THE GREATEST GIFT

Bill Swearingen / CYBER DEFENSE

BILL SWEARINGEN

DIRECTOR OF CYBER DEFENSE, CENTURYLINK

Cyber Incident Response Team

Cybersecurity Vulnerability Services

Corporate Forensics

Cybersecurity Infrastructure and Architecture

Internet Security Services

Defenders have to get security right every time

An attacker only has to ***get it right once.***

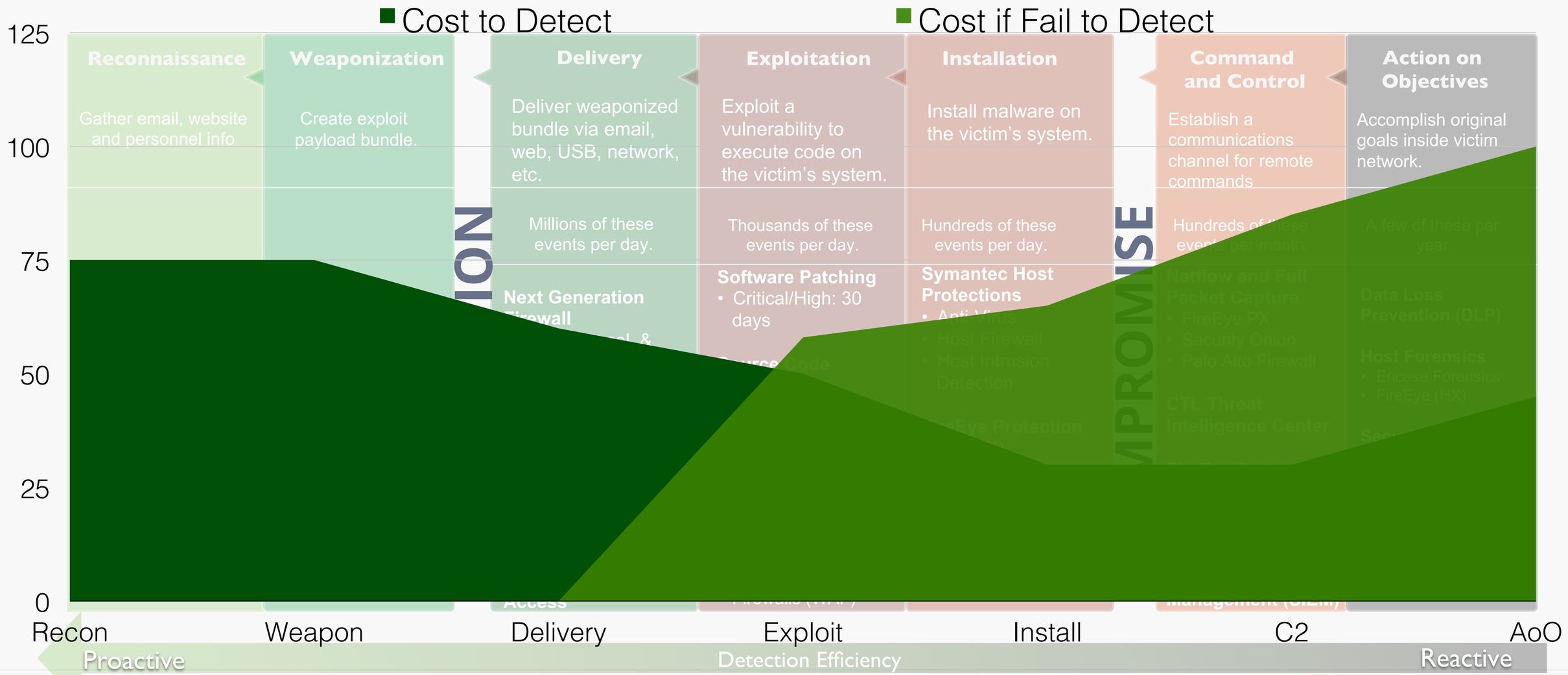
Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Action on Objectives
Gather email, website and personnel info	Create exploit payload bundle.	Deliver weaponized bundle via email, web, USB, network, etc.	Exploit a vulnerability to execute code on the victim's system.	Install malware on the victim's system.	Establish a communications channel for remote commands	Accomplish original goals inside victim network.
		Millions of these events per day.	Thousands of these events per day.	Hundreds of these events per day.	Hundreds of these events per month.	A few of these per year.
		• Port, Protocol, & State Analysis • Default deny policy • User Awareness • Threat Intelligence Feed **Email Gateway** 98.9% of all inbound email is filtered (spam or phishing) **Two Factor Remote Access**	**Software Patching** **Source Code Analysis** **Intrusion Detection Systems** **Advanced Network Protection**	**Host Protections** • Anti-Virus • Host Firewall • Host Intrusion Detection **Limited administrator rights** **Endpoint visibility**	**Network Visibility** **Netflow and Full Packet Capture** **CTL Threat Intelligence Center** **Security Information and Event Management (SIEM)**	**Data Loss Prevention (DLP)** **Host Forensics** **Security Information and Event Management (SIEM)** **System Backup**

