Security Operation Center

Proactive Approach to Cybersecurity

June, 2017

About me

Andoni Valverde Villar

https://www.linkedin.com/in/andoni-valverde-villar/

SIEM, OSINT, SOC/CERT, Deception

Index

1. Introduction
2. State of the Art
3. SOC 4.0
4. Strategic Threat “Thinking”
5. Proactive Threat Hunting Approaches
6. Conclusions

1. Introduction

Introduction

Audience

Some polls…

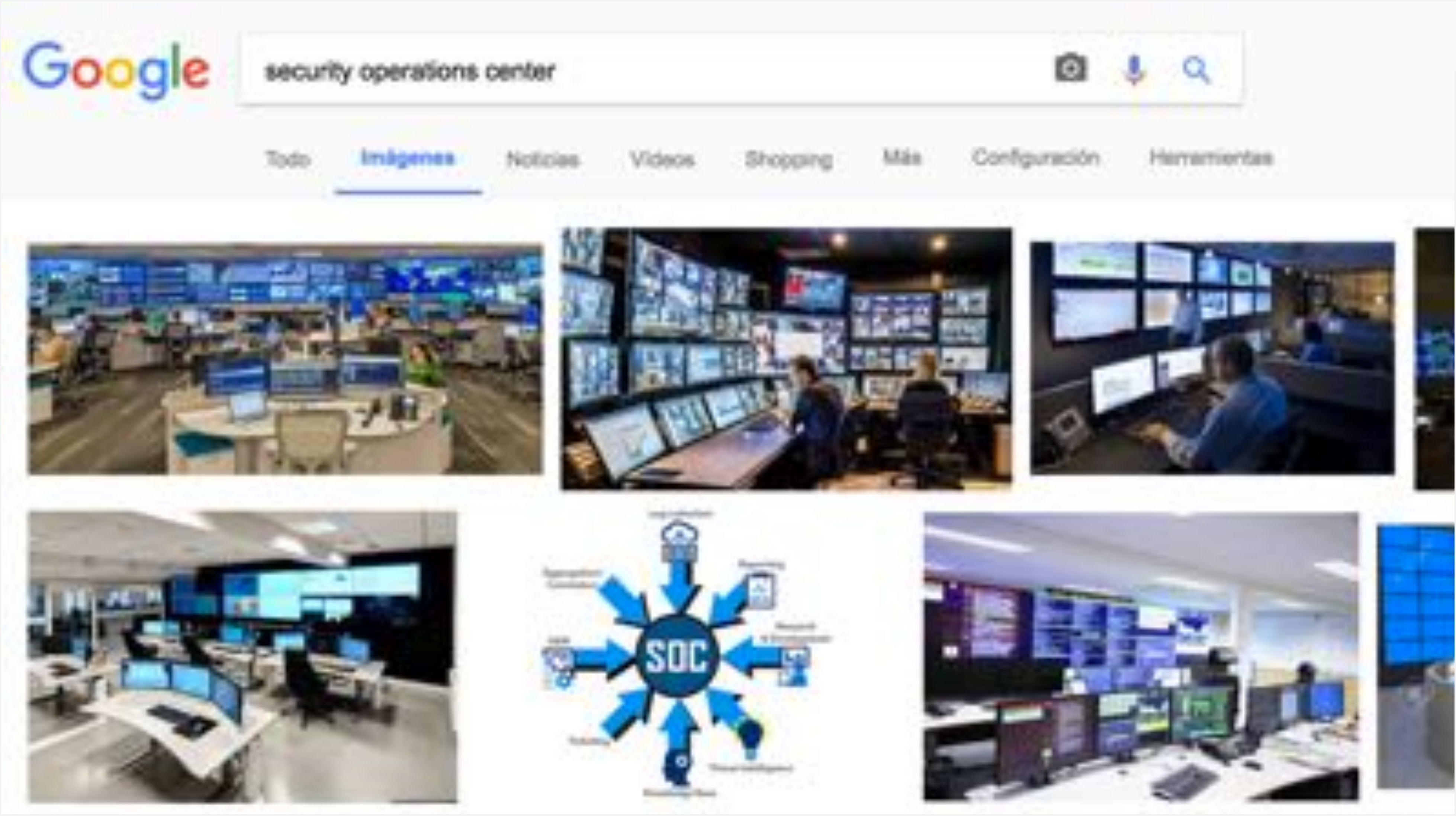
1. **Part of a SOC**: Attendees who work or have worked in a SOC.

