Detecting Threats via Network Anomalies

Gregory Pickett

- Hellfire Security
- Cybersecurity Operations

@shogun7273
gregory.pickett@hellfiresecurity.com

Not Like The Others...

Utilizing Anomalies

- What Are They?
- Why Are They Important

What Are They?

a·nom·a·ly

/əˈnäməlē/

noun

1. something that deviates from what is standard, normal, or expected.
   "there are a number of anomalies in the present system"
   synonyms: oddity, peculiarity, abnormality, irregularity, inconsistency, incongruity, aberration, quirk, rarity
   "the growth on the duck's bill is a harmless anomaly"

2. ASTRONOMY
   the angular distance of a planet or satellite from its last perihelion or perigee.

Why Are They Important?

Your business operates on processes, regular predictable processes. Your staff operates the same way … habits, regular, repeating, predictable, and knowable. It is the threats that are different, foreign, and ultimately stick out as abnormalities from your established baseline.

Your Network

- Understanding It
  - Analytical Reference
  - Baselining It
- Established Flowspace

Analytical Reference

- Critical Assets
  - Systems
  - Infrastructure
- Processes
  - Users
  - Software
  - Cycles Involved

Collecting Data

- Asset Tracking
  - Hardware
  - Software
- Shadow IT
  - Discovery and Scanning
  - Rogue System Detectors

Adding Dimensions

- Geographic Area
  - Where
- Payloads
  - Volume
  - Type

Established Flow Space

- Operational Processes and Cycles
  - Who
  - When
- Applications and Tools
  - What
  - How

Example

- File Server (Central United States)
- Flows
  - **Who** (R+D United States, R+D France)
  - **When** (12:00-23:00 UTC, 06:00-17:00 UTC)
  - **What** (Microsoft Office, Documentum Client)
  - **How** (TCP 445)
  - **Where** (10.10.160.0/24, 10.10.200.0/24)
  - **Payload** (SMB)

Baselining It

- Tools
  - Network Behavioral Analysis
  - Machine Learning
- Improving

Improving

- Quality
  - Limit Scope (Critical Assets)
  - Limit Flowspace
  - Longer Sampling
- Effectiveness
  - More Granularity
- Feedback Loops
  - Against Analytical Reference
  - False Positives