DETECTION

COMPROMISE

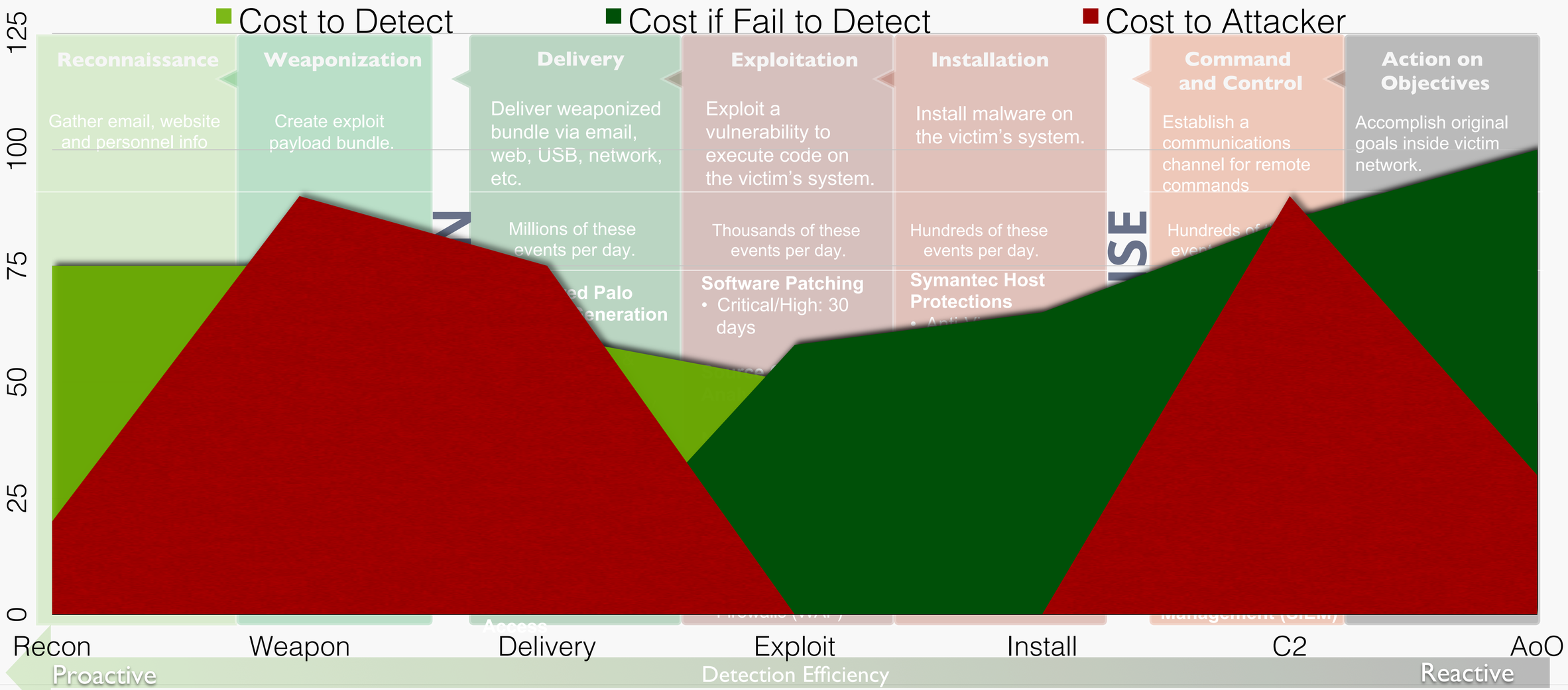
Proactive — Detection Efficiency — Reactive

