

SIEM

SECURITY INFORMATION AND EVENT MANAGEMENT

LOG SOURCES

- SECURITY DEVICES
- ENDPOINTS
- NETWORK DEVICES
- ETC.

ALPHAWOLF R V CONNEX

CYBERSECURITY OPERATION CENTER

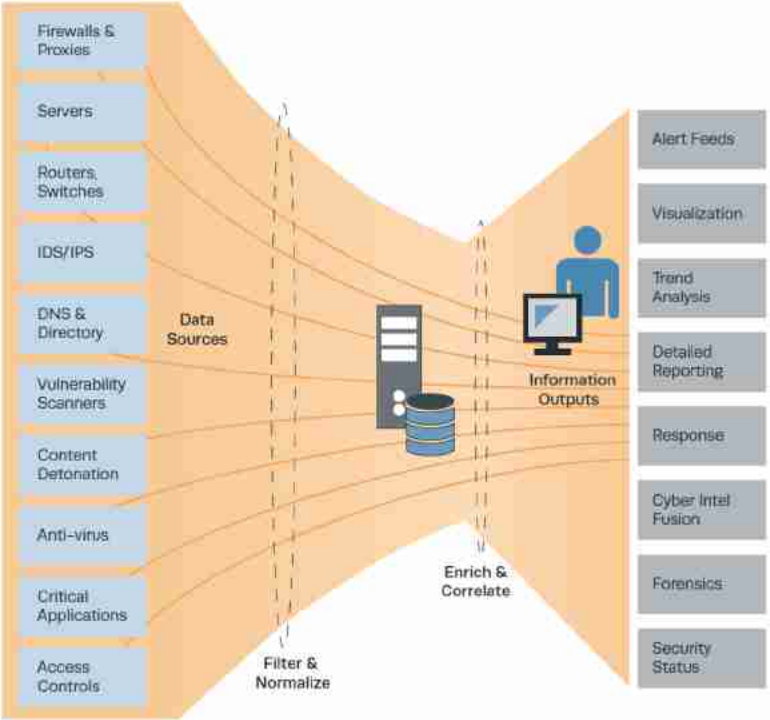
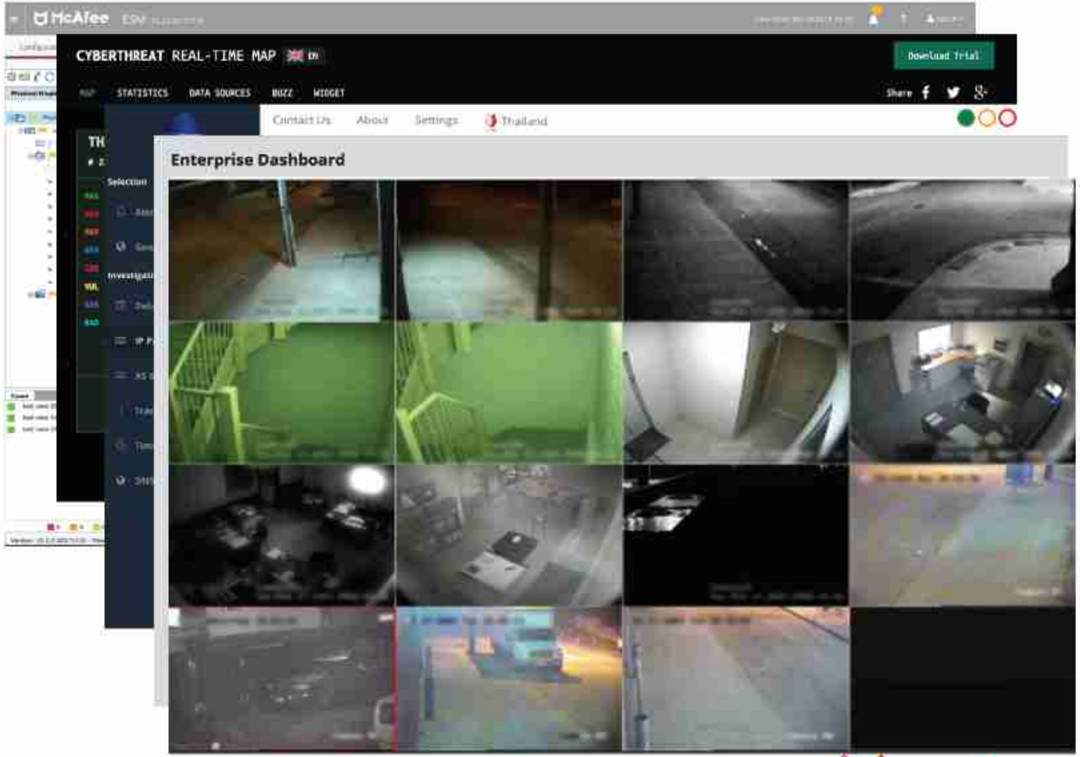