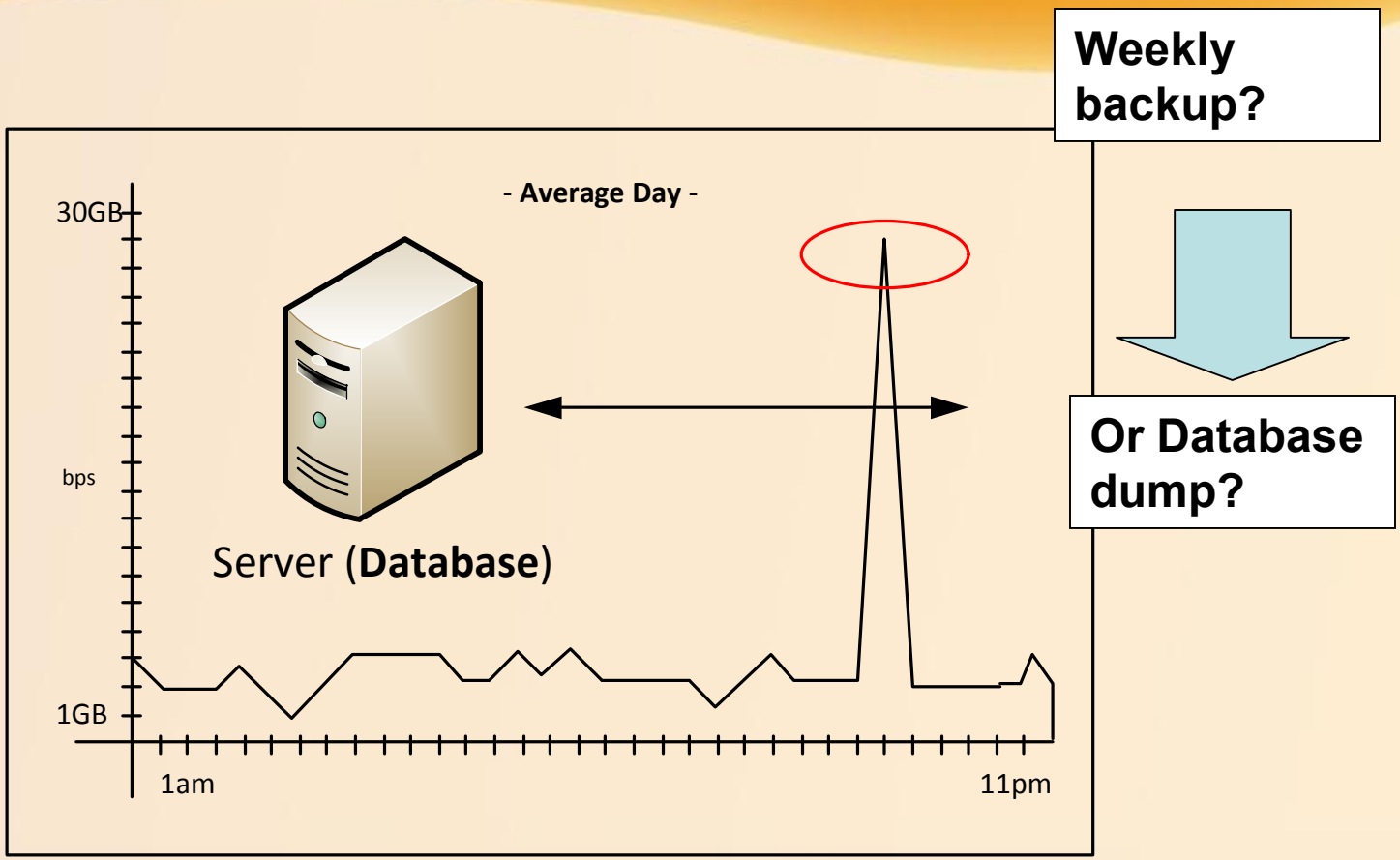
Detecting Threats

- Anomalies to Look Into
- Likely Threats

Anomalies to Look Into

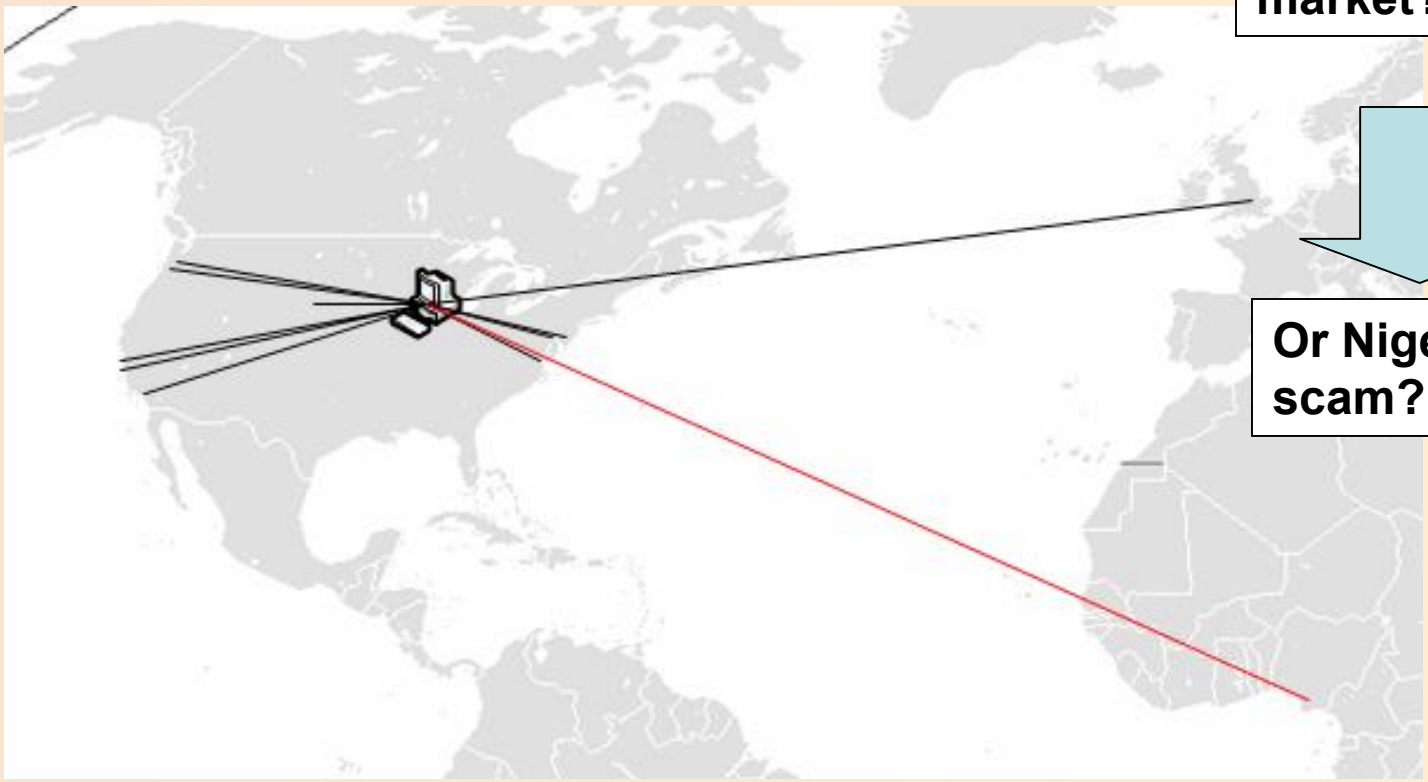
- Volumetric
- Geographic
- Temporal
- Role
- Boundary
- Protocol