CYBER KILL CHAIN



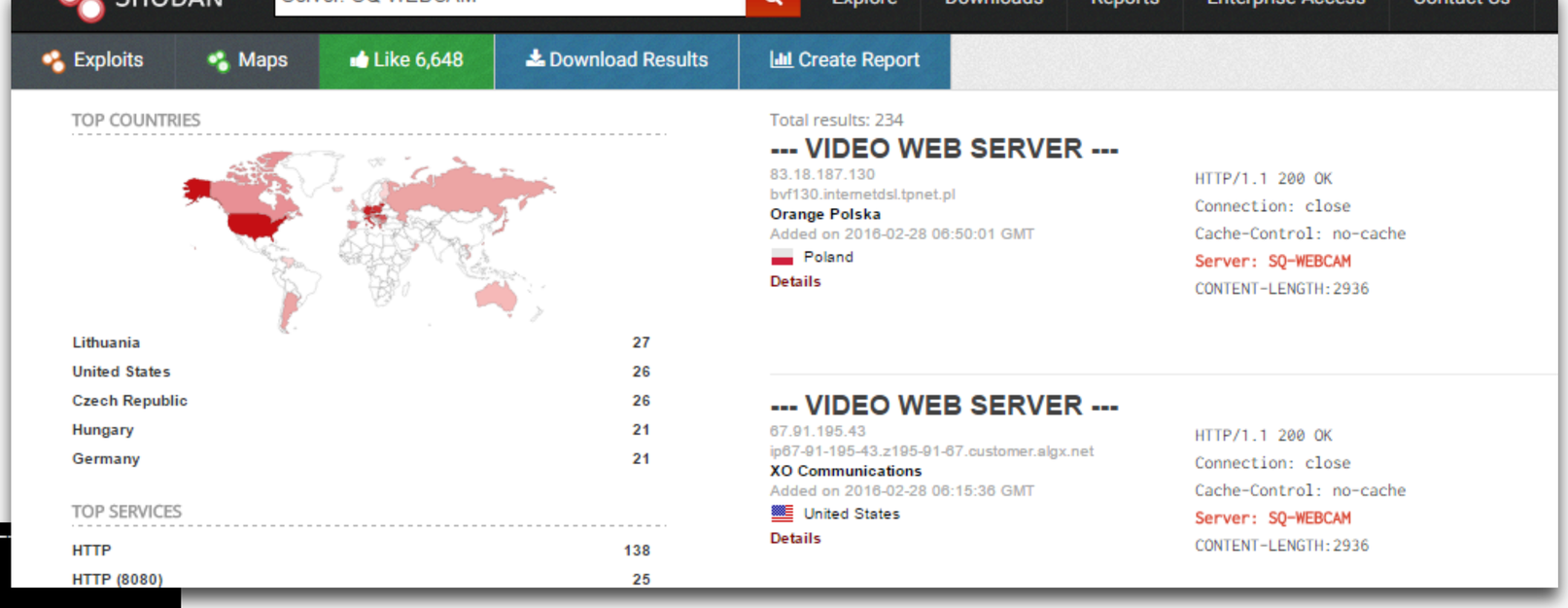
THE ATTACKER

CYBER KILL CHAIN



SHODAN

WPScan®




```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.9.1
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.
```