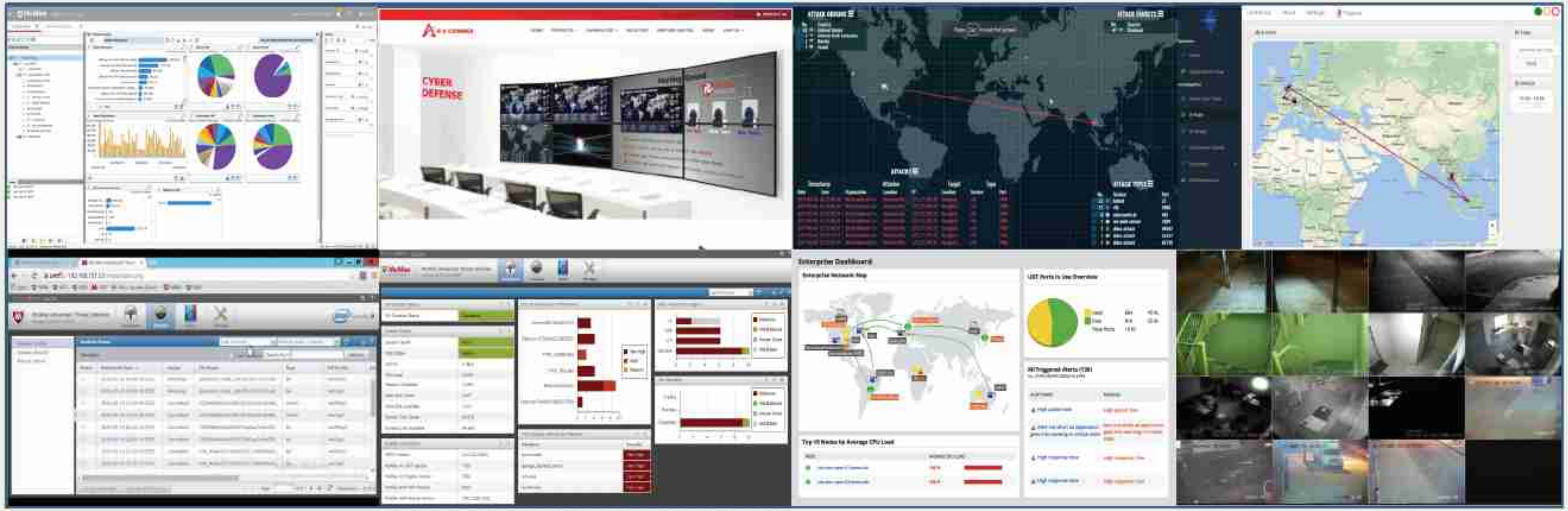
Figure 21. SIEM Overview



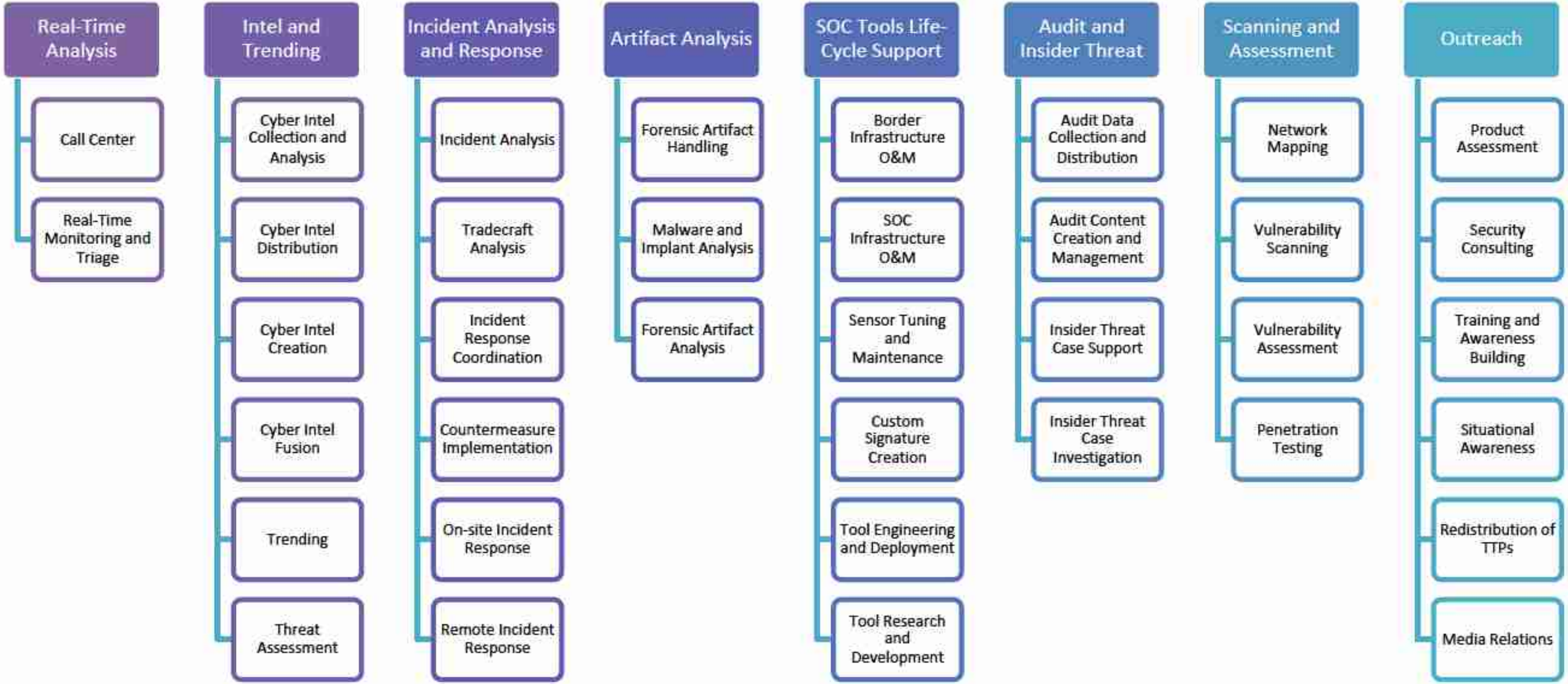
ALPHAWOLF

R V CONNEX

CSOC DASHBOARD EXAMPLE



ALPHAWOLF R V CONNEX



Real-Time Analysis
- Call Center
- Real-Time Monitoring and Triage

Intel and Trending
- Cyber Intel Collection and Analysis
- Cyber Intel Distribution
- Cyber Intel Creation
- Cyber Intel Fusion
- Trending
- Threat Assessment

Incident Analysis and Response
- Incident Analysis
- Tradecraft Analysis
- Incident Response Coordination
- Countermeasure Implementation
- On-site Incident Response
- Remote Incident Response

Artifact Analysis
- Forensic Artifact Handling
- Malware and Implant Analysis
- Forensic Artifact Analysis

SOC Tools Life-Cycle Support
- Border Infrastructure O&M
- SOC Infrastructure O&M
- Sensor Tuning and Maintenance
- Custom Signature Creation
- Tool Engineering and Deployment
- Tool Research and Development

Audit and Insider Threat
- Audit Data Collection and Distribution
- Audit Content Creation and Management
- Insider Threat Case Support
- Insider Threat Case Investigation

Scanning and Assessment
- Network Mapping
- Vulnerability Scanning
- Vulnerability Assessment
- Penetration Testing