Volumetric



* Can be measured in pps, bps, or fps

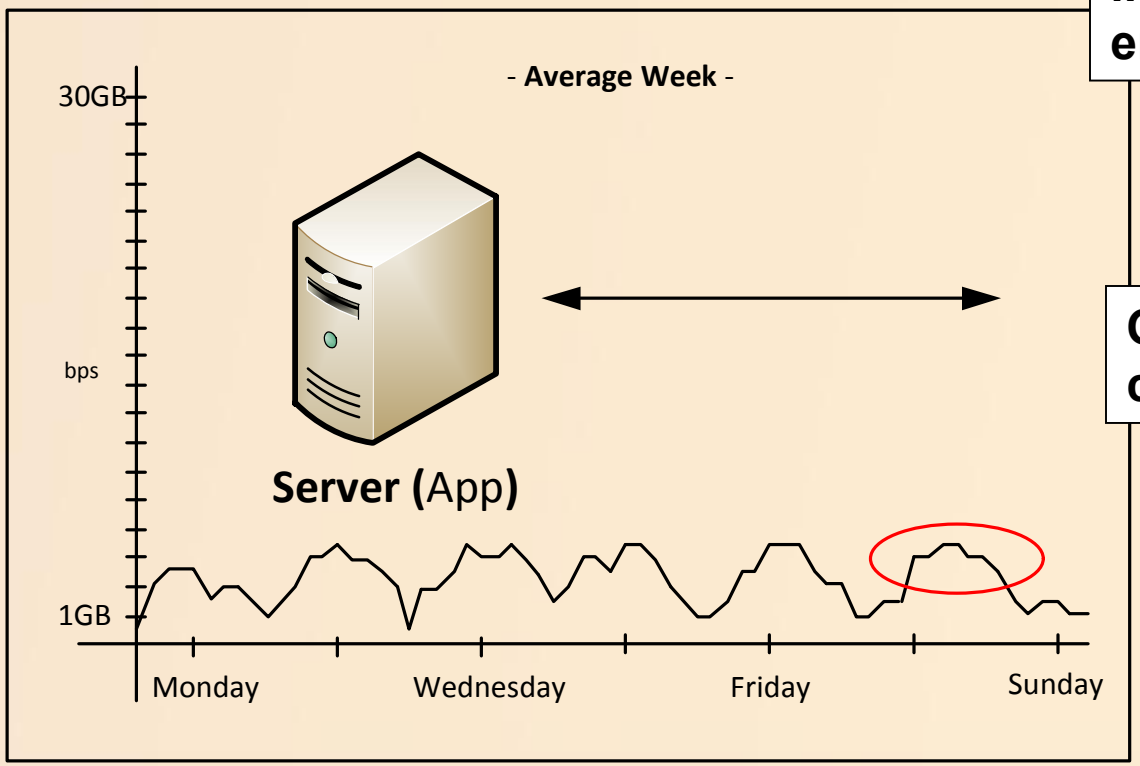
Geographic



Emerging market?

Or Nigerian scam?

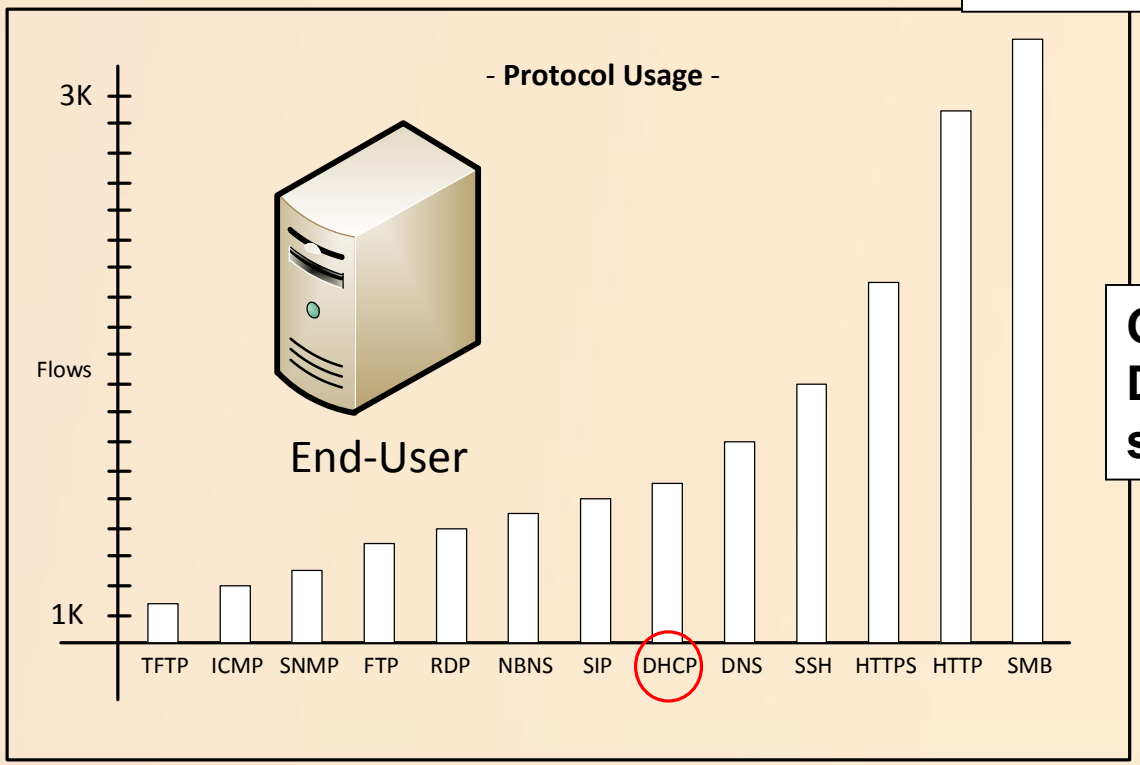
Temporal



Accounting in for month end?

Or data collection?