Google Dork

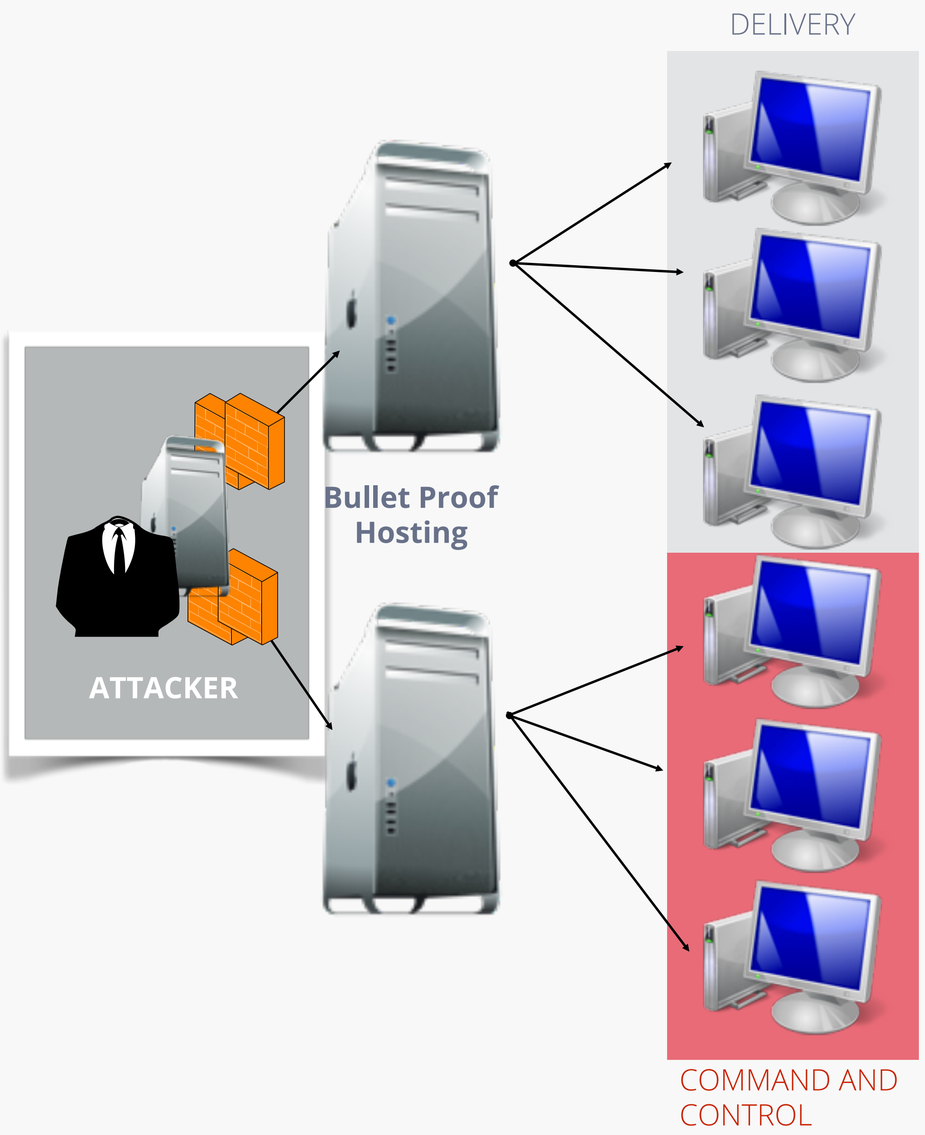
"index of" inurl:wp-content/

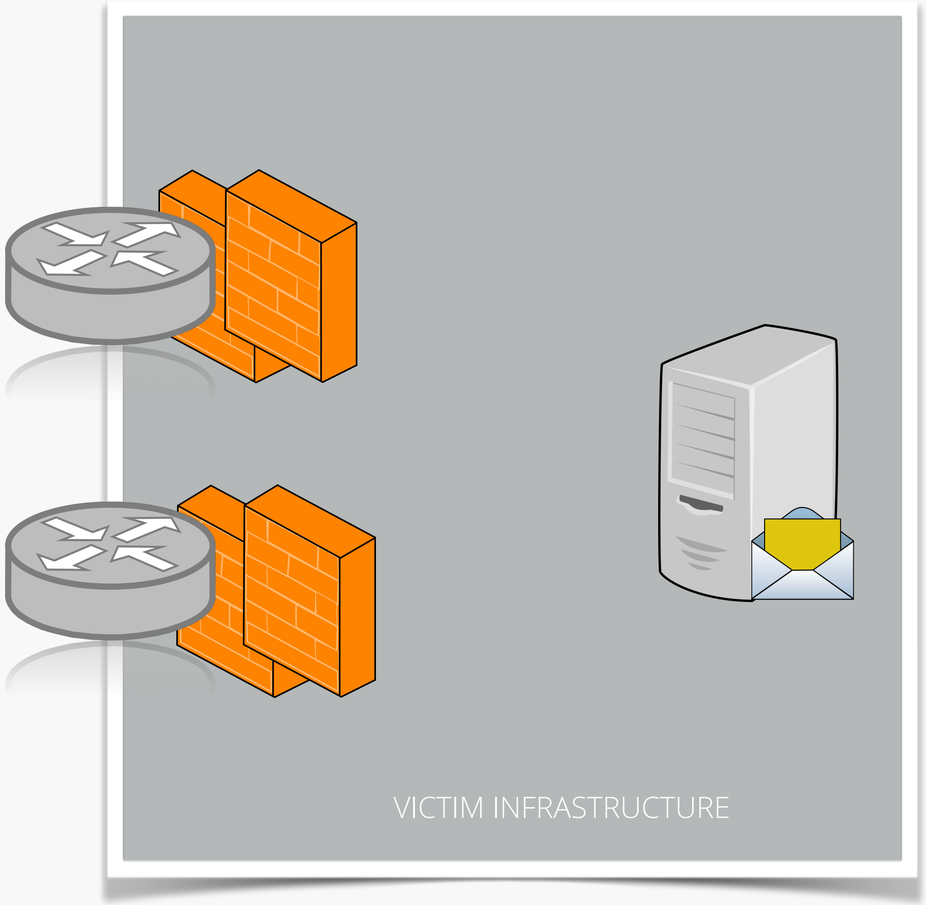
"inurl:"/wp-content/plugins/wp-shopping-cart/"

"inurl:wp-content/plugins/wp-dbmanager/"

Specific plugins are targeted when critical vulnerabilities and exploits are published

