ANU LECTURE

FIFTH DOMAIN

OVERVIEW

1. Introduction to Cyber
2. Threat Actors
3. Offensive Tradecraft
4. Cyber Crime Ecosystem
5. Defensive Strategies

CYBERSPACE

WHAT IS CYBER?

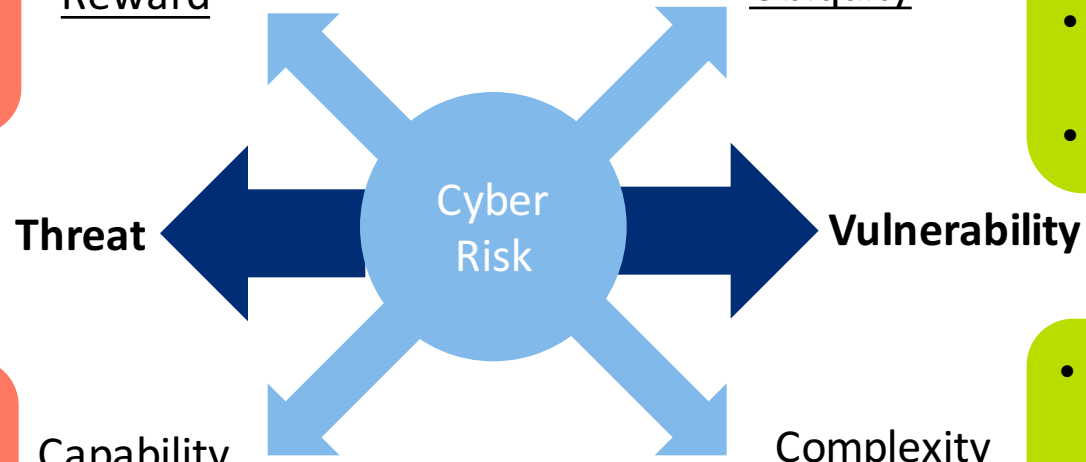
- Tagging the internet and the digital world with the term ‘cyber’ is a recent event.
  - *Both the term cyber and the internet existed prior to adoption*
  - *What changed?*

- What is the difference between cyber security and IT security?
  - *Is the difference technical?*

WHAT IS DRIVING CYBER SECURITY?

- Financial fraud
- Intellectual Property
- Identity theft
- Extortion & Ransom

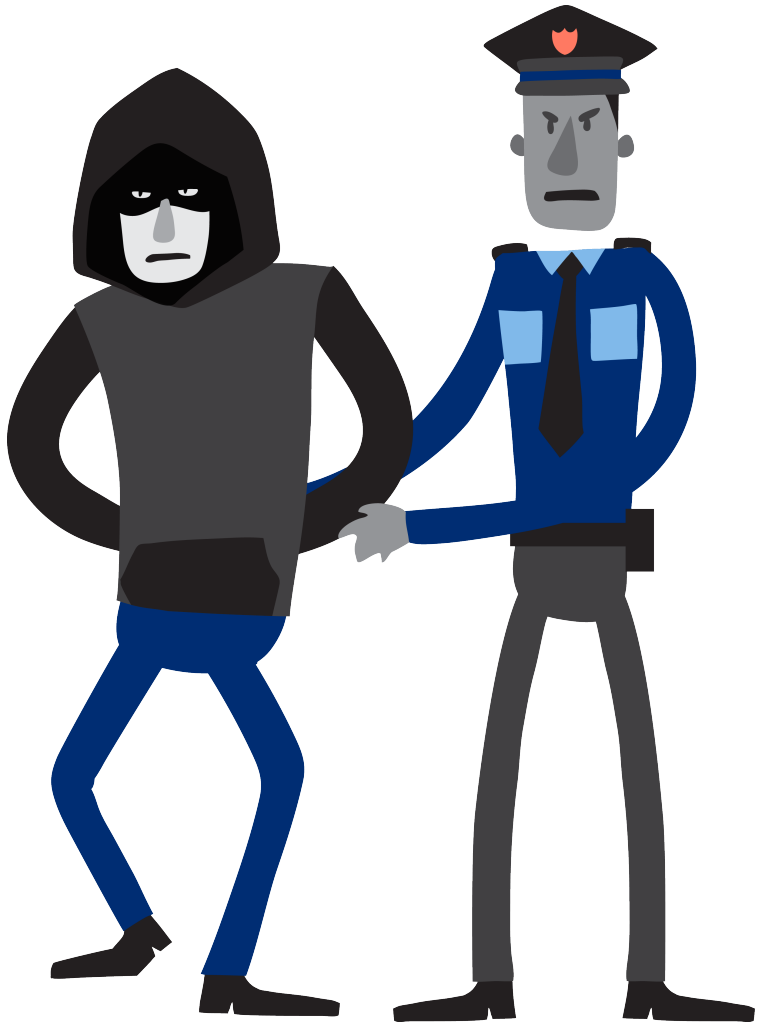
- Hacking as a service
- Online Black-markets
- Digital currencies
- Training & education



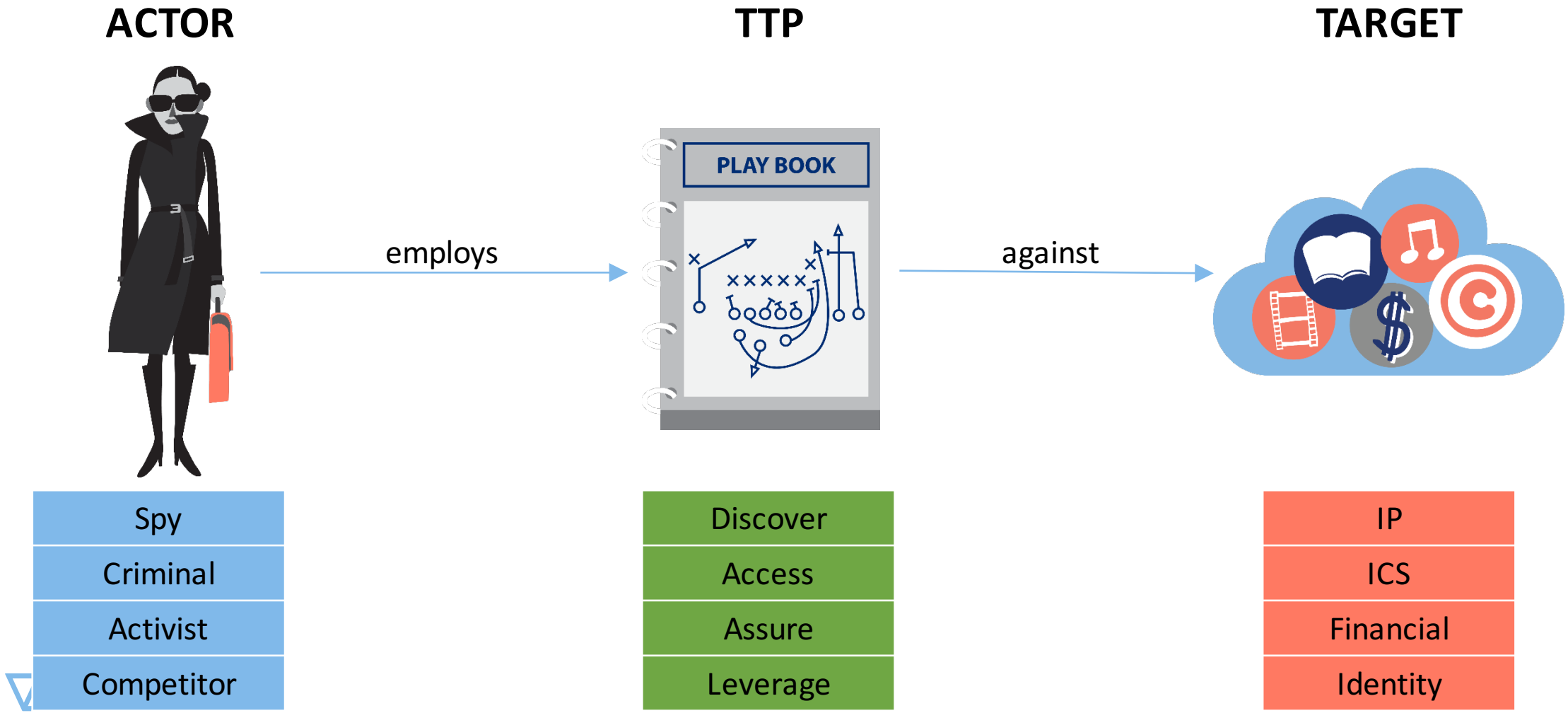
- Device proliferation (IoT)
- Integration with daily life
- Societal Dependence