Outreach
- Product Assessment
- Security Consulting
- Training and Awareness Building
- Situational Awareness
- Redistribution of TTPs
- Media Relations

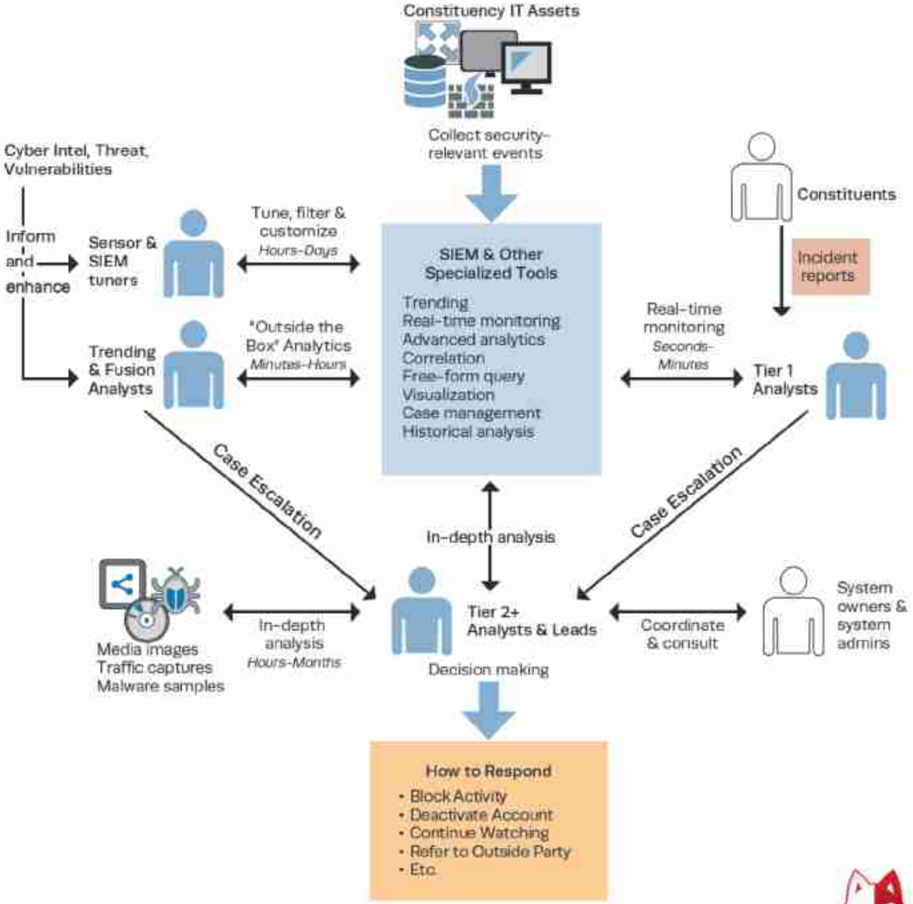
REF: mitre.org

ALPHAWOLF

R V CONNEX

INCIDENT HANDLING PROCESSES

- DDOS
- PHISHING & SPAM
- MALWARE
- RANSOMWARE
- WEBPAGE DEFACEMENT
- SQL INJECTION & XSS
- DB ATTACKS
- SERVER ATTACKS
- MISCONFIGURATION



Constituency IT Assets

Collect security-relevant events

Cyber Intel, Threat, Vulnerabilities

Inform and enhance

Sensor & SIEM tuners

Tune, filter & customize
Hours-Days

Trending & Fusion Analysts

"Outside the Box" Analytics
Minutes-Hours

SIEM & Other Specialized Tools

Trending
Real-time monitoring
Advanced analytics
Correlation
Free-form query
Visualization
Case management
Historical analysis