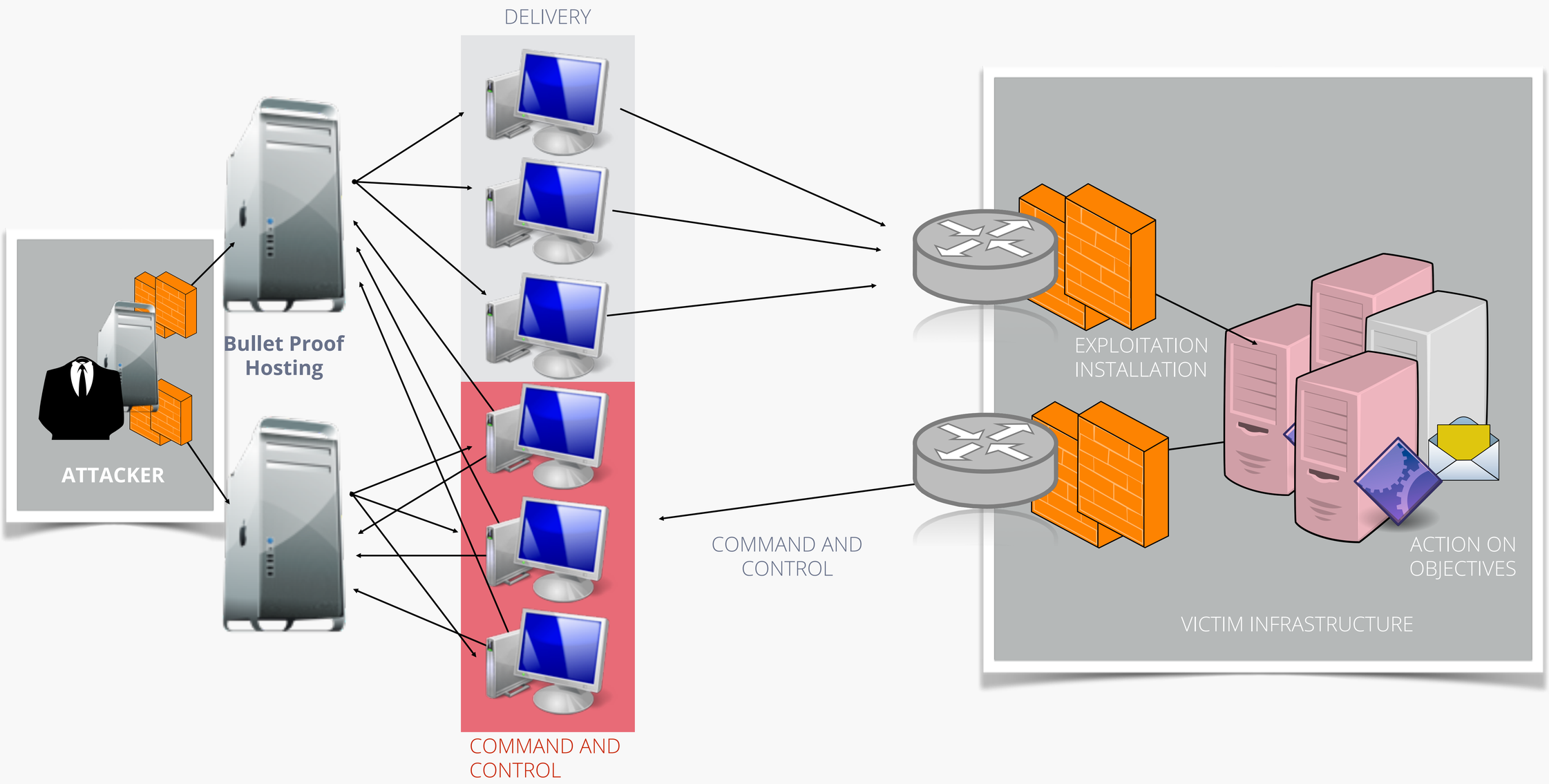
ATTACK INFRASTRUCTURE





Reconnaissance | Weaponization

ATTACK INFRASTRUCTURE



Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Action on Objectives

Will the red team please stand up.

CYBER KILL CHAIN

Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command and Control	Action on Objectives
Gather email, website and personnel info	Create exploit payload bundle.	Deliver weaponized bundle via email, web, USB, network, etc.	Exploit a vulnerability to execute code on the victim's system.	Install malware on the victim's system.	Establish a communications channel for remote commands	Accomplish original goals inside victim network.
		Millions of these events per day.	Thousands of these events per day.	Hundreds of these events per day.	Hundreds of these events per month.	A few of these per year.
		• Port, Protocol, & State Analysis • Default deny policy • User Awareness • Threat Intelligence Feed **Email Gateway** 98.9% of all inbound email is filtered (spam or phishing) **Two Factor Remote Access**	**Software Patching** **Source Code Analysis** **Intrusion Detection Systems** **Advanced Network Protection**	**Host Protections** • Anti-Virus • Host Firewall • Host Intrusion Detection **Limited administrator rights** **Endpoint visibility**	**Network Visibility** **Netflow and Full Packet Capture** **CTL Threat Intelligence Center** **Security Information and Event Management (SIEM)**	**Data Loss Prevention (DLP)** **Host Forensics** **Security Information and Event Management (SIEM)** **System Backup**