- Software – more code per application
- Networks – BYOD, mobile

THREAT ACTORS



OBSERVE – DIRECTION – THREAT MODELING

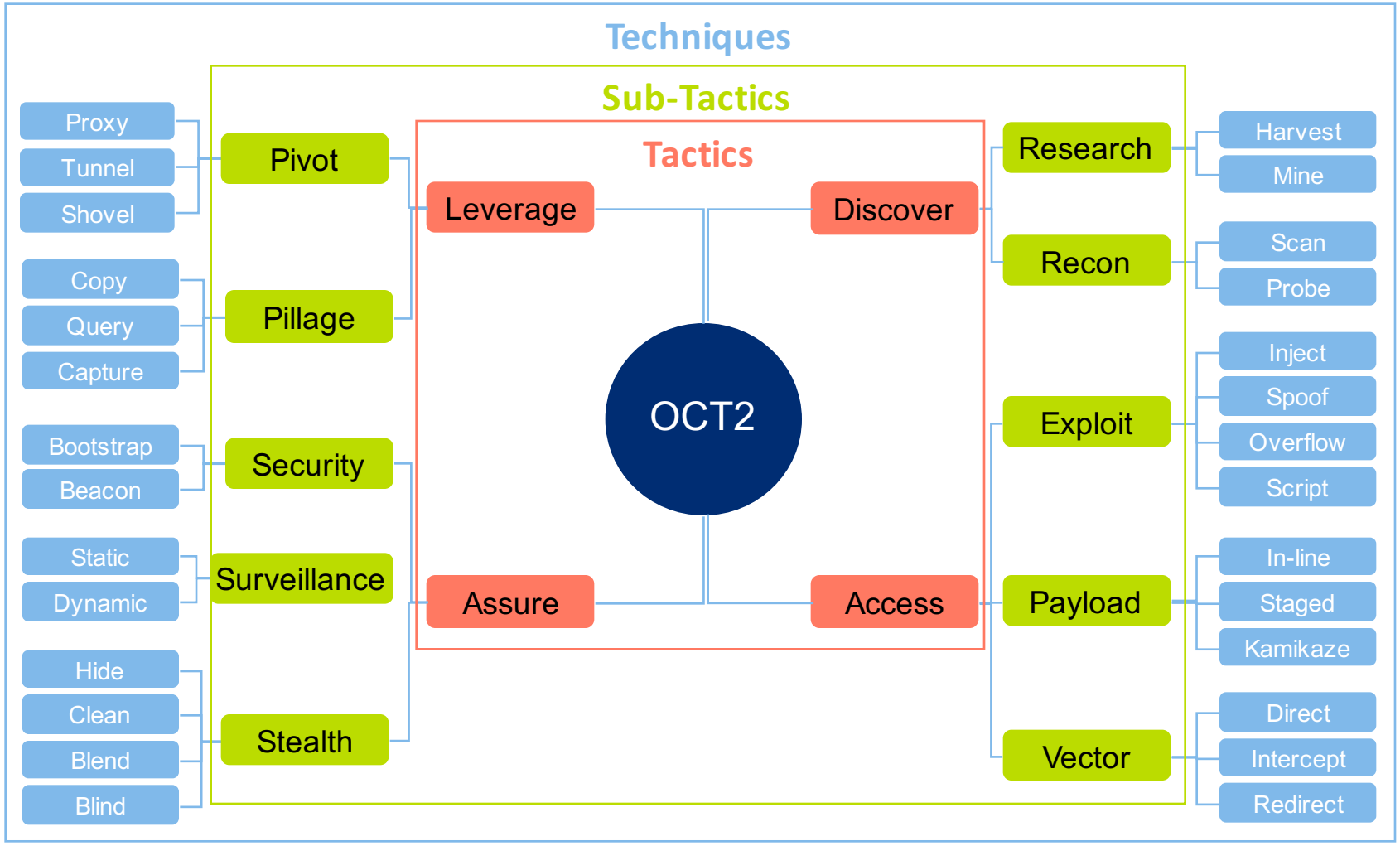


THREAT ACTORS

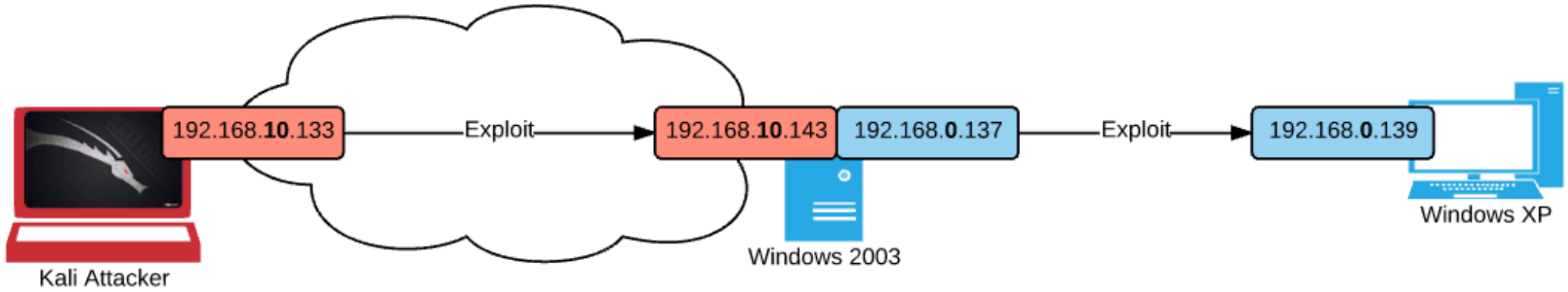



Actor	Spies	Criminals	Activists	Competitors
Goals	• Political & Economic intelligence. • Sabotage	• Financial • Fraud • Ransom • Extortion	• Embarrass • Discredit • Attract attention to cause	• Competitive advantage
Targets	• Classified information • Critical infrastructure	• Computer systems • Valuable data • Credentials	• Private information • Website / Social media	• Intellectual property • Marking / Budget data
Vectors & TTPs	• Close Access • Remote Access • Supply chain	• Denial of Service • Spray and pray email • Watering hole	• Denial of Service • Defacement	• Insiders • Remote access • Spear Phishing

The Offensive Cyber Tradecraft Taxonomy (OCT2) describes the spectrum of tactics and techniques.



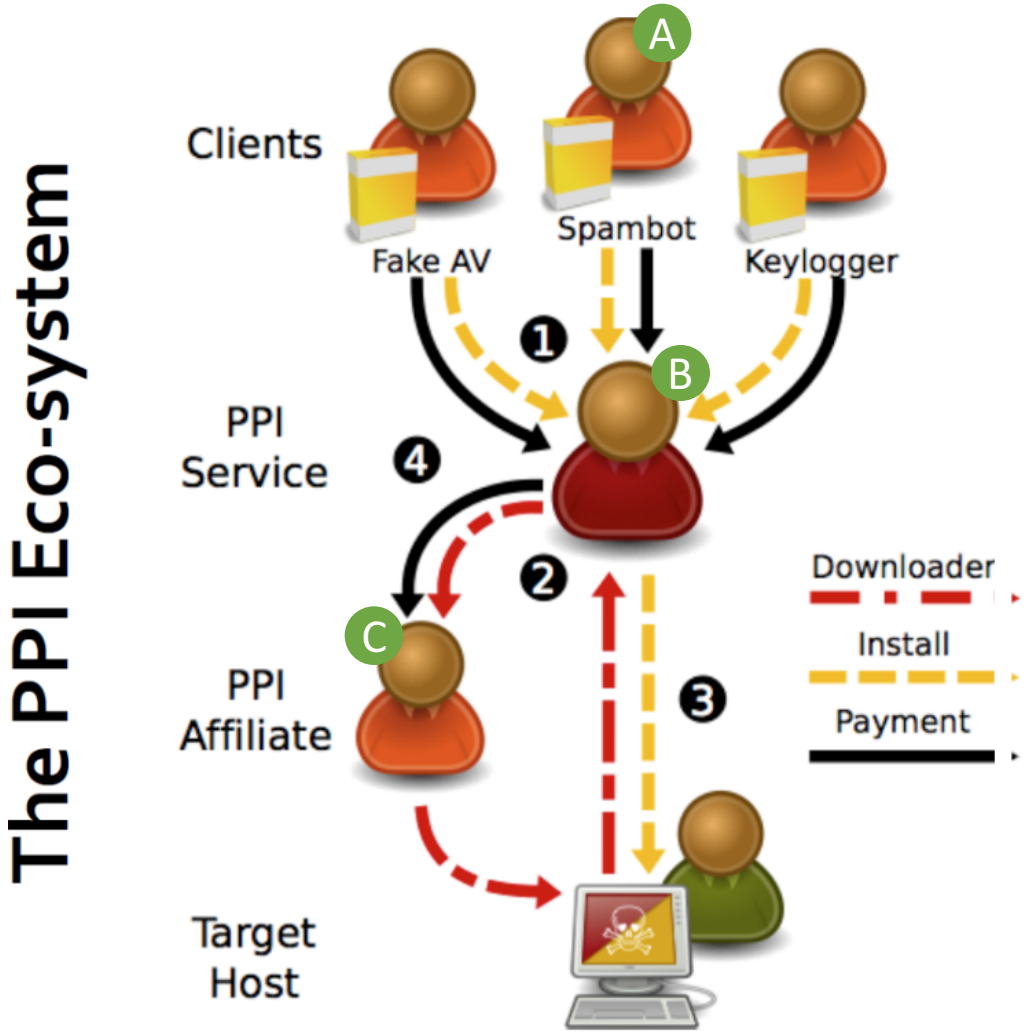
CYBER ADVERSARY TRADECRAFT – AUTOMATION



CRIMINALS

ECOSYSTEM - SIMPLE

- A Clients who want malware installed – developers, buyers
- B Brokers who only interface between other service providers
- C Affiliates who own and control websites that will infect or redirect to infection server