Constituents

Incident reports

Real-time monitoring
Seconds-Minutes

Tier 1 Analysts

Case Escalation

Case Escalation

In-depth analysis

Media images
Traffic captures
Malware samples

In-depth analysis
Hours-Months

Tier 2+ Analysts & Leads

Decision making

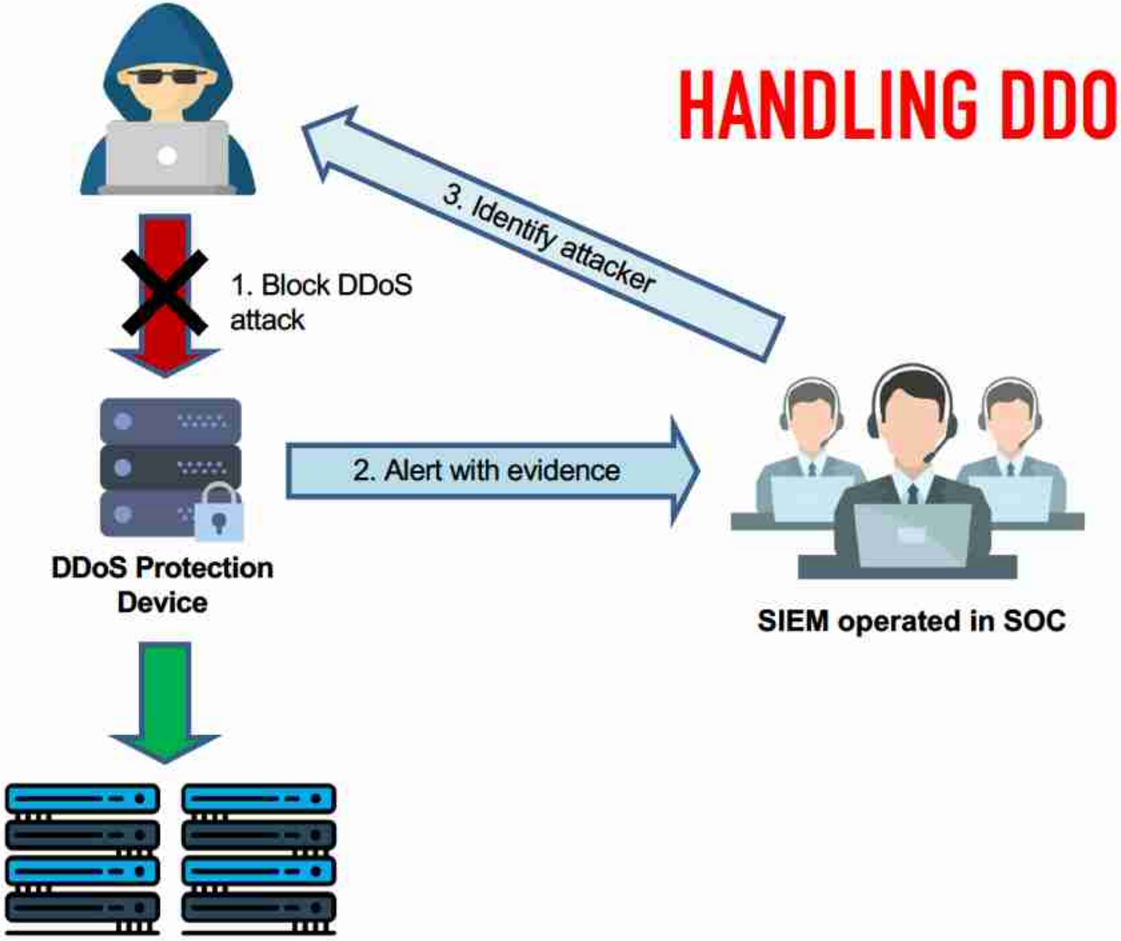
Coordinate & consult

System owners & system admins

How to Respond

- Block Activity
- Deactivate Account
- Continue Watching
- Refer to Outside Party
- Etc