DETECTION

COMPROMISE

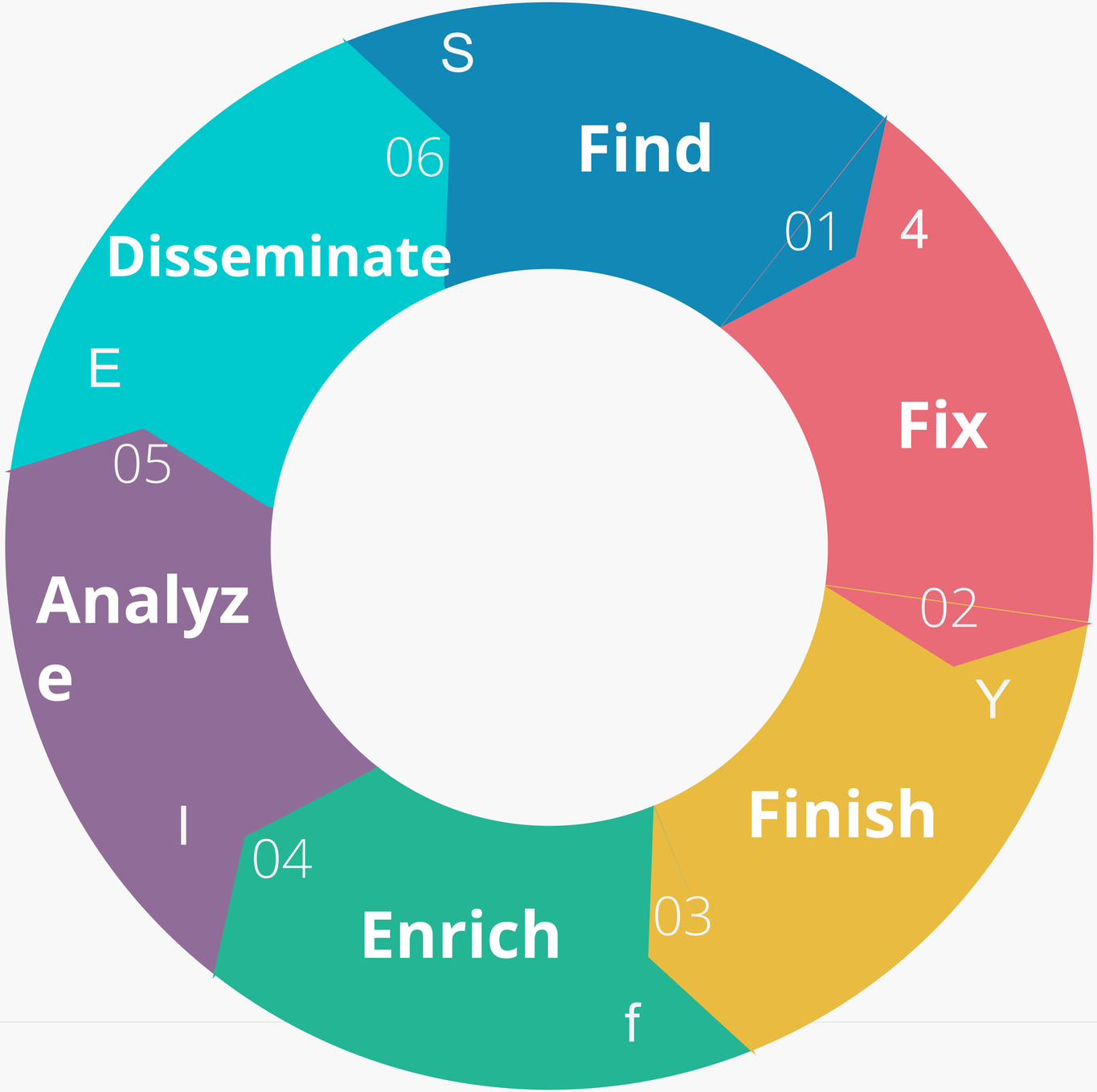
Proactive — Detection Efficiency — Reactive