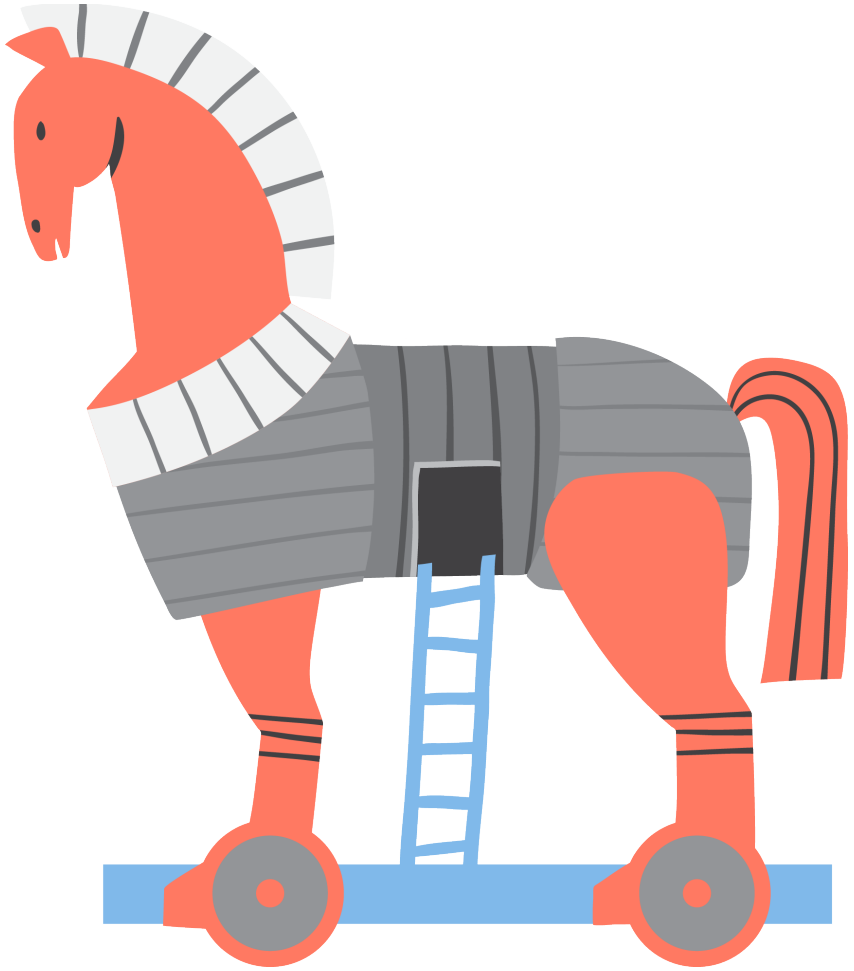


CRIMINAL SUPPLIERS

Service	Description	$$$$ 2013
Consulting services such as botnet setup		$300-$400
Infection / spreading services	Watering Holes/	~$100 per 1k installs
Botnets & Rentals	Horde of controlled computers.	DDoS $550 for 5 hours x 7 days
Email spam	Redirect victims exploit servers.	$40 / 20k emails
Web spam	Web sites that serve only to manipulate Google search results – keyword stuffing, link schemes	$2 /30 posts
QA - Crypters and scanners	Anti-virus and IDS testing and assurance.	$10 per month
Affiliate programs	On selling malware and other black market services.	$5k per day
Hosting (VPNs & Proxies)	Domain respawning. g00gle. C2, collect	$3 per month
Blackhat SEO	Reputable sites linking to bad ones	$80 / 20k backlinks
Money exchange and mule services	Real currency must be transferred to currency accounts	25% commission
CAPTCHA Breaking	Human enabled	$1 / 1k CAPTCHAs
Password Cracking	GPU and ASIC farms / Botnets	$17 / 300M attempts

TOOLS

1. Bugs
2. Exploits
3. Implants



BUGS

- Bugs are errors and weaknesses in code and protocols.
  - *CWE lists common code errors*
- Accepted rule of thumb 10-20 errors per 1000 lines of code.
  - *Windows 10: 50M lines of code = 500k – 1M bugs*
- Bugs may crash the application - be benign, or present opportunity to inject commands.
  - *Not all bugs can be weaponized*
- Fuzzing is the automated testing for bugs
  - *Providing invalid data to applications to cause a failure*

EXPLOIT KITS

- Exploit kits are the software product in the cybercrime value chain.
- Developers produce once and sell to many (unless exclusivity rights)
- Consists of all the code to gain and maintain access to a target system.
- Like legitimate software can come as:
  - *Product: purchased or leased with support and updates*
  - *Service: just need to supply the targets*

- The variety of exploit kits is as wide as tools are in a shed.
  - *All built differently to do a specific job.*

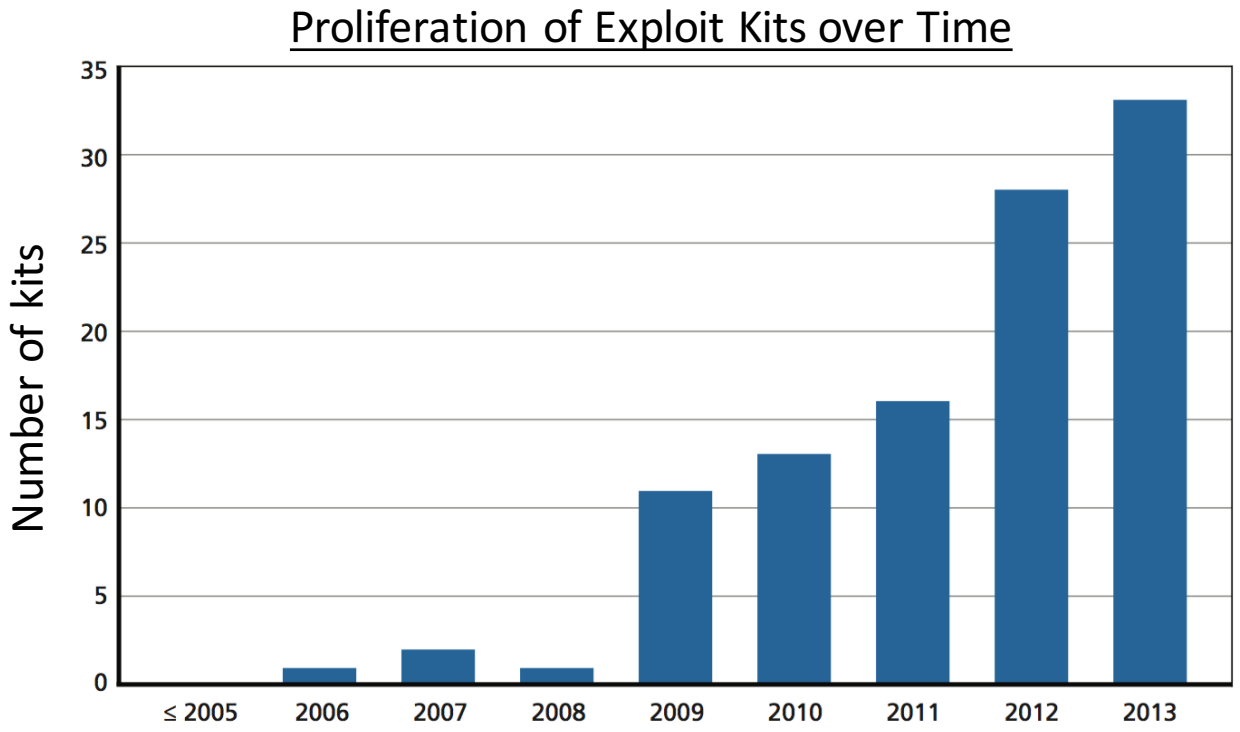
EXPLOIT KIT PROLIFERATION

More developers

- *Learning from reverse engineering*

Larger market

- *More money online, more vulnerabilities, more hackers*



Source: RAND (2014)

EXPLOIT KIT COMPONENTS

- Targets the software vulnerability.
- The '0-day' component.
- Forces the system to run injected commands.

- Mini-program to confirm target susceptibility.
- Downloads and installs 2nd stage payload.
- Protects exposure of the payload.

- The implant or malware.
- Usually retrieved from remote server.
- Configures persistence an ensures interactivity with the target.