HANDLING DDOS ATTACK



1. Block DDoS attack

2. Alert with evidence

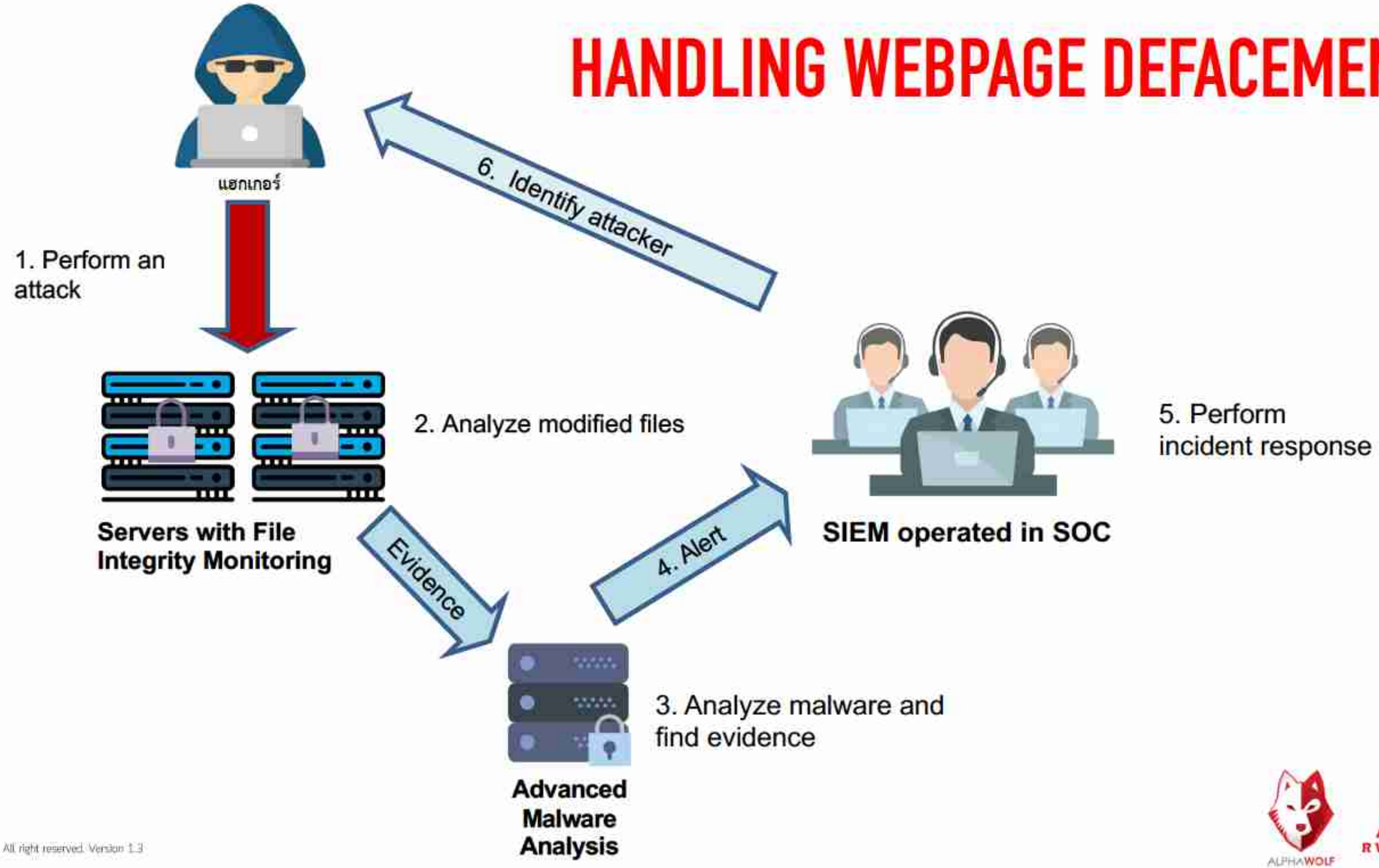
3. Identify attacker

DDoS Protection Device

SIEM operated in SOC

Internal networks & servers

HANDLING WEBPAGE DEFACEMENT



แฮกเกอร์

1. Perform an attack

Servers with File Integrity Monitoring

2. Analyze modified files

Evidence

Advanced Malware Analysis

3. Analyze malware and find evidence

4. Alert

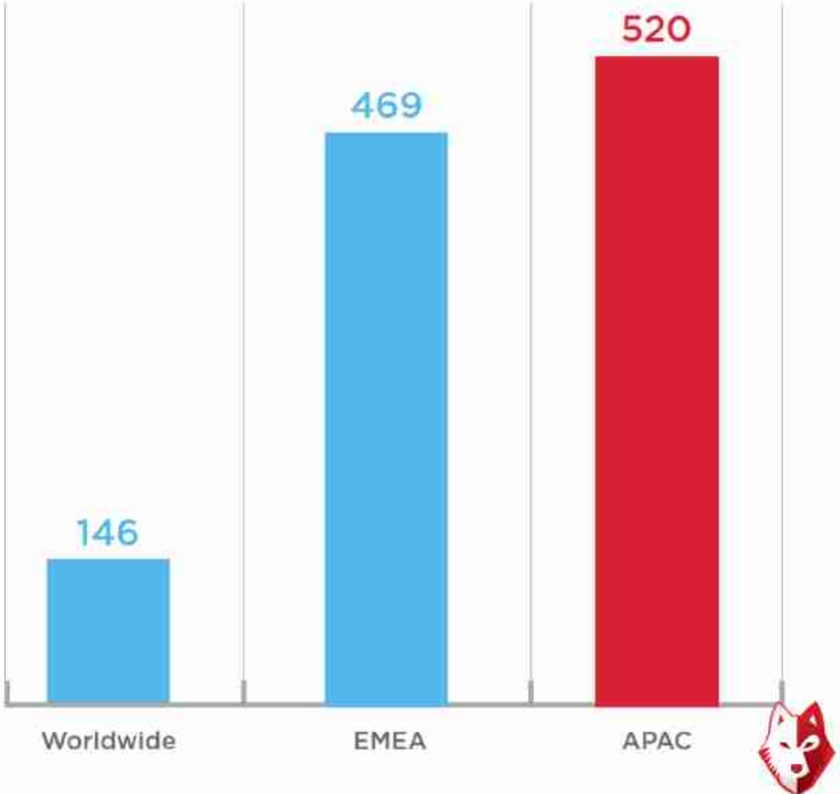
SIEM operated in SOC

5. Perform incident response

6. Identify attacker

DAYS UNTIL BREACH IS DISCOVERED

The lower global statistic includes the U.S., where the security maturity baseline is higher and proactive hunting for malicious activity is becoming a key capability of organizations' security teams.



REF: M-Trends 2016, APAC Edition