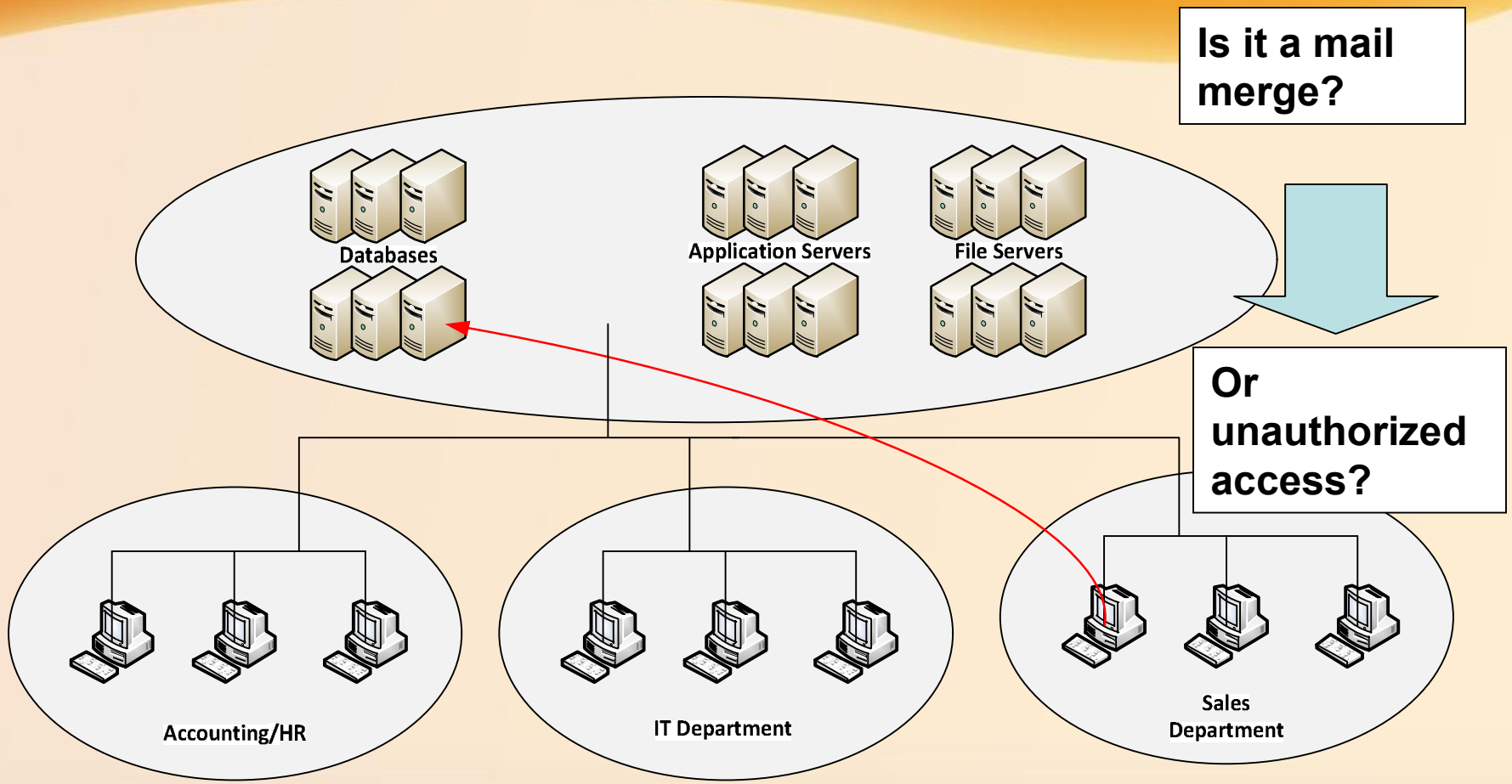
Role



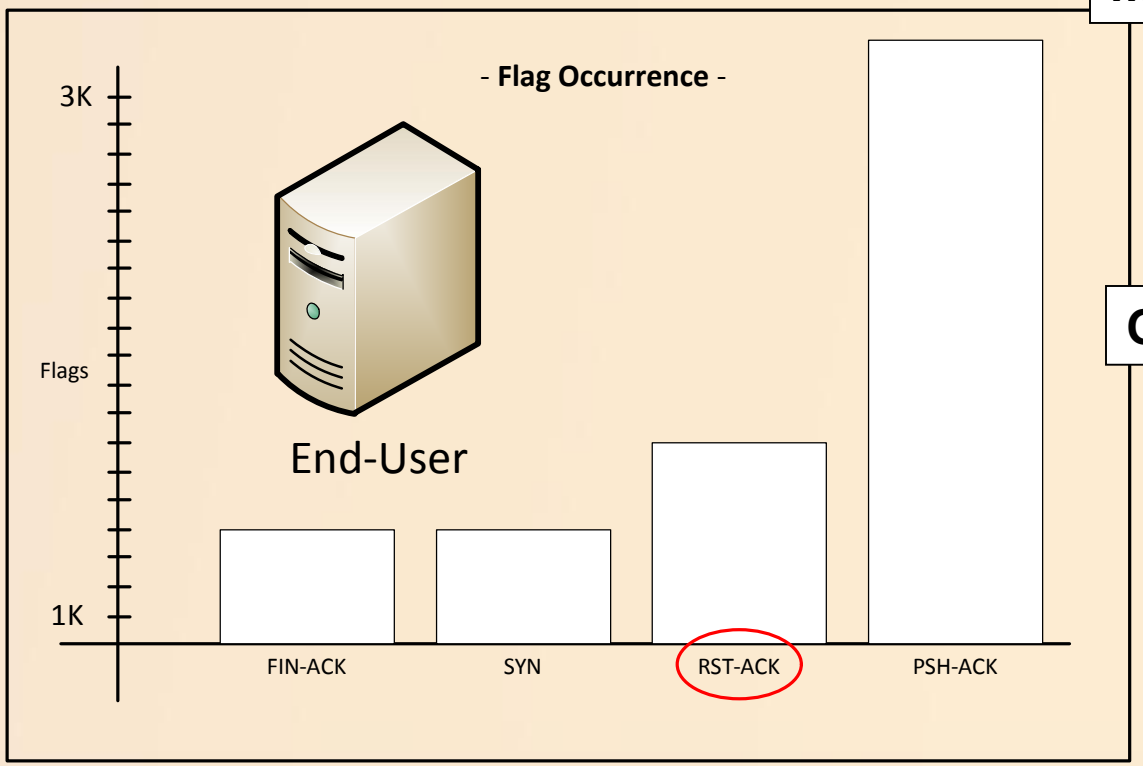
Misconfiguration?

Or rogue DHCP server?

Boundary


Is it a mail merge?
Databases
Application Servers
File Servers
Or unauthorized access?
Accounting/HR
IT Department
Sales Department