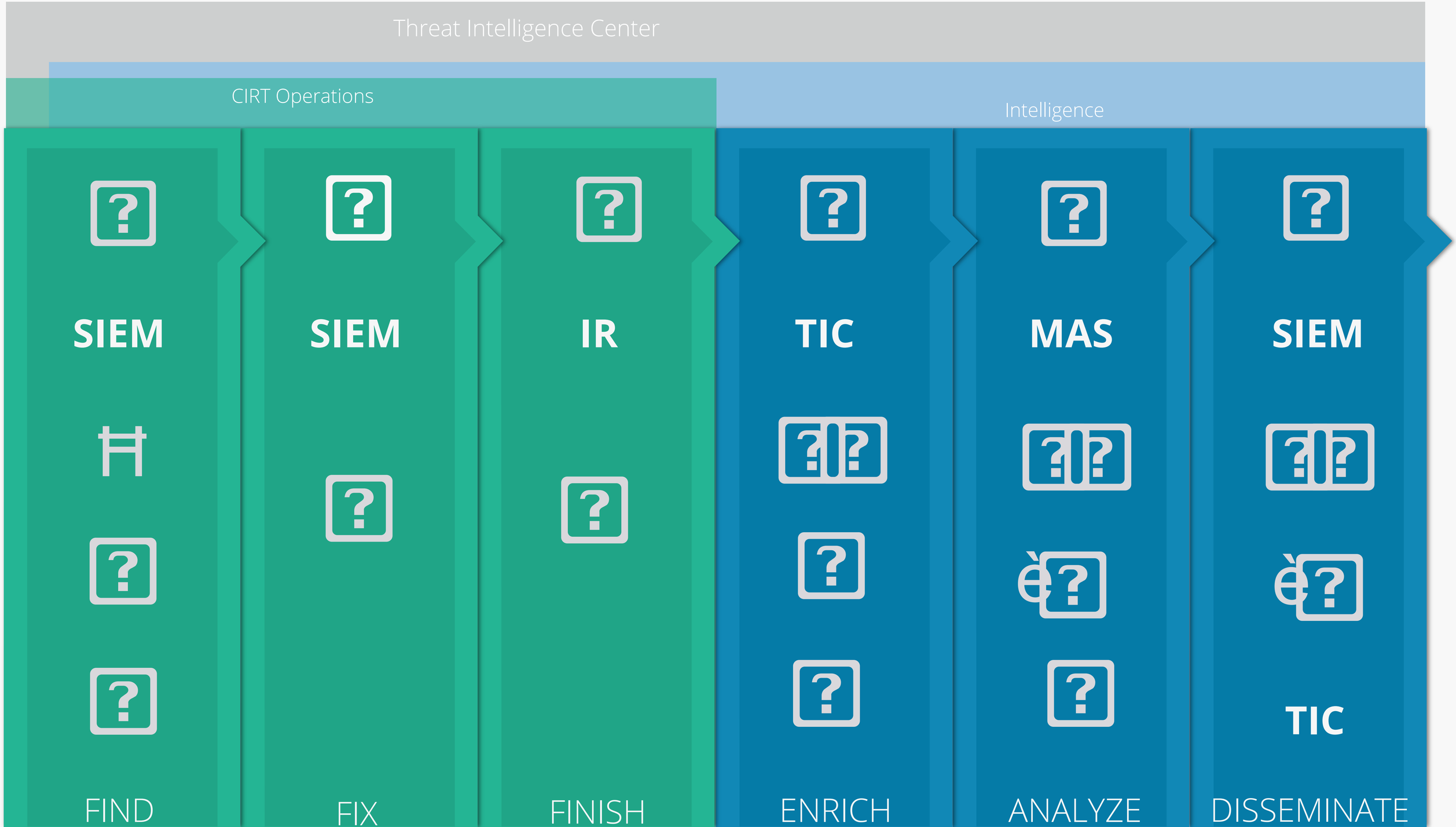
OBJECTIVE COMPLETE

ON THE LAST DAY OF THE ENGAGEMENT

MAKE ATTACKING EXPENSIVE

F3EAD


S
Find
01
4
Fix
02
Y
Finish
03
f
Enrich
04
I
Analyz
e
05
E
Disseminate
06


Threat Intelligence Center
CIRT Operations
Intelligence
SIEM
SIEM
IR
TIC
MAS
SIEM
TIC
FIND
FIX
FINISH
ENRICH
ANALYZE
DISSEMINATE

MALWARE IS THE GREATEST GIFT AN ATTACKER CAN GIVE

The phishing email attempted to hide in plain site by intermixing legitimate Amazon links

Malicious Link #1:
hxxp://www.aquadrift.sk/wp-content/themes/yoo_glass_wp/1.php

Malicious Link #2:
hxxp://cartorioalbuquerque.com.br/images/1.php

Malicious Link #3:
hxxp://capdienphuthai.com/wp-content/themes/RaoThue/1.php

Malicious Link #4:
hxxp://hydroac.info/wp-content/themes/twentyfourteen/1.php

Malicious Link #5:
hxxp://urduacademyjeddah.com/wp-content/themes/inovado/1.php

Samples hosted in countries all over the world including Russia, Thailand, Brazil, Solvak Republic, and United States

hxxp://www.aquadrift.sk/wp-content/themes/yoo_glass_wp/1.php
hxxp://cartorioalbuquerque.com.br/images/1.php
hxxp://capdienphuthai.com/wp-content/themes/RaoThue/1.php
hxxp://hydroac.info/wp-content/themes/twentyfourteen/1.php
hxxp://urduacademyjeddah.com/wpcontent/themes/inovado/1.php