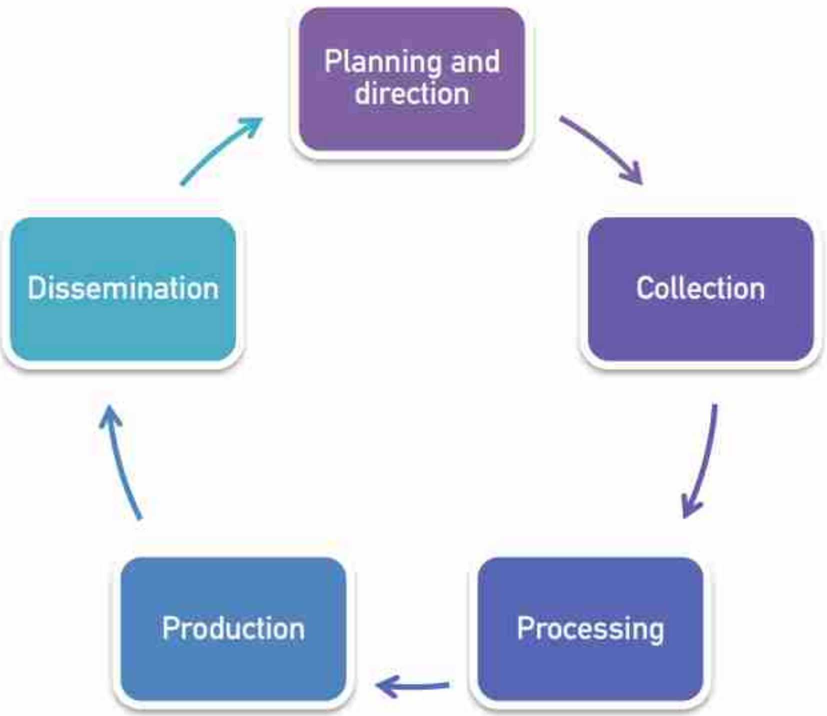
CYBER INTELLIGENCE

DEFINITION OF CYBER INTELLIGENCE

- The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations

REF: https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/

INTELLIGENCE CYCLE



REF: https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/

CYBER THREAT INTELLIGENCE (CTI)

Cyber Threat Intelligence (CTI) is based on the collection of intelligence using open source intelligence (OSINT), social media intelligence (SOCMINT), human Intelligence (HUMINT) or intelligence from the deep and dark web. CTI's key mission is to research and analyze trends and technical developments in three areas:

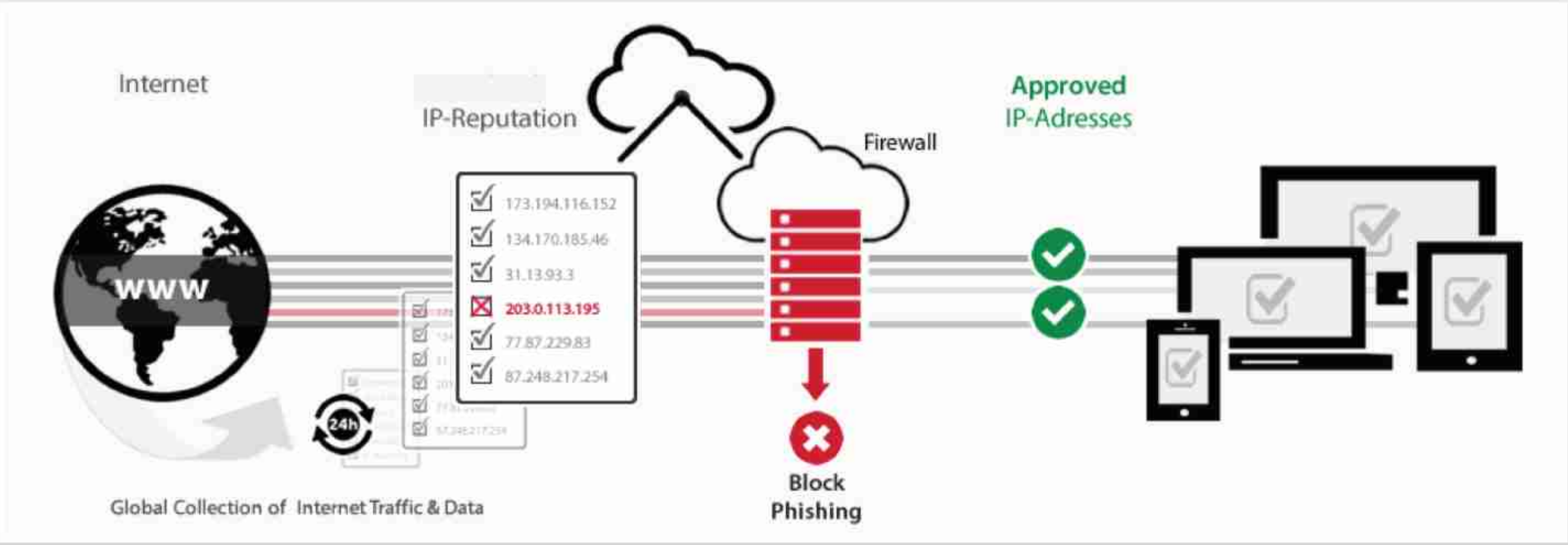
- Cyber crime
- Cyber hactivism
- Cyber espionage (advanced persistent threat or APT)