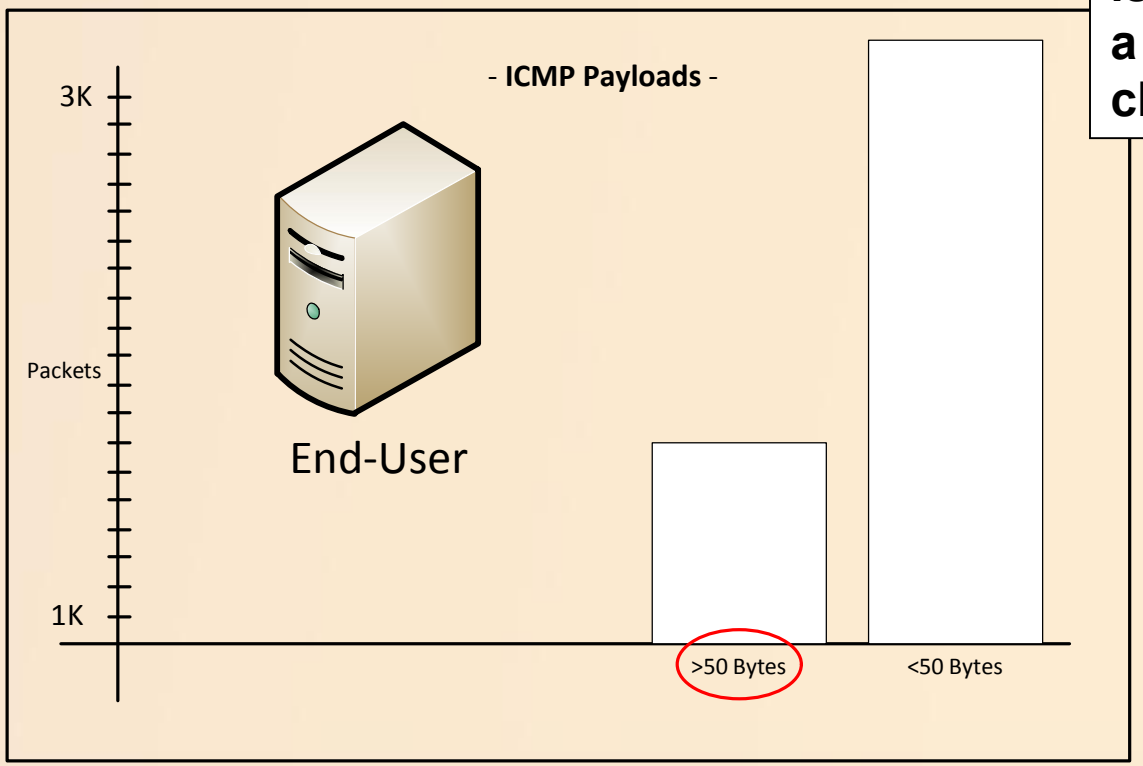
Protocol



Poor change management?

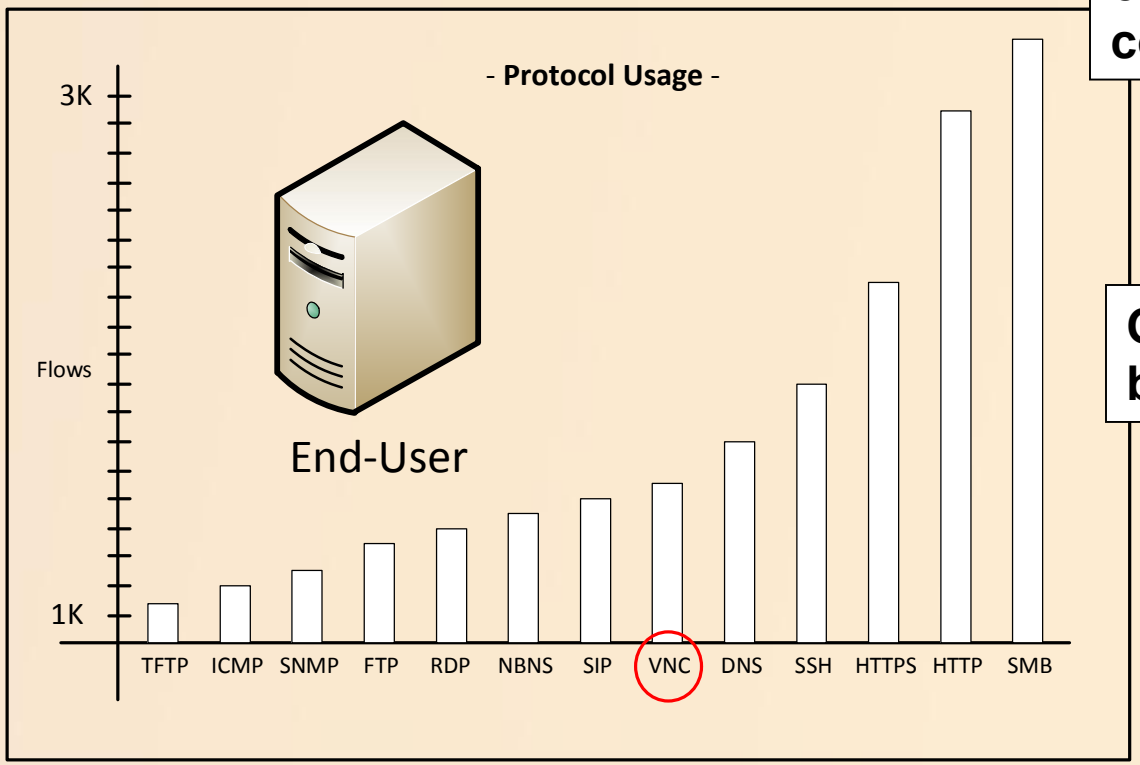
Or a scan?

Protocol (Other)



OK … This is probably a covert channel!