INFECTION SERVICES

- Now that I have my tool kit I need to infect victims
- There are a number of ways that I can infect systems
- Two methods of exploitation:
    1. *Redirect victims to a malicious website*
    2. *Deliver exploit or embed exploit in document*
- Redirection can be achieved via:
    1. *Spear phish email with a link*
    2. *Webspam / Affiliation*
    3. *Malvertising*
-

SPEAR PHISHING

- We understand what an email is but where do I get email addresses?
  - *Active reconnaissance*
  - *Spam email lists*

- Scratching the surface
  - *URL masking & misspelling (m1cros0ft.com)*
  - *URL shorteners (bit.ly)*
  - *URL subdomains (paypal.badness.com)*

SPAM SITES - SEO

- Serve no other purpose other than to redirect visitors to exploit delivering websites.
- Attract visitors via blackhat Search Engine Optimization (SEO)
  - *Google ranking algorithm; constantly changing*
  - *Content: Unique & changing, specific HTML tags, navigation*
  - *Relationship: visits, links to website in other pages*

- Blackhat SEO aims to subvert the Google ranking systems
  - *Ranking not always dependent on human readable content*
  - *Hacking websites to insert invisible links – similar key words*

BLACKHAT SEO

Blackhat SEO aims to subvert the Google ranking systems

- *Hacking websites to insert invisible links – back-linking*
- *Defeat spam detection = similar key words*

Post CSS code into website visitor 'leave a message' box – Cross-site scripting

```
<div style=\"\\64\\69\\73\\70\\6c\\61\\79:\\6e\\6f\\6e\\65\">

<a
href=\"http://www.fcit.usf.edu/li/viagra.html\">viagra</a>\r\n<a
href=\"http://www.fcit.usf.edu/li/free-viagra.html\">free
viagra</a>\r\n

</div>
```

`display: none`

Example Domain
www.example.com/
This site may be hacked.
Example Domain. This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information...

SPAMSITE

1. Register a domain and hosting service willredirecttoexploit.com
2. Add superficial content to mask nefariousness
3. Create multiple webpages
4. Insert redirection links to exploit delivering website

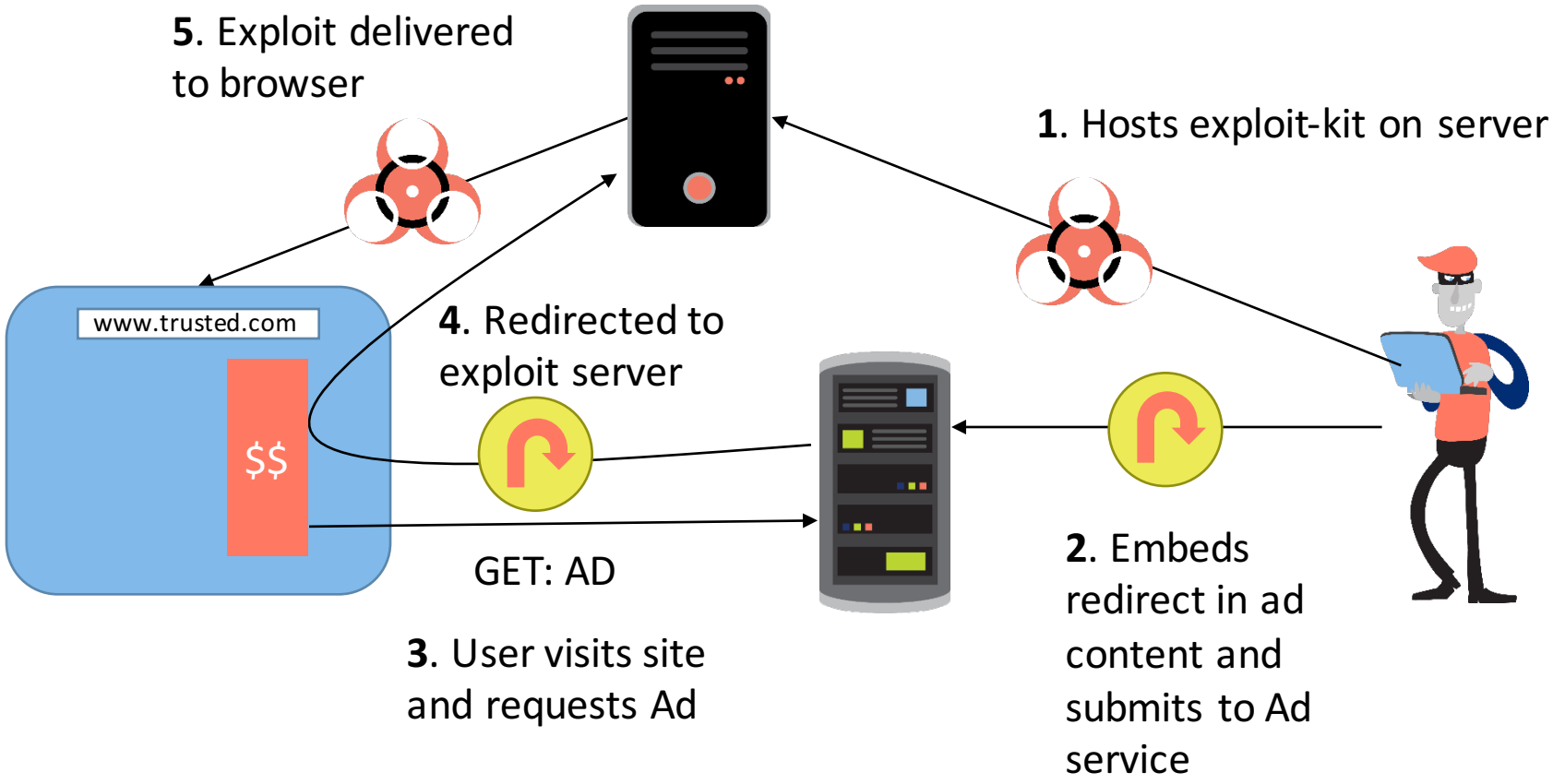
- `<meta http-equiv="refresh" content="0; URL=http://www.g00gle.com">`
- The website delivering the exploit tracks the referring website through user-agent string or through customer subdomain link.
- `Referer: http://www.willredirecttoexploit.com`
- Redirector receives payment based on number of redirect logs.

MALVERTISING

- Malicious Advertising is the latest trend in serving malware
- Not everything on the webpage is produced by the website owner
  - *In-page ads are 'webpages within webpages'*
  - *You visit a trusted site but that site has invited malicious advertisers*

- Criminals are posing as legitimate advertisers or taking over control of established advertising accounts
  - *Criminals registering businesses, setting up websites to appear legitimate to Advertising services*
  - *Criminals able to update Ad content as needed*

MALVERTISING IN ACTION



BOTNETS

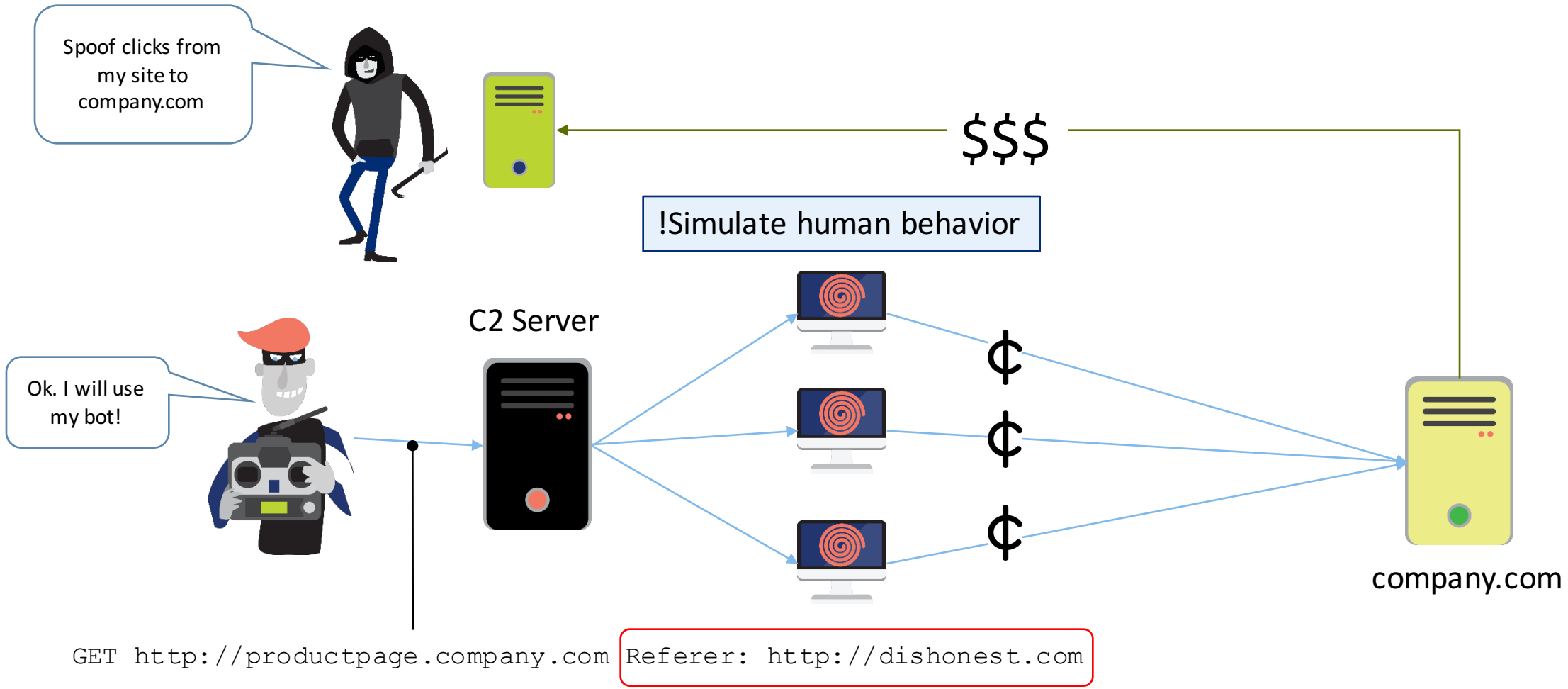
A botnet is a group of computers under the control of one master.