INTELLIGENCE GATHERED

- Attacker source IP ranges
- Malware metadata
- Typical hardware/software leveraged by the attacker
- Typical hardware/software targeted by the attacker
- Typical times of attacker operations (i.e. typically active between 0400 – 0900 GMT on Thursday, Friday, or Saturday)
- Hardware/software used to access the sensitive data and business processes
- Patch level and patching schedule for identified hardware and software
- Previous attack information (If available)
- Detailed identity and access information associated with the resources (i.e. who can access them, and what privileges do they have?)

ALPHAWOLF R V CONNEX

IP REPUTATION / FILE REPUTATION / URL REPUTATION



Internet

IP-Reputation

☑ 173.194.116.152

☑ 134.170.185.46

☑ 31.13.93.3

☒ 203.0.113.195

☑ 77.87.229.83

☑ 87.248.217.254

Firewall

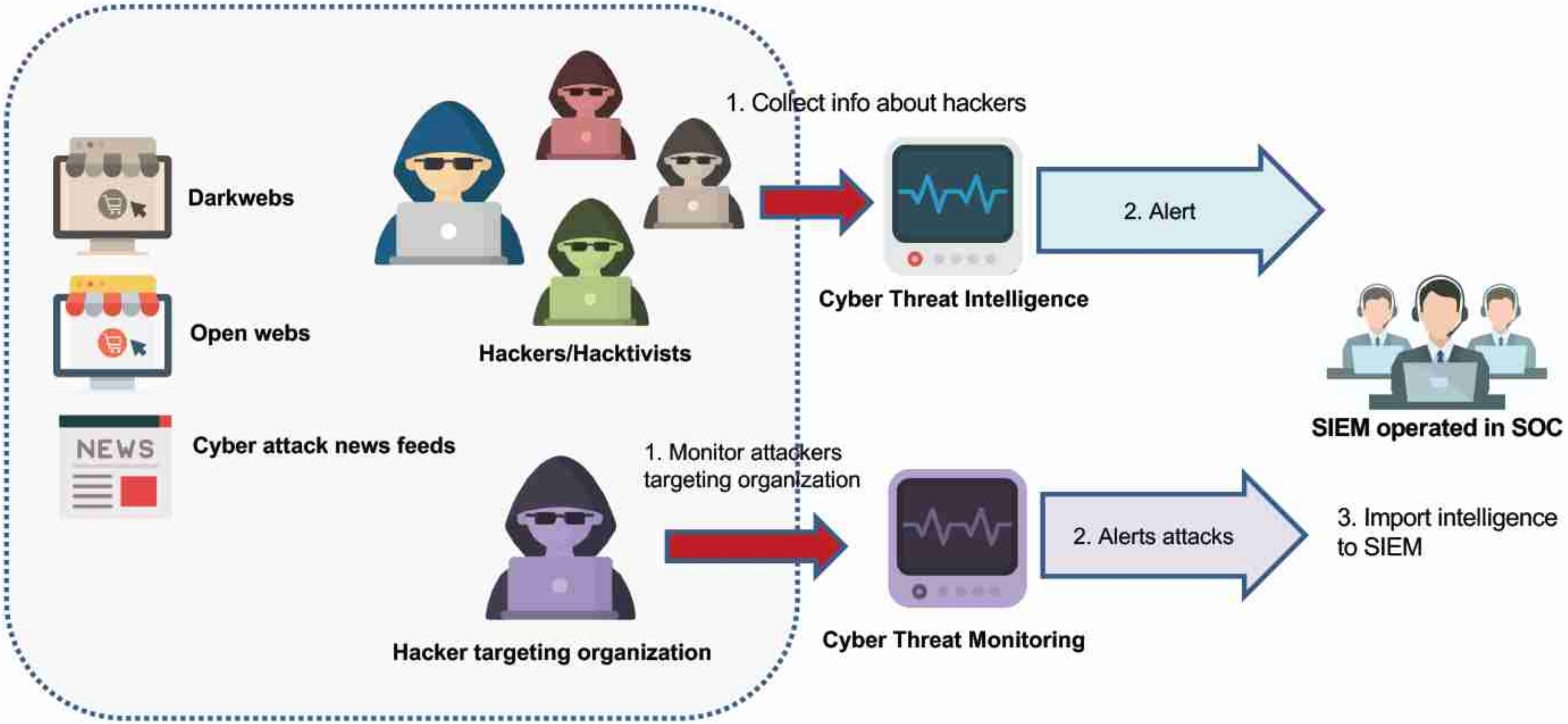
Approved IP-Adresses

Block Phishing

Global Collection of Internet Traffic & Data

OUTSIDE-IN CYBER MONITORING

CYBER MONITORING FROM HACKER'S POINT OF VIEW



Darkwebs

Open webs

Cyber attack news feeds

Hackers/Hacktivists

Hacker targeting organization

1. Collect info about hackers

Cyber Threat Intelligence

2. Alert

1. Monitor attackers targeting organization

Cyber Threat Monitoring

2. Alerts attacks

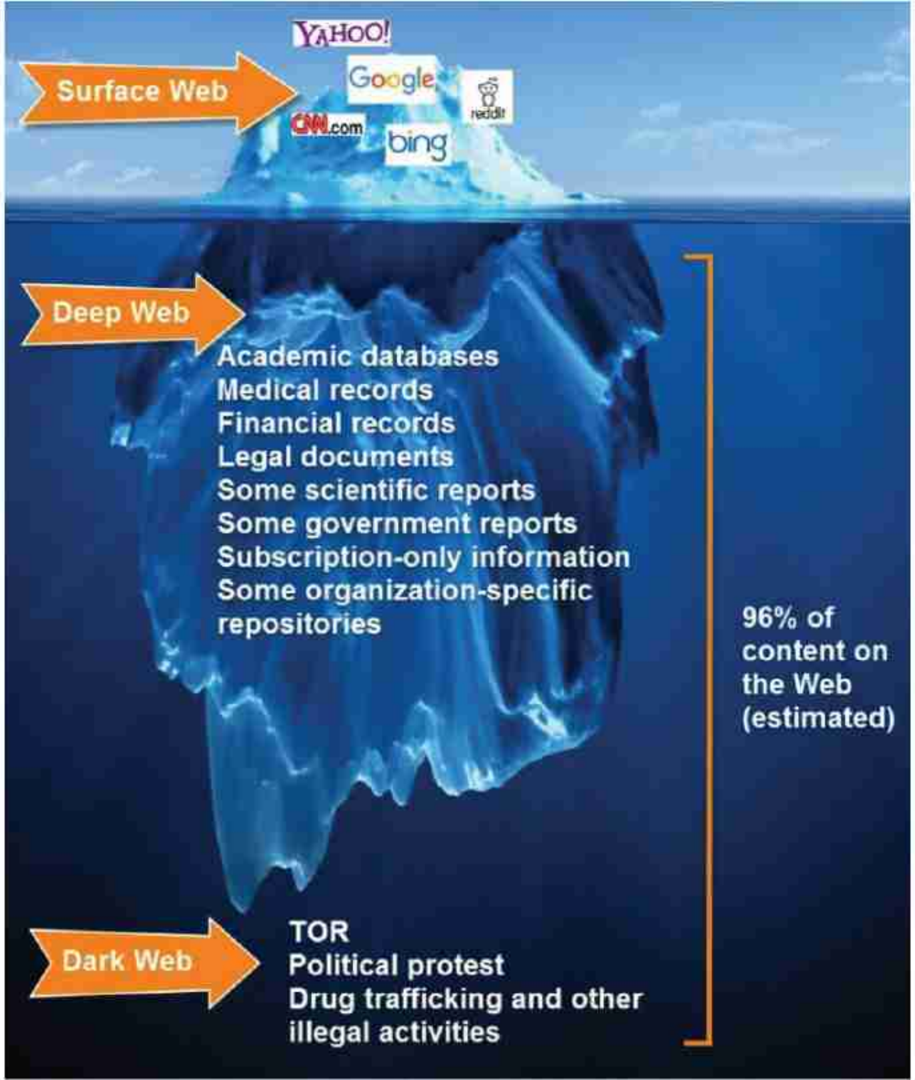
SIEM operated in SOC

3. Import intelligence to SIEM

ALPHAWOLF R V CONNEX

DARKNET INTELLIGENCE

DARKNET / DARKWEB



Surface Web

Deep Web

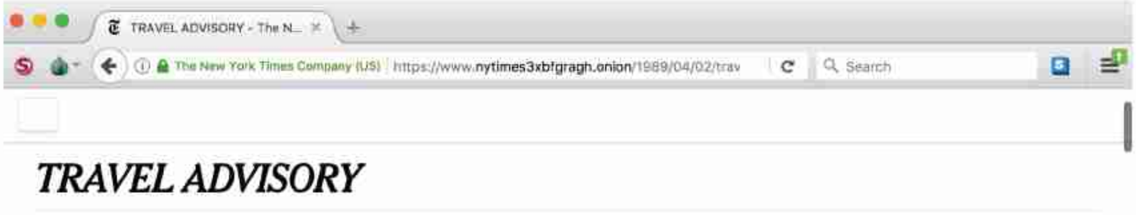
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription-only information
Some organization-specific repositories

Dark Web

TOR
Political protest
Drug trafficking and other illegal activities

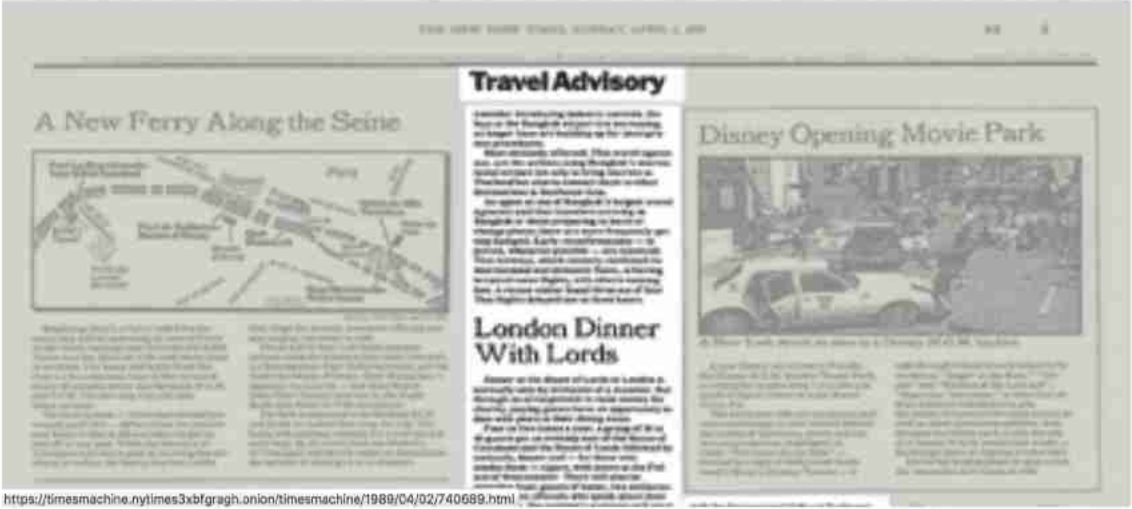
96% of content on the Web (estimated)