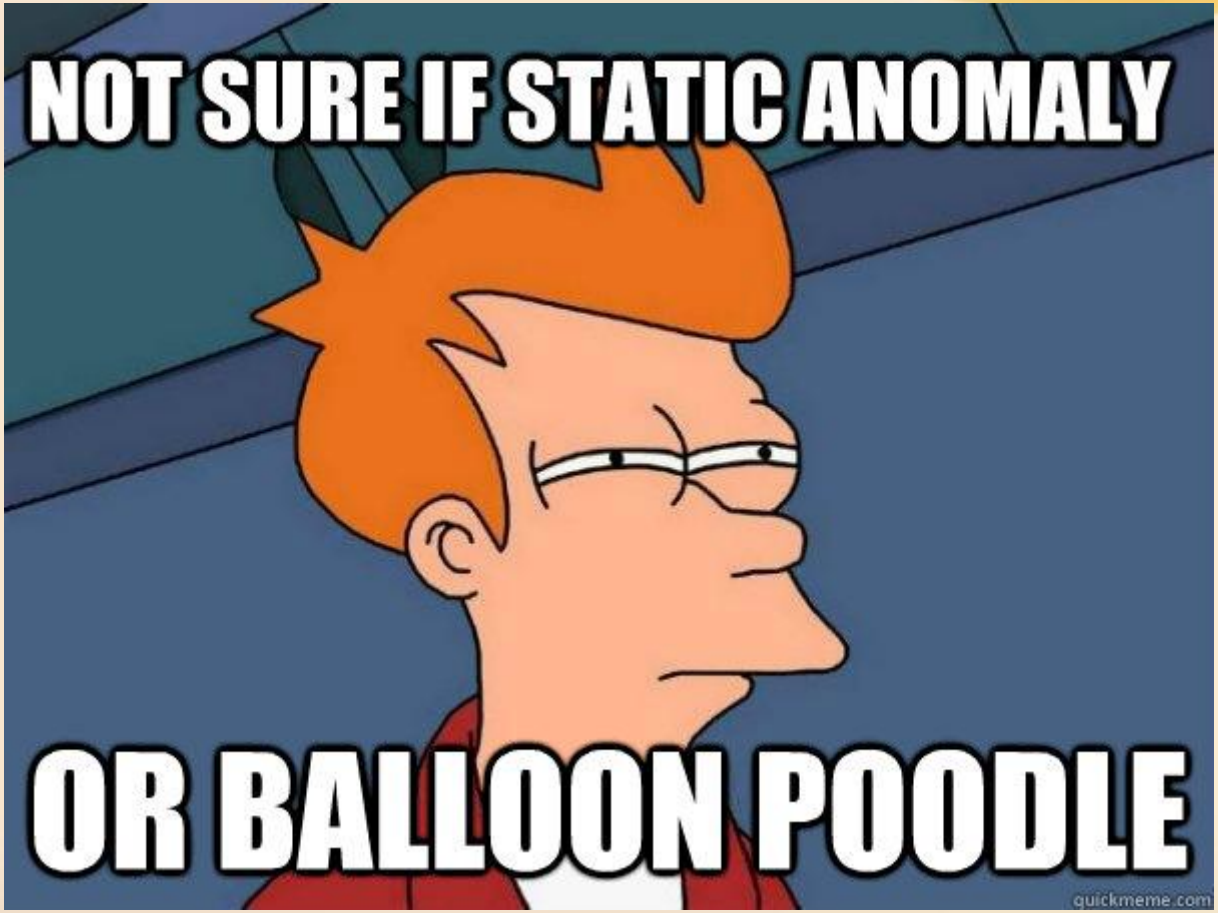
Protocol (Other)



Administrator out of compliance?

Or backdoor?

So The Question Is …



Threat Indicators

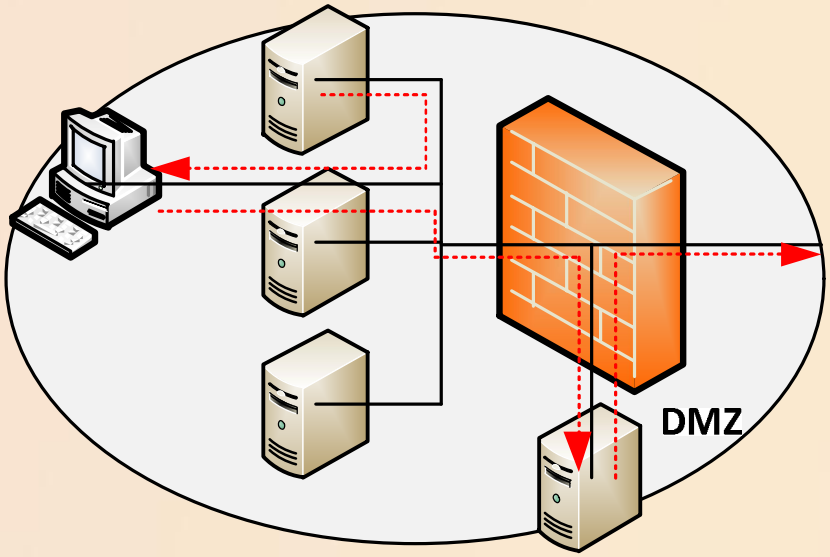
- Correlation
  - Other Activity?
  - Other Abnormalities?
  - Other Alerts?
- Comorbidity (Progression)
- Goal-Oriented Behavior
  - Keep An Inventory
  - Match Against