- *Exploit kit is sold and controlled by buyer but a botnet remains under the control of the bot-herder*

Botnets are rented to preform tasks:

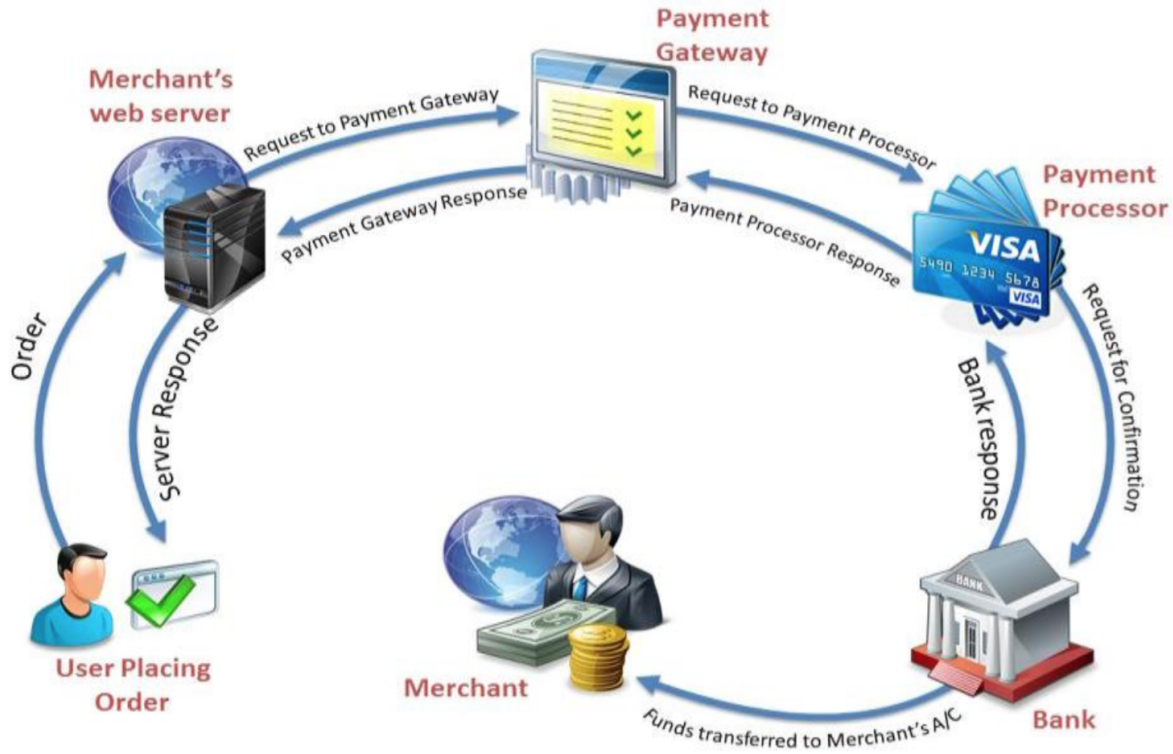
- *Send spam emails*
- *Install other malware*
- *DDoS*
- *Credential harvesting*
- *Pay per click fraud (SMS – mobile)*

BOTNETS – CLICK FRAUD



VOXIS PLATFORM – LAUNDERING AS A SERVICE

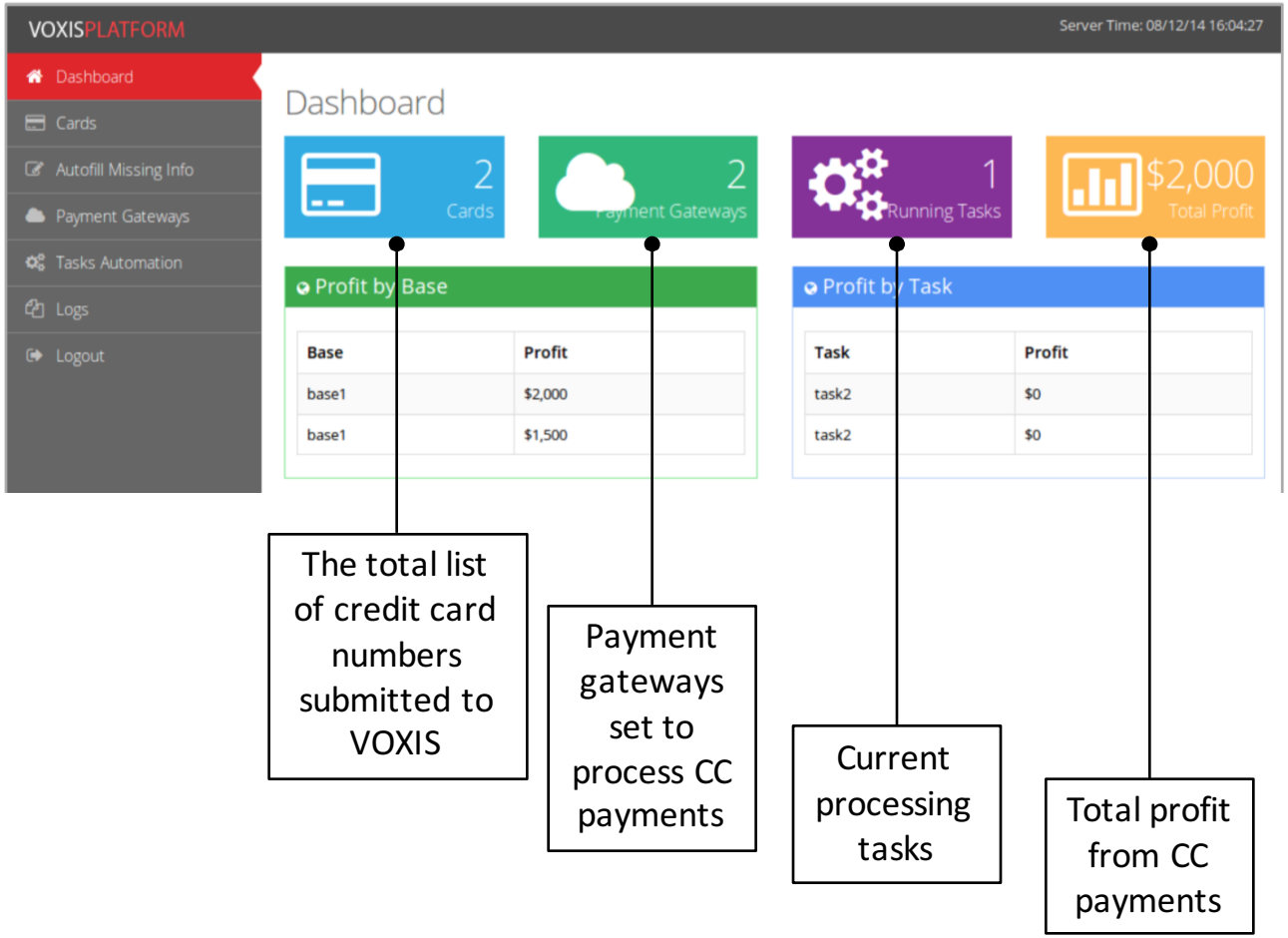
- Automated money laundering
  - *First reported by IntelCrawler in 2014*
- Masquerades as online store to interface with legitimate payment gateways – PayPal,
  - *Digital evidence proving online store legitimacy is forged*
- Voxis provides this 'shell-merchant-as-a-service' for 32 payment gateways