ACCESSING DARKNET


TRAVEL ADVISORY - The N...
The New York Times Company (US)
https://www.nytimes3xbfgragh.onion/1989/04/02/trav
Search

TRAVEL ADVISORY

https://www.nytimes3xbfgragh.onion/1989/04/02/travel/travel-advisory-740689.html



Travel Advisory

A New Ferry Along the Seine

Disney Opening Movie Park

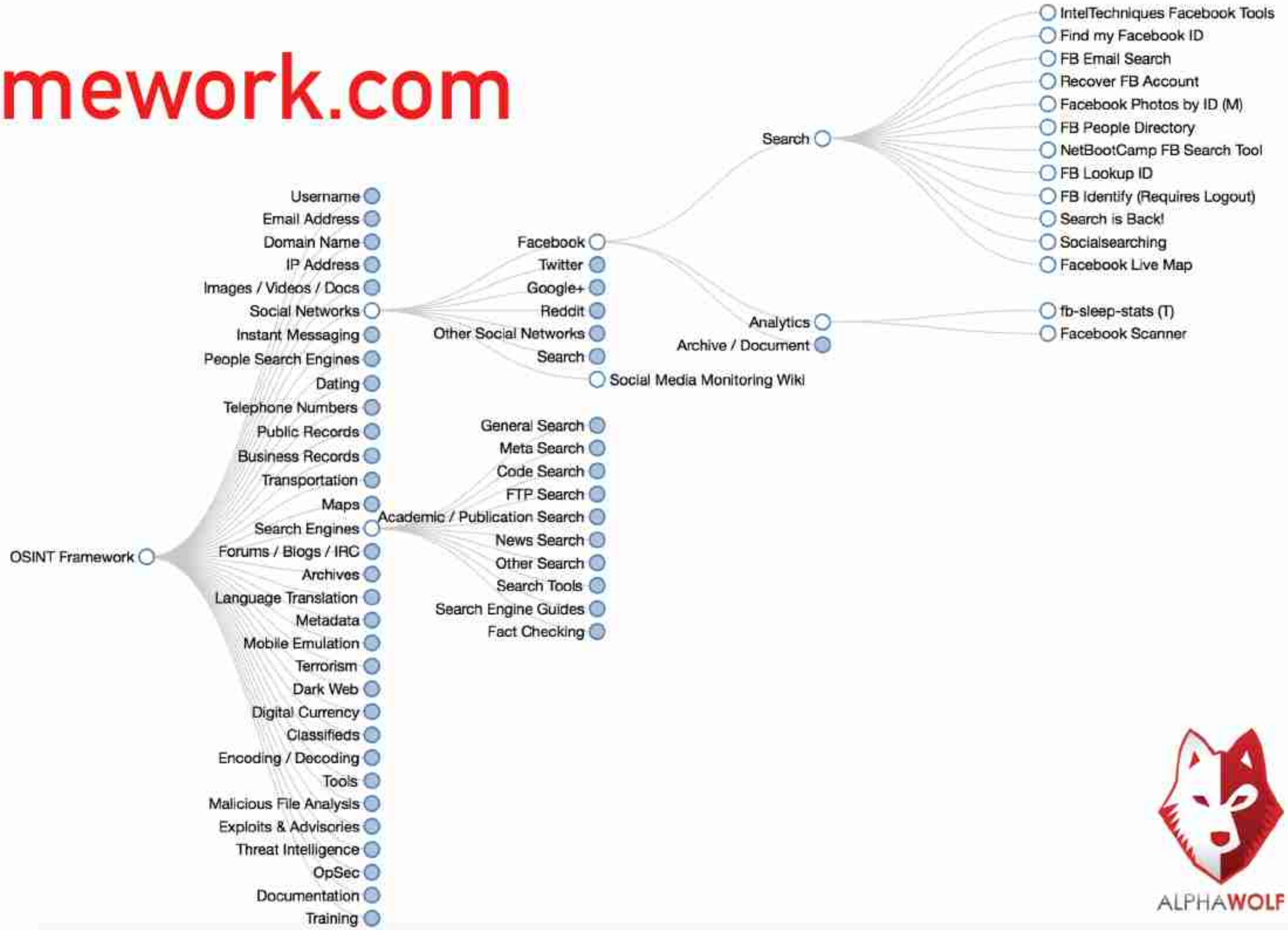
London Dinner With Lords

https://timesmachine.nytimes3xbfgragh.onion/timesmachine/1989/04/02/740689.html

ALPHAWOLF R V CONNEX

SOCIAL MEDIA INTELLIGENCE

osintframework.com



OSINT Framework

Username
Email Address
Domain Name
IP Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Maps
Search Engines
Forums / Blogs / IRC
Archives
Language Translation
Metadata
Mobile Emulation
Terrorism
Dark Web
Digital Currency
Classifieds
Encoding / Decoding
Tools
Malicious File Analysis
Exploits & Advisories
Threat Intelligence
OpSec
Documentation
Training

Facebook
Twitter
Google+
Reddit
Other Social Networks
Search
Social Media Monitoring Wiki

General Search
Meta Search
Code Search
FTP Search
Academic / Publication Search
News Search
Other Search
Search Tools
Search Engine Guides
Fact Checking

Search
Analytics
Archive / Document

IntelTechniques Facebook Tools
Find my Facebook ID
FB Email Search
Recover FB Account
Facebook Photos by ID (M)
FB People Directory
NetBootCamp FB Search Tool
FB Lookup ID
FB Identify (Requires Logout)
Search is Back!
Socialsearching
Facebook Live Map

fb-sleep-stats (T)
Facebook Scanner

ALPHAWOLF

R V CONNEX

TRANSFORMING POTENTIAL

www.rvconnex.com

THANK YOU