Likely Threats

- Goal-Oriented Behavior
  - Determinstic
  - Learning
- Discriminating

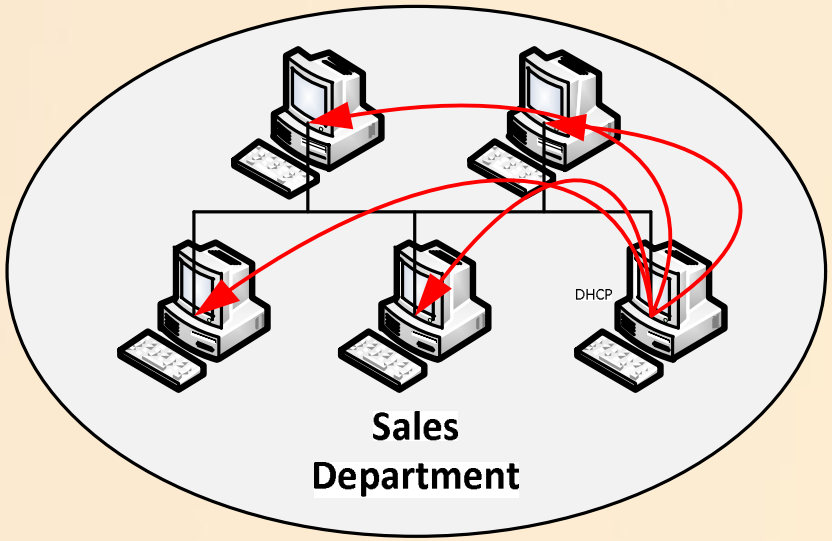
Deterministic

- Incoming to Host
- Outgoing to External



→ Exfiltration

→Rogue DHCP Server

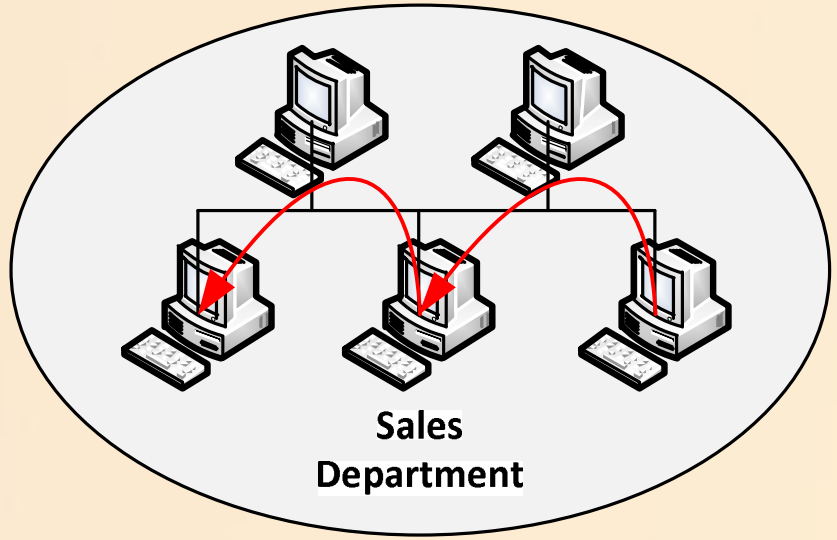


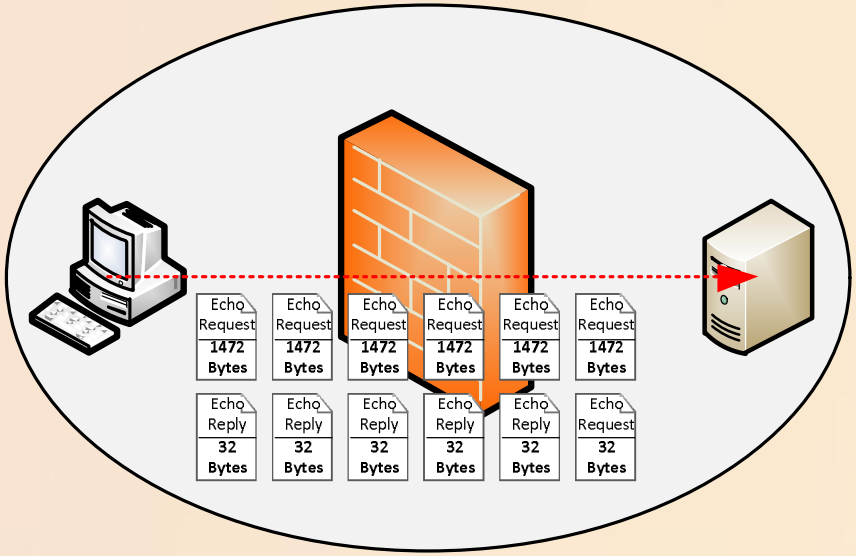
- DHCP (UDP 67)
- Between Peers

Deterministic

- ICMP (Payload > 50)
- Outgoing (Foreign)