Source: RSA - 2015

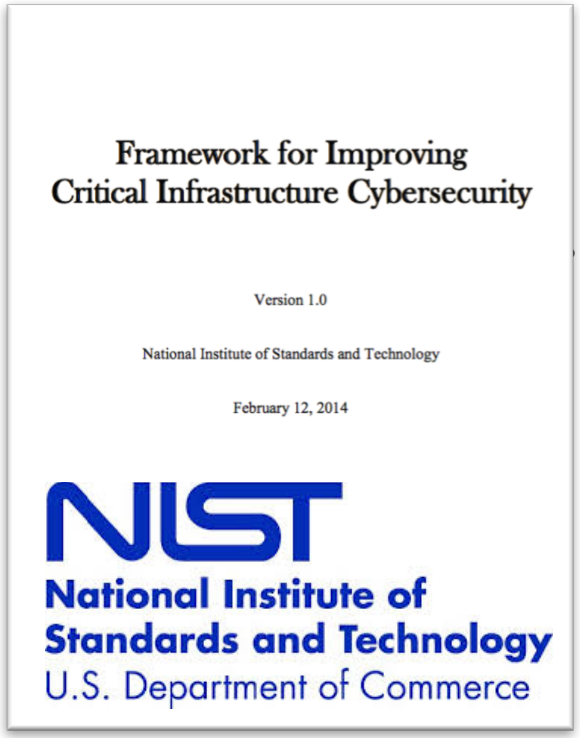
VOXIS USER EXPERIENCE

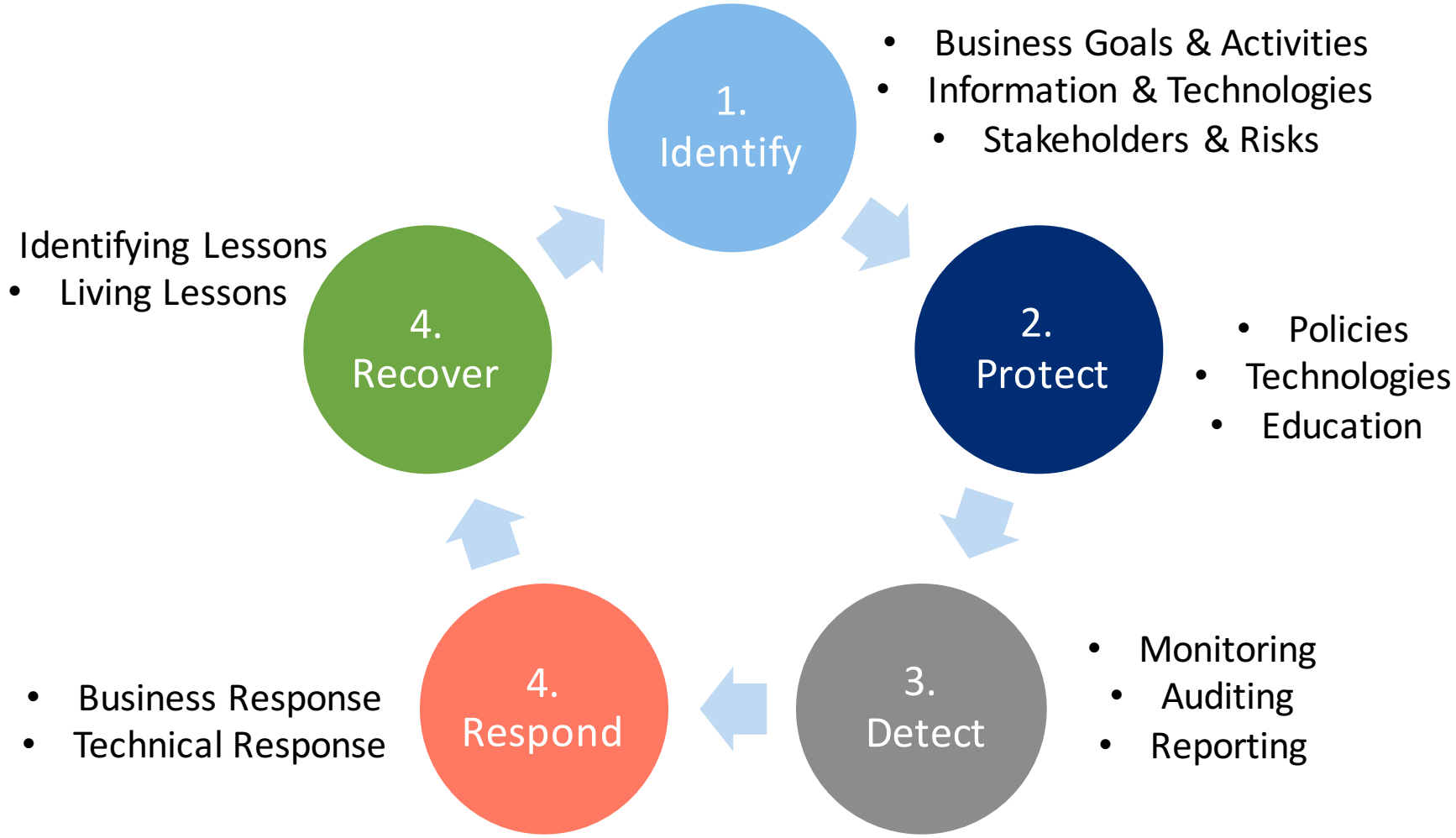
- Mimics real behavior
- Thieves can define:
  - *Any of 32 payment portals*
  - *Schedule recurring payments*
- Voxis searches pipl.com for card owner information to submit
- Voxis source-code 'borrowed' from open-source payment project



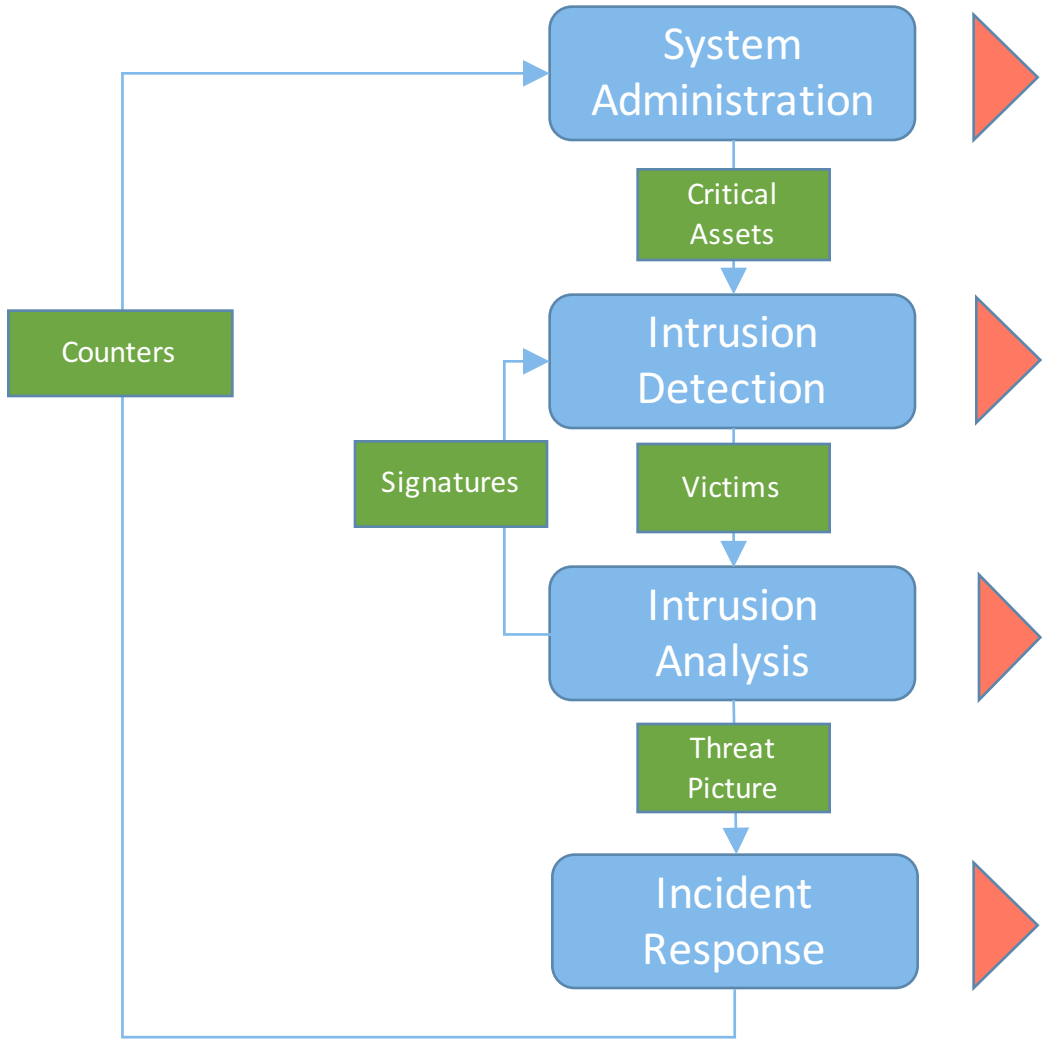
DEFENDERS

WHAT IS THE NIST FRAMEWORK?





WHAT IS SECURITY OPERATIONS?



Protecting systems through conventional security.

2. Protect

Network and host based sensor and signature management.