2. **Interact with a SOC**: Attendees who have or have had some work relationship with a SOC.

Introduction

The image

Looking for pictures on Google…



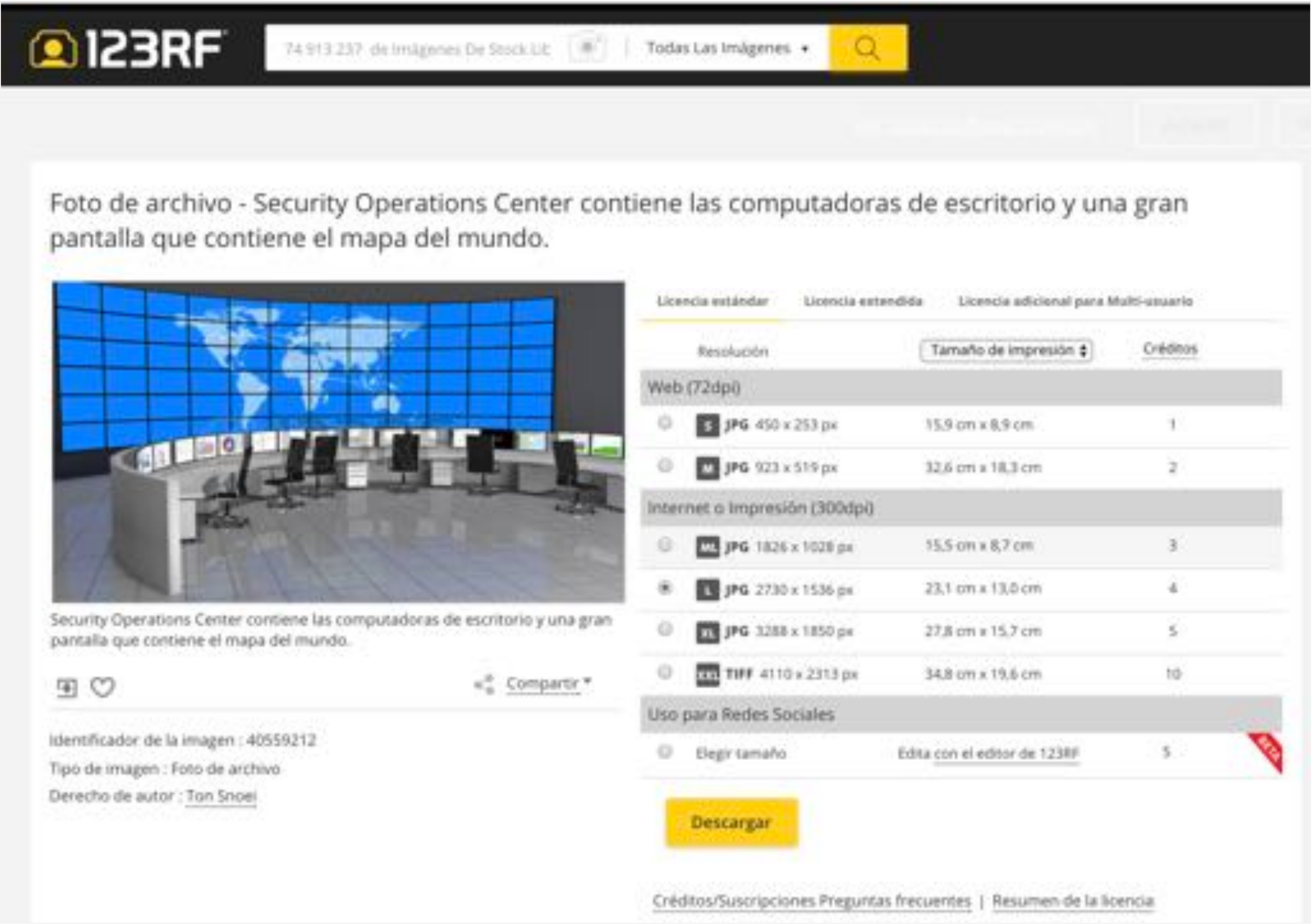


Foto de archivo - Security Operations Center contiene las computadoras de escritorio y una gran pantalla que contiene el mapa del mundo.