INDICATOR OF COMPROMISE

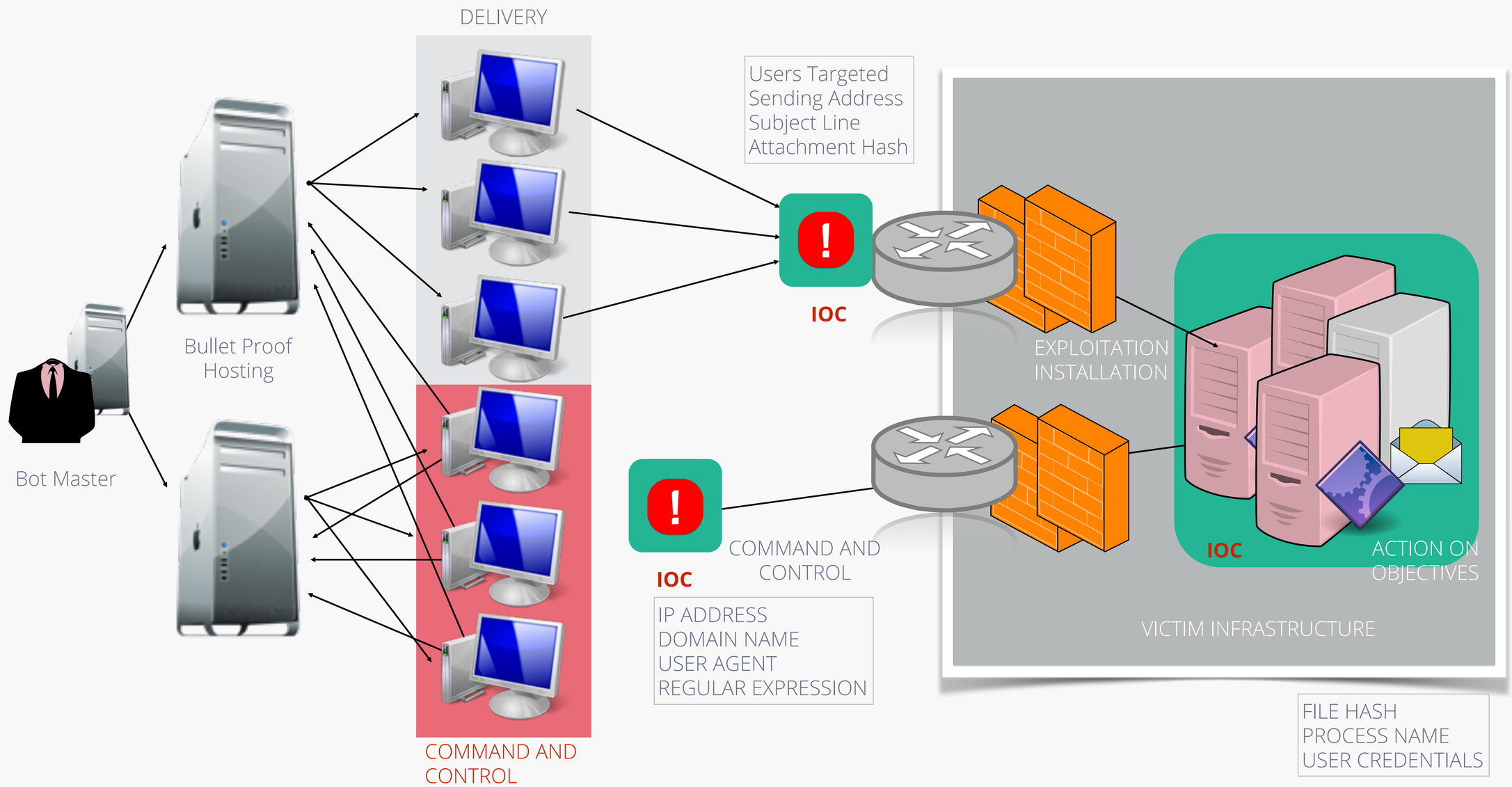
hxxp://www.aquadrift.sk/wp-content/themes/yoo_glass_wp/1.php
hxxp://cartorioalbuquerque.com.br/images/1.php
hxxp://capdienphuthai.com/wp-content/themes/RaoThue/1.php
hxxp://hydroac.info/wp-content/themes/twentyfourteen/1.php
hxxp://urduacademyjeddah.com/wpcontent/themes/inovado/1.php

INDICATOR OF COMPROMISE

hxxp://www.aquadrift.sk/wp-content/themes/yoo_glass_wp/1.php
hxxp://cartorioalbuquerque.com.br/images/1.php
hxxp://capdienphuthai.com/wp-content/themes/RaoThue/1.php
hxxp://hydroac.info/wp-content/themes/twentyfourteen/1.php
hxxp://urduacademyjeddah.com/wpcontent/themes/inovado/1.php

THREAT INTELLIGENCE

WHAT IS THREAT INTELLIGENCE



THREAT INTELLIGENCE

Workspace Tools

Local Sandbox

- Cuckoo Sandbox: www.cuckoosandbox.org
- Remnux: remnux.org
- Malheur: mlsec.org/malheur

Cloud Sandbox

- Malwr: malwr.com
- Payload Security: hybrid-analysis.com
- Mastiff-Online: mastiff-online.korelogic.com
- ThreatExpert: threatexpert.com
- Anubis: anubis.iseclab.org
- VirusTotal: virustotal.com

Office and PDF Scanners –Local

- OfficeMalScanner: reconstructer.org
- OffVis: aldeid.com/wiki/OffVis
- PDFxRay_Lite: github.com/9b/pdfxray_lite

Office and PDF Scanners – Cloud

- XecScan: scan.xecure-lab.com
- Malware Tracker: malwaretracker.com

Sandbox Behavioral Tools

- Regshot: sourceforge.net/projects/regshot
- MAP: github.com/dzzie/MAP
- Sysinternals: live.sysinternals.com

Virtual Machine

- Virtualbox: virtualbox.org/wiki/Downloads
- Vmware: vmware.com/products/player

Reverse Engineering

- IDA Pro: hex-rays.com/products/ida/
- OllyDbg: ollydbg.de/download.htm

Threat Intelligence

- CRITS: crits.github.io
- SOLTRA: soltra.com

CenturyLink™

Attackers only have to be wrong once