3. Detect

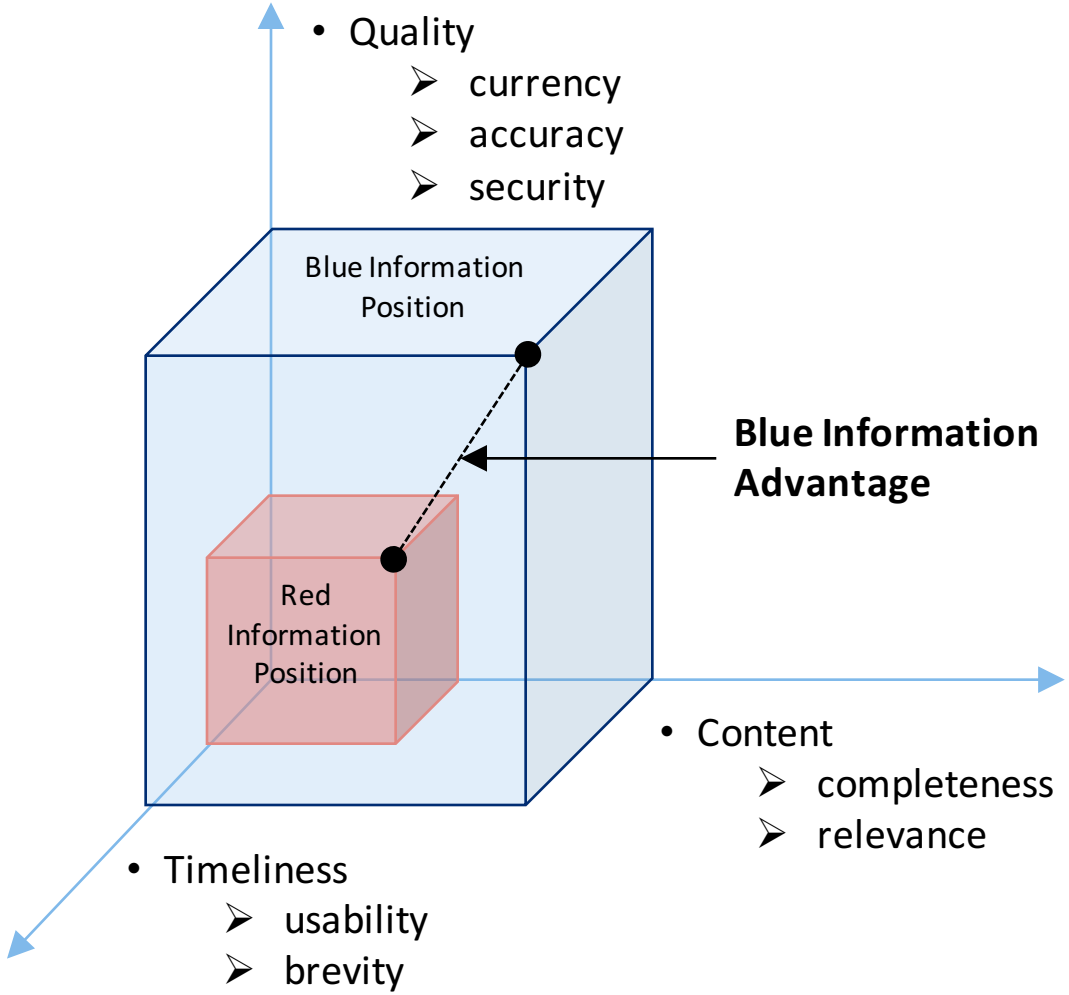
Network and host investigation.

Threat containment, eradication & recovery.

4. Respond

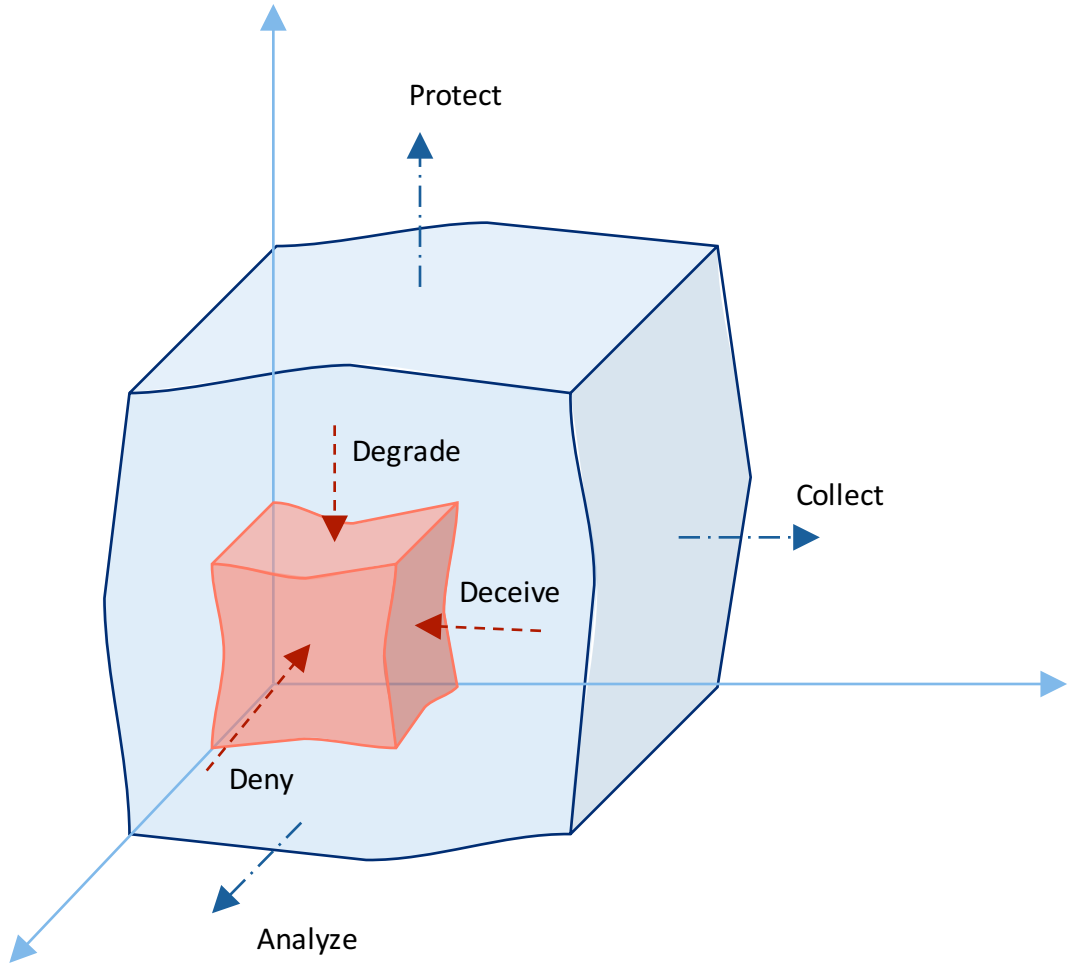
INFORMATION SUPERIORITY…

- Quantity is not quality!
- Information superiority is relative to:
  - *Own objectives*
  - *Adversary objectives*
- Information requirements may be asymmetrical
  - *Objectives and capabilities determine information requirements*

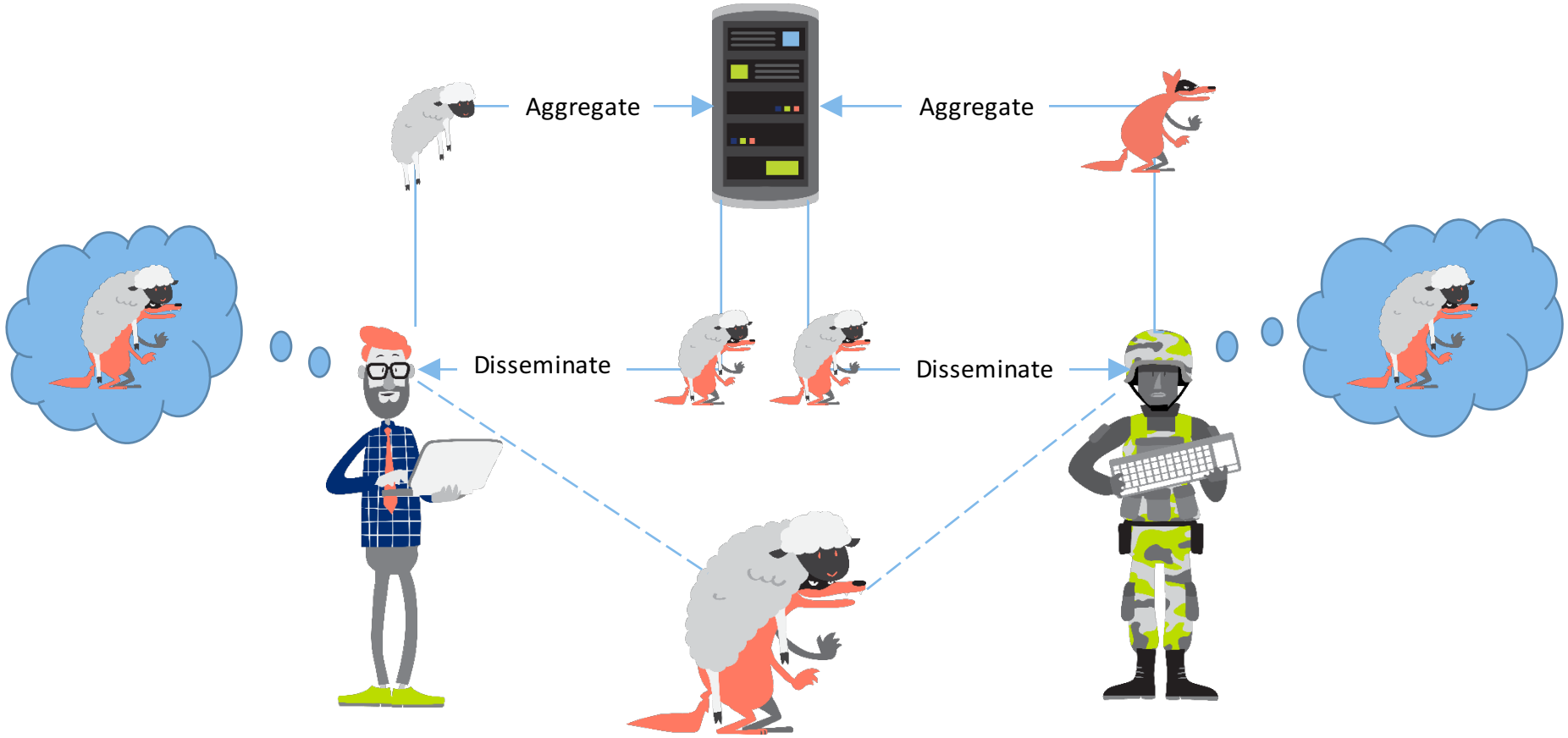


…IS A RELATIVE POSITION

- The objective is to improve the delta between own and the adversary information position.
  - *Attempts to improve own information position may leak information to the adversary and become counter productive.*