→ **Worming**



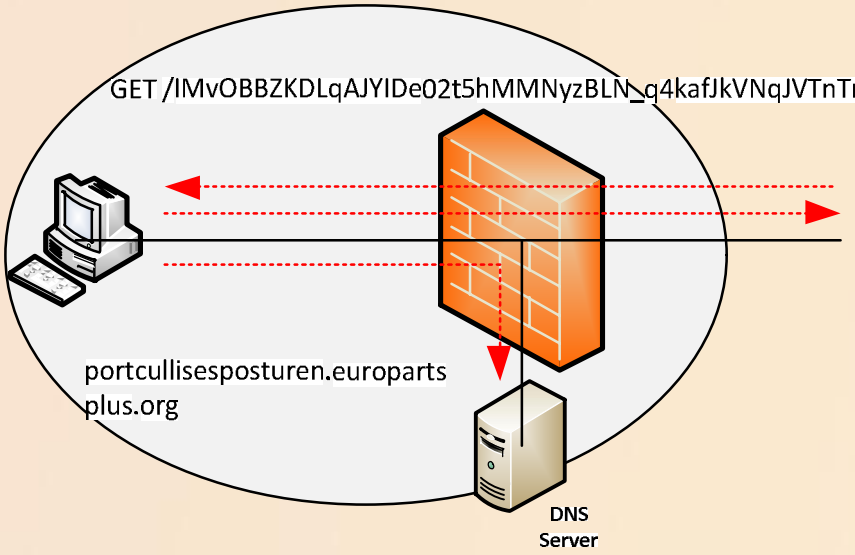


→ **Exfiltration**

- Incoming to Host
- Outgoing to Peer

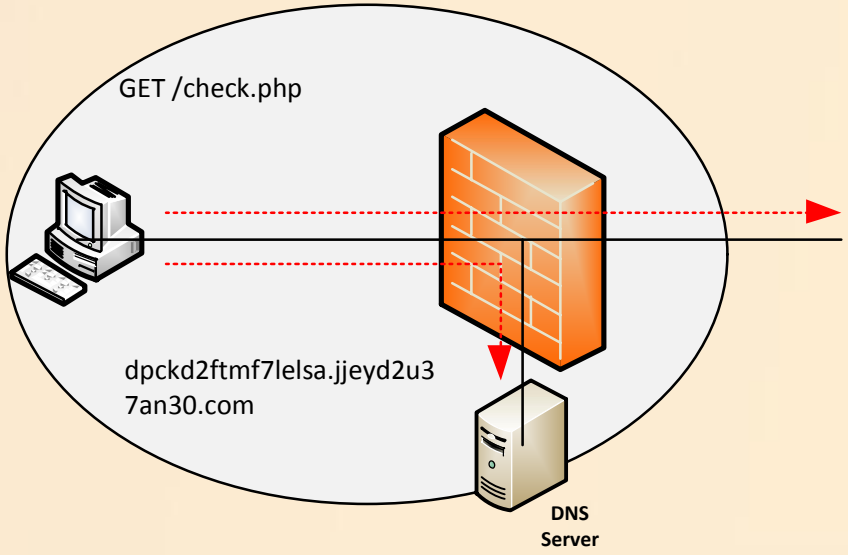
Deterministic

- Entropy (URL)
- Outgoing (Foreign)



→ **Exploitation**
→ **Malware Drop**

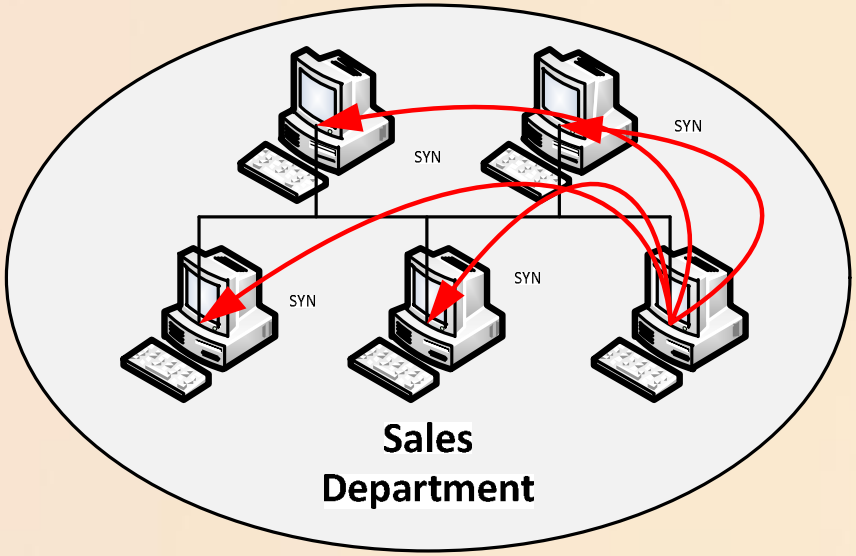
- Entropy (DNS)
- Outgoing (Foreign)



→**Command and Control**

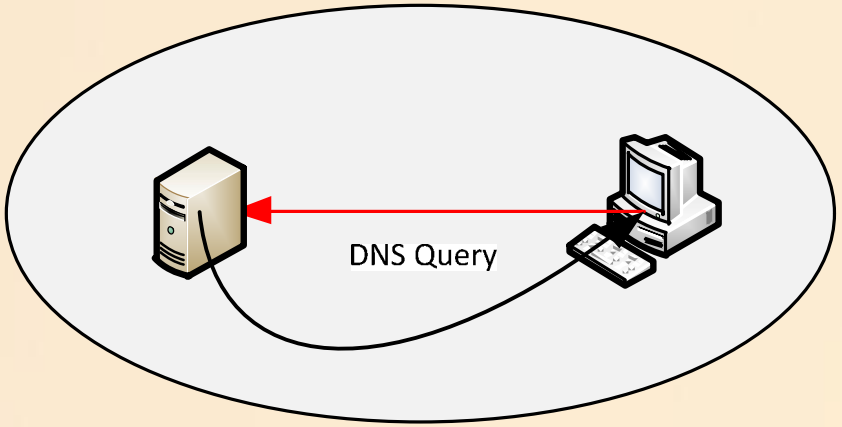
Learning

- Repeats Message
- Different Target



→ **Host Discovery**
→ **Service Discovery**

→ **Port Scans**
→ **Brute-Forcing***



- Different Messages
- Same Target

Discriminating

1. How does it compare against reference?
2. What is different about it?
3. Is this malicious behavior?
   a) Is it correlated with Other activity? Other abnormalities? Other alerts?
   b) Does comorbid activity occur?
   c) Number of Threat Indicators? Do these strengthen or weaken your conclusion?

Common False Positives

- Lack Context
  - Baseline Deficiencies
  - Modified Processes
  - Additional Workflows
- Change Management
- Other
  - Visiting Systems
  - Misconfigured Systems

Challenges

- Gaps
  - Baseline
  - Policy
- Non-Compliant
  - Systems
  - Applications

Culprits

- Rogue Elements
- Foothold Situations
- Advanced Actors

Rogue Elements

- Examples
  - Physical Breaches
  - Contractor Laptop
  - Mobile Devices (BYOD)
- Anomalies
  - Role
  - Boundary (Peer)
  - Volumetric

Foothold Situations

- Examples
  - Malware
- Anomalies
  - Geographic
  - Protocol
    - Entropy
    - Payload
    - NXDomain, 404s, 503s, and Failed Logins
    - VNC, RDP, and Unknowns

Advanced Actors

- Examples
  - Industrial Espionage
  - National States
- Anomalies
  - Boundary (Critical)
  - Temporal
  - Protocol (Payload)

Advanced Actors

- Traditional Solutions Likely To Fail
  - Extended Timeline
  - Existing Access
  - Exploitation and Privilege Escalation
- Lateral Movements
- Requires Additional Skill Sets
  - Others Tools
  - Host and Network Forensics

Your Plan

- Acquire Solution
- Know Your Own Battlespace
  - Analytical Reference
  - Baseline It
- Start A Work Process
  - Update Regularly
  - Disseminate to Team Members
- Triage Effectively

Questions