Security Operations Center contiene las computadoras de escritorio y una gran pantalla que contiene el mapa del mundo.

Compartir

Identificador de la imagen : 40559212
Tipo de imagen : Foto de archivo
Derecho de autor : Ton Snoei

Licencia estándar | Licencia extendida | Licencia adicional para Multi-usuario

	Resolución	Tamaño de impresión	Créditos
	Web (72dpi)		
○	S JPG 450 x 253 px	15,9 cm x 8,9 cm	1
○	M JPG 923 x 519 px	32,6 cm x 18,3 cm	2
	Internet o Impresión (300dpi)		
○	ML JPG 1826 x 1028 px	15,5 cm x 8,7 cm	3
●	L JPG 2730 x 1536 px	23,1 cm x 13,0 cm	4
○	XL JPG 3288 x 1850 px	27,8 cm x 15,7 cm	5
○	XXL TIFF 4110 x 2313 px	34,8 cm x 19,6 cm	10
	Uso para Redes Sociales		
○	Elegir tamaño	Edita con el editor de 123RF	5

Descargar

Créditos/Suscripciones Preguntas frecuentes | Resumen de la licencia

Introduction

Types – Goals – Environment – Constituency

advanced
asoc
cdc
center
cert
cirt
computer
consulting
csirt
csoc
cyber
defense
emergency
incident
industrial
intelligence
irt
isoc
operations
response
secuirty
security
sert
sioc
soc
team

Sectors:

- Academic
- Commercial
- Governmental
- Internal
- Military
- National / International
- Small / medium enterprise
- Vendor / support

Characteristics:

Centralized	Decentralized
Standard	Highly customized
Externally managed	Internally managed
Low cost	High cost

Introduction

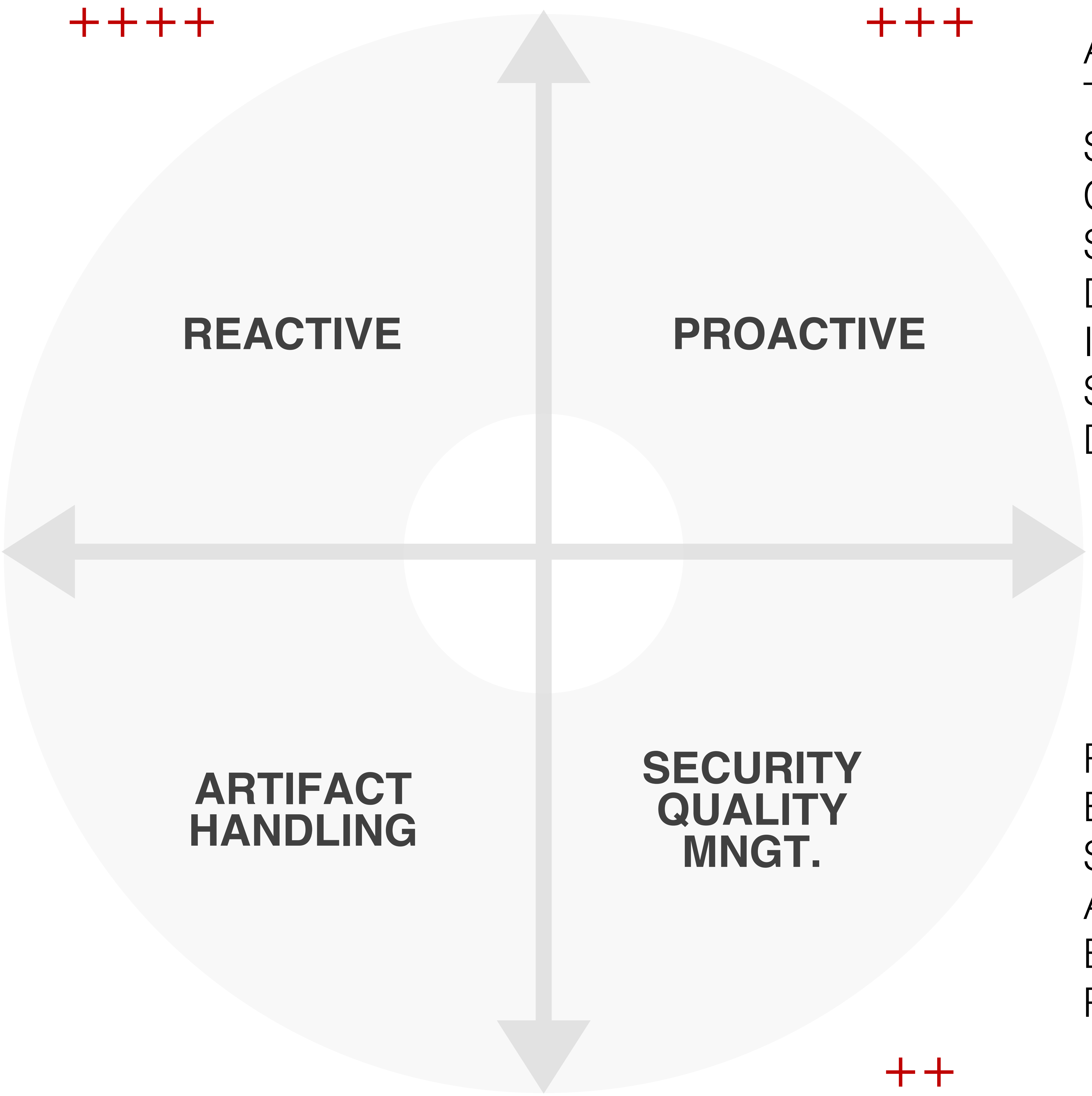
Contextualization of this talk

“As presented, there are different types of SOC with different goals and characteristics. Capabilities and provided services are also miscellaneous. Furthermore, there is usually to be a (desirable) relationship with other entities (CERT/CSIRT/IRT…) and in some cases those are an extension of the SOC themselves. Whatever your situation or experience is, this talk is focused from a generalist point of view. I hope there will be useful information for your projects progress and your enjoyment.”

Introduction

More than SIEM… Connected services = Gain efficiency = ↑ Adaptive defence

Alerts and Warnings
Incident Handling
Incident analysis
Incident response support
Incident response coordination
Incident response on site
Vulnerability Handling
Vulnerability analysis
Vulnerability response
Vulnerability response coordination



Announcements
Technology Watch
Security Audits or Assessments
Configuration and Maintenance of Security
Development of Security Tools
Intrusion Detection Services
Security-Related Information Dissemination

Artefact analysis
Artefact response
Artefact response coordination

Risk Analysis
Business Continuity and Disaster Recovery
Security Consulting
Awareness Building
Education/Training
Product Evaluation or Certification

Sources:

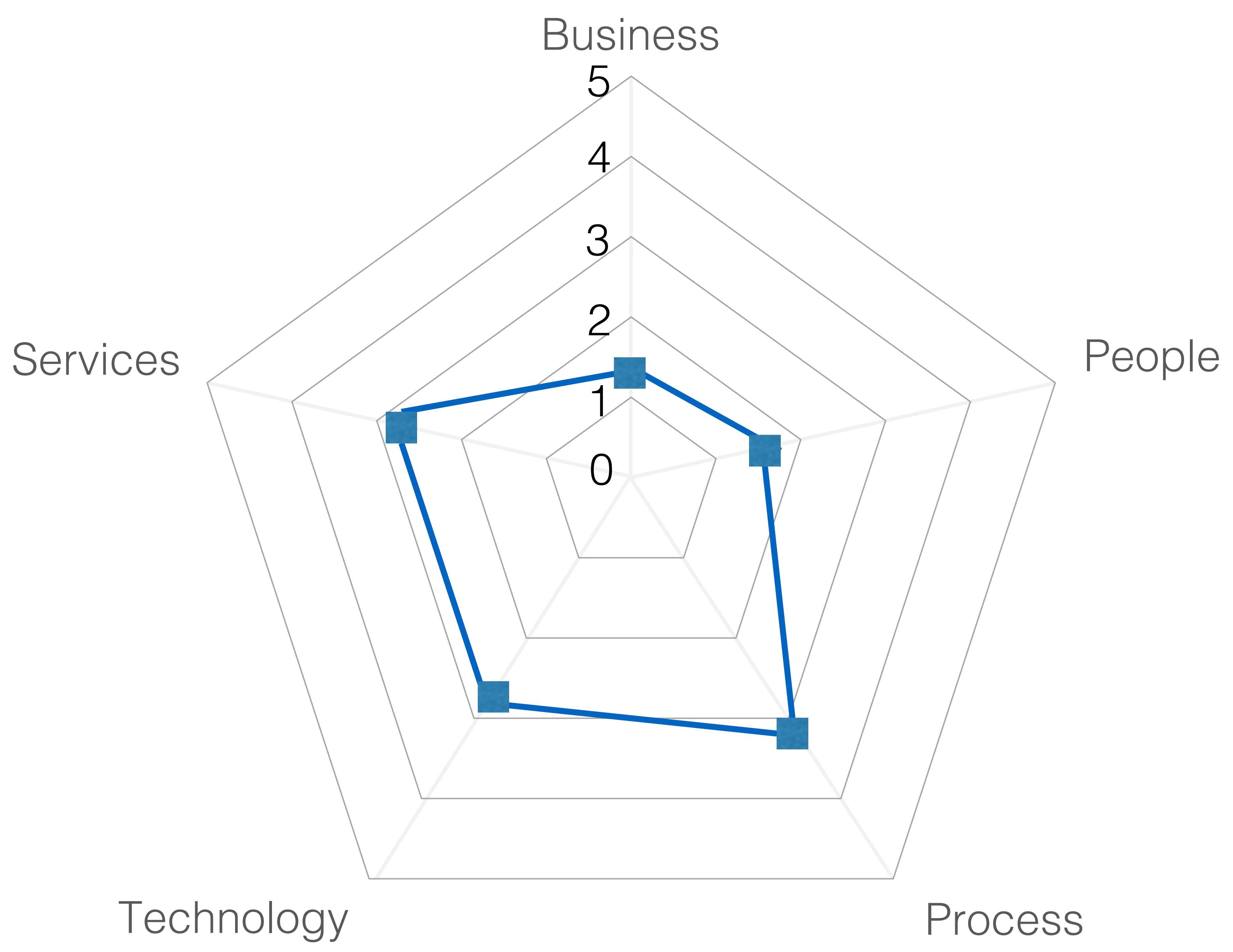
- ENISA WP2006

2. State of the Art

State of the Art

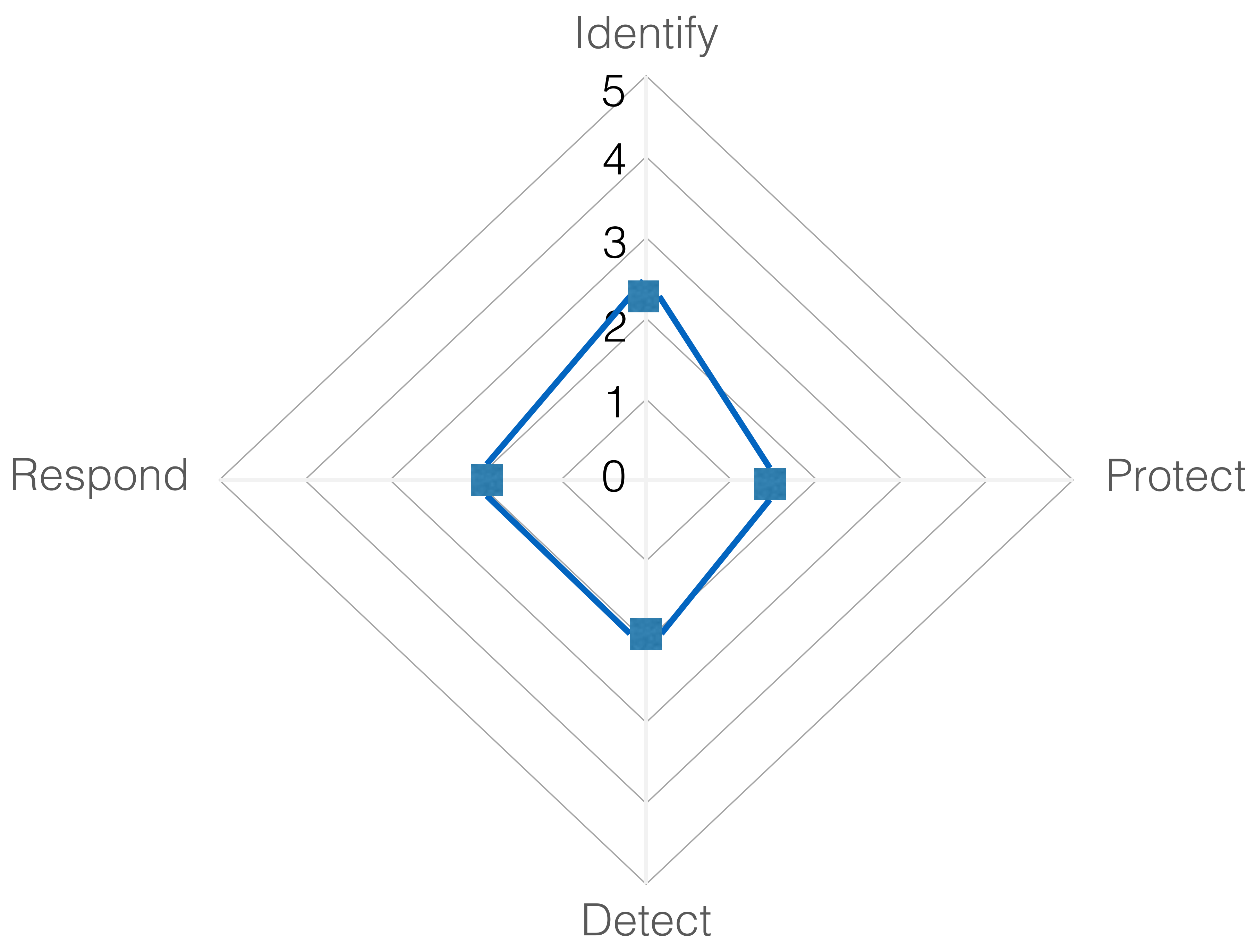
Capability & Maturity Model (SOC-CMM)

SOC-CMM



1 Initial 2 Managed 3 Defined 4 Quantitatively managed 5 Optimized

NIST CSF



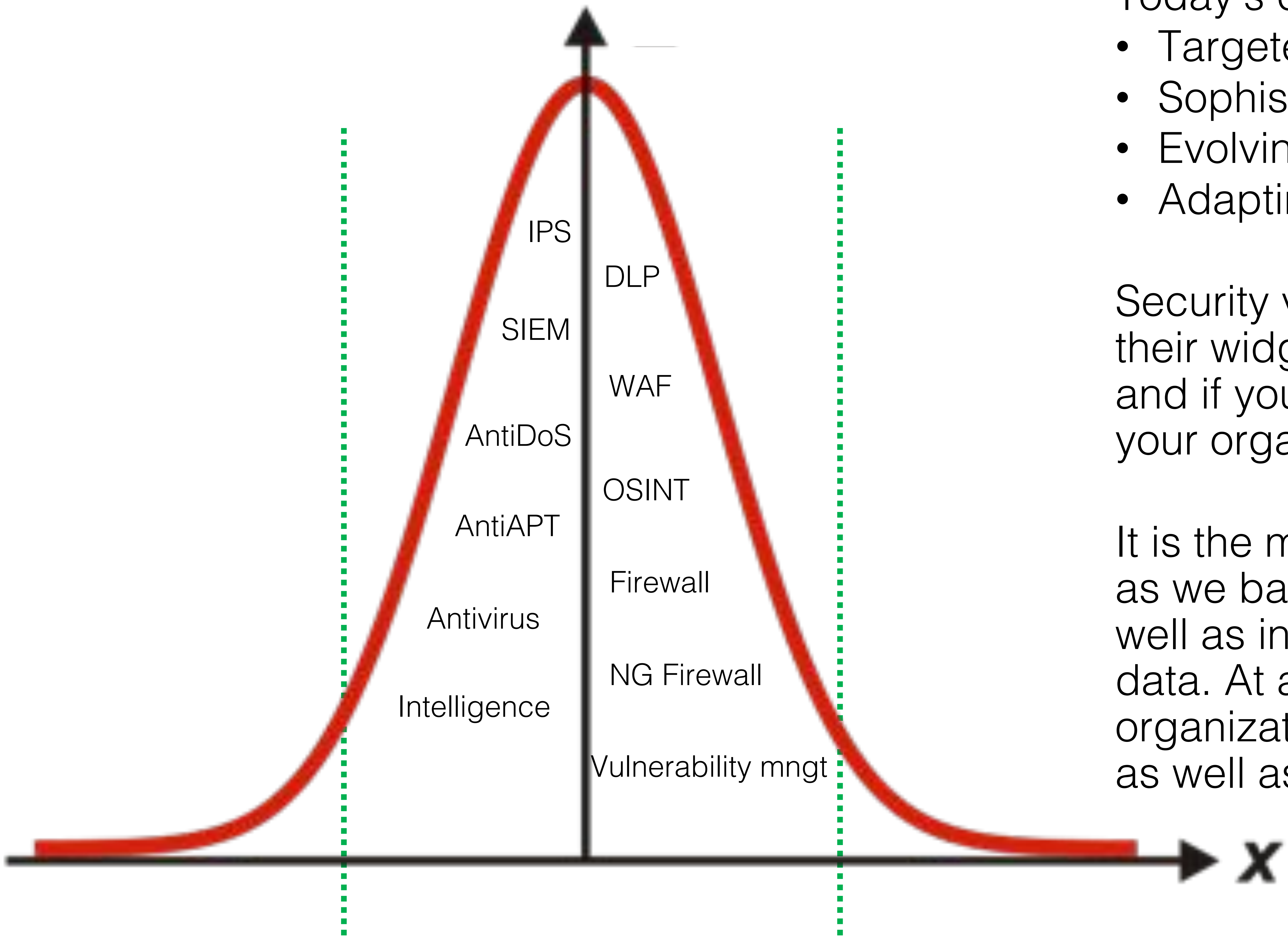
1 Initial 2 Minimal 3 Procedural 4 Innovative 5 Leading

Sources:

- Software Engineering Institute (SEI)
- HP, EY, PwC…
- https://www.soc-cmm.com
- NIST, Cyber Security Framework

State of the Art

Technologies don’t cover all spectrum



Today’s critical attacks:

- Targeted
- Sophisticated
- Evolving
- Adapting

Security vendors and solution providers have claimed their widgets were all you needed to prevent attacks and if you would only buy this feature or that add-on, your organization would be practically un-hackable.

It is the moment to rethinking the security approaches as we battle zero-day and highly targeted attacks as well as insiders attempting to exfiltration sensitive data. At a time where data breaches are on the rise, organizations are looking to improve threat detection as well as perimeter defense.

Sources:

- FireEye, From Passive to Aggressive
- Carbonblack

State of the Art

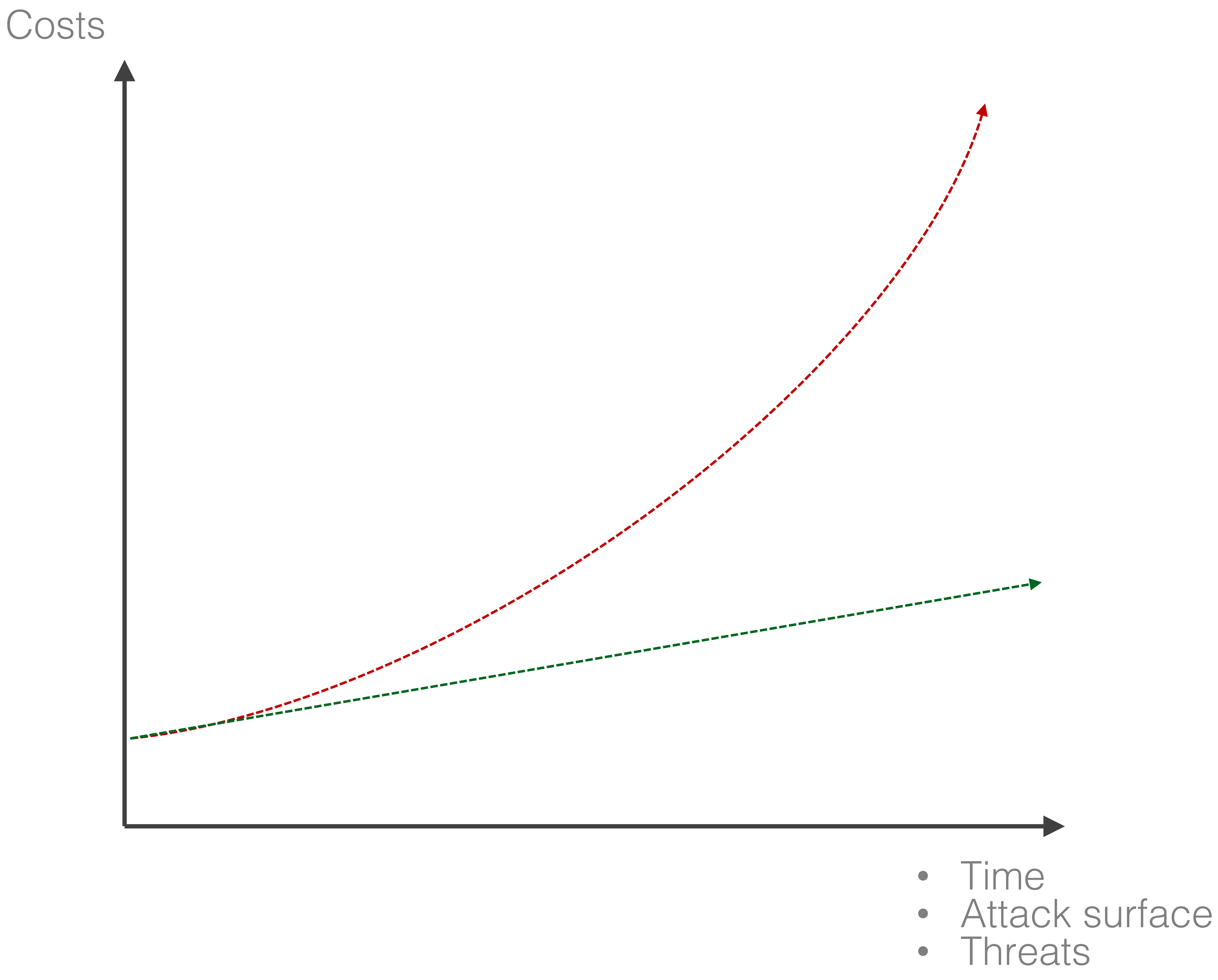
Without evolution, hopefully… it'll work as the first time

Martin Cooper

In 1983, Motorola released its first commercial mobile phone, known as the Motorola DynaTAC 8000X. The handset offered 30 minutes of talk-time, six hours standby, and could store 30 phone numbers. It also cost £2639.

State of the Art

Security is far too dynamic for someone to survive as a generalist



Time / Attack surface / Threats

- Technology
- Human resources
- Organizational

State of the Art

Why the traditional monitoring approach fails [1/4]

1. Evolving threats – Cannot prevent a breach by simply writing a check, a rule, a procedure

- Detection of advanced threats (hidden, unknown, and emerging)
- The lack of expert security staff to assist with threat mitigation
- Too much time wasted on false positive alerts

State of the Art

Why the traditional monitoring approach fails [2/4]

2. Console mentality

Waiting for an alert – Alert fatigue

- Not all the alerts are worthless, but building an entire workflow around them is the problem
- You may not have all the necessary data to know you have been attacked

State of the Art

Why the traditional monitoring approach fails [3/4]

3. Staffing crisis

State of the Art

Why the traditional monitoring approach fails [4/4]

4. Customer's thoughts (*rightly or wrongly*)