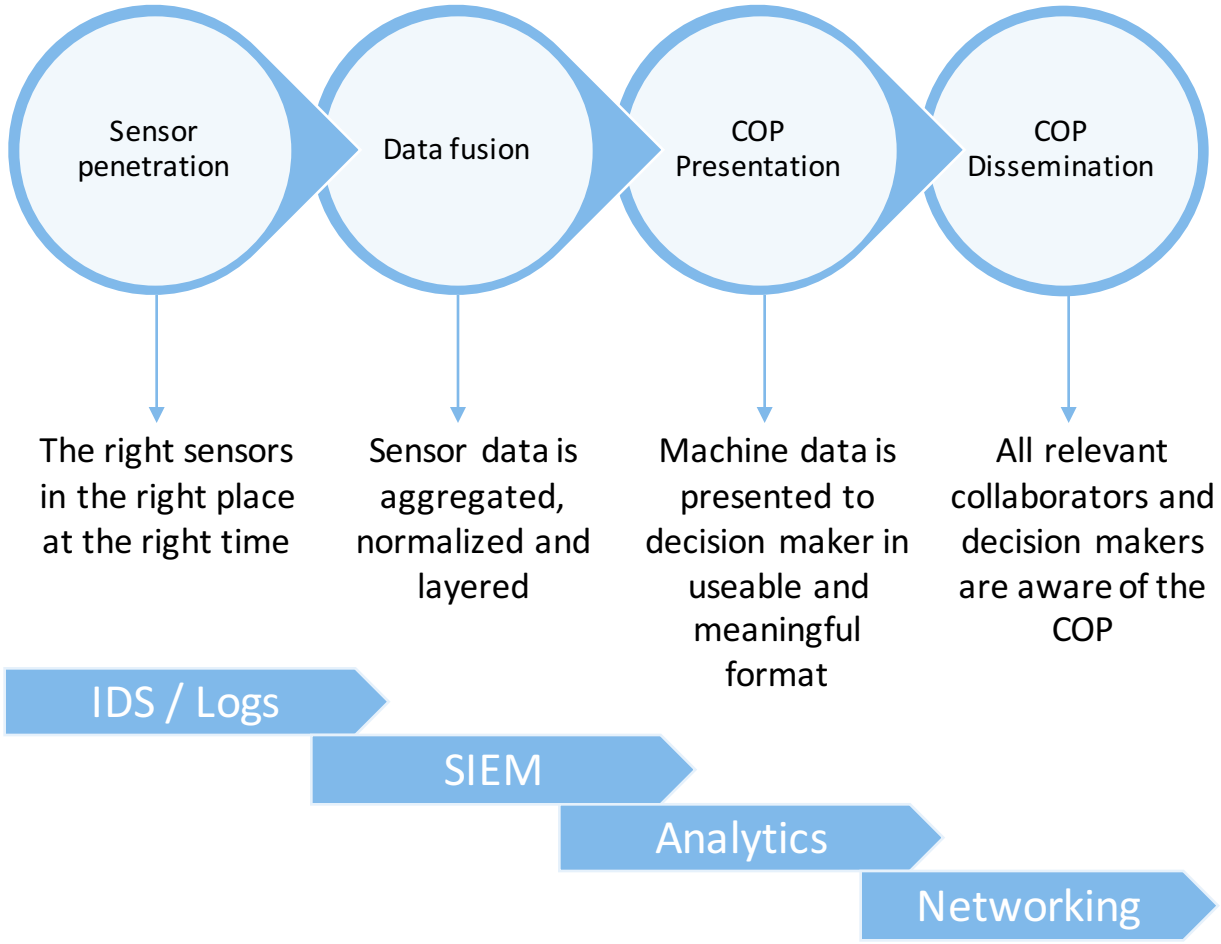
SHARED SITUATIONAL AWARENESS



NCW VALUE-CHAIN

- It is not enough to just collect network data, it must be made meaningful and presented to the right people.
  - *Lack of data is rarely the reason why intrusions persist. It is rather a lack of meaning from existing data.*

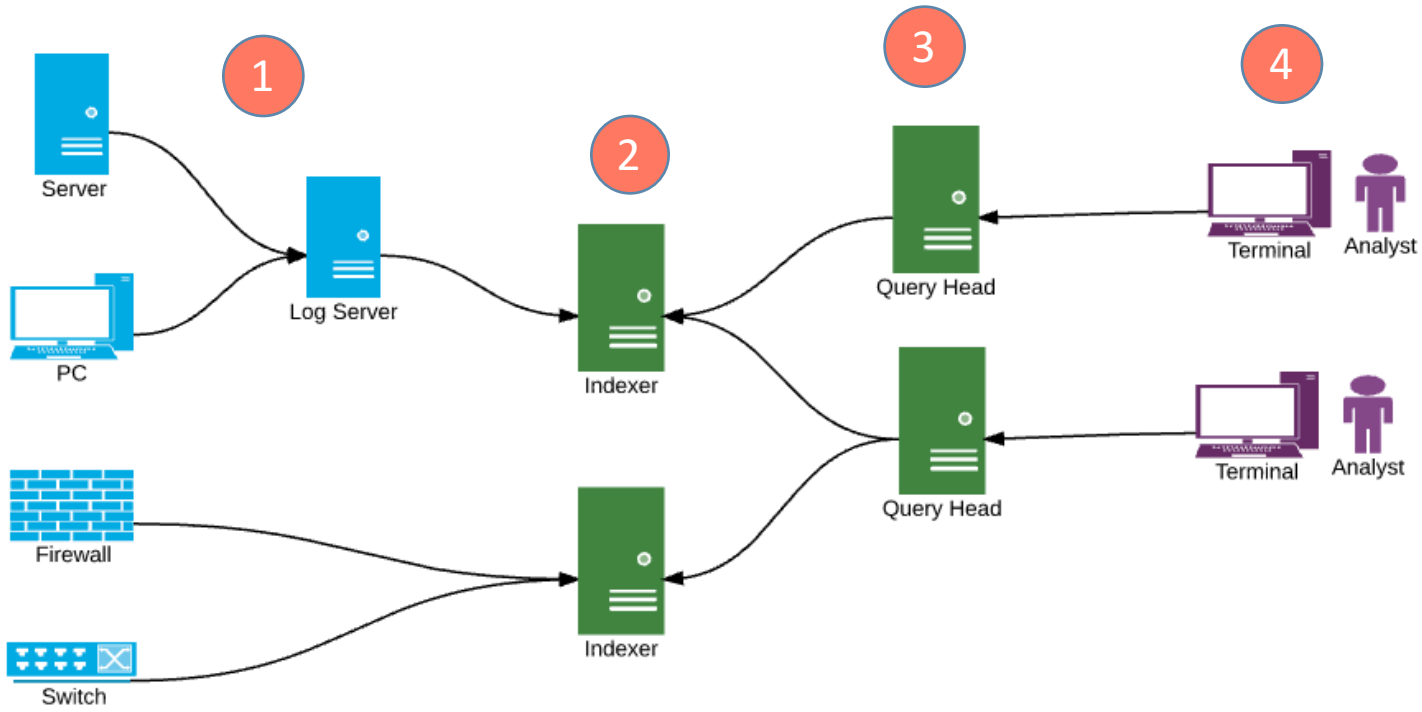
1. Deploy and task sensors
2. Ensure data is formatted
3. Generate queries & rules
4. Communicate results



GENERATING SITUATIONAL AWARENESS - CYBER

- SIEM
  - *Security Information & Event Management*

1. Machines generating logs and data
2. Forward data to Indexer for processing normalization.
3. Query Head queries Indexers for required data.
4. Analyst views dashboards and runs queries.



SO WHAT DOES IT MEAN FOR ENGINEERS?

- You don’t have to be perfect.
  - *Flawless technology is not possible*
- You just have to be better than the person trying to break what you build.

100% of of all cyber crime, espionage and sabotage is caused by …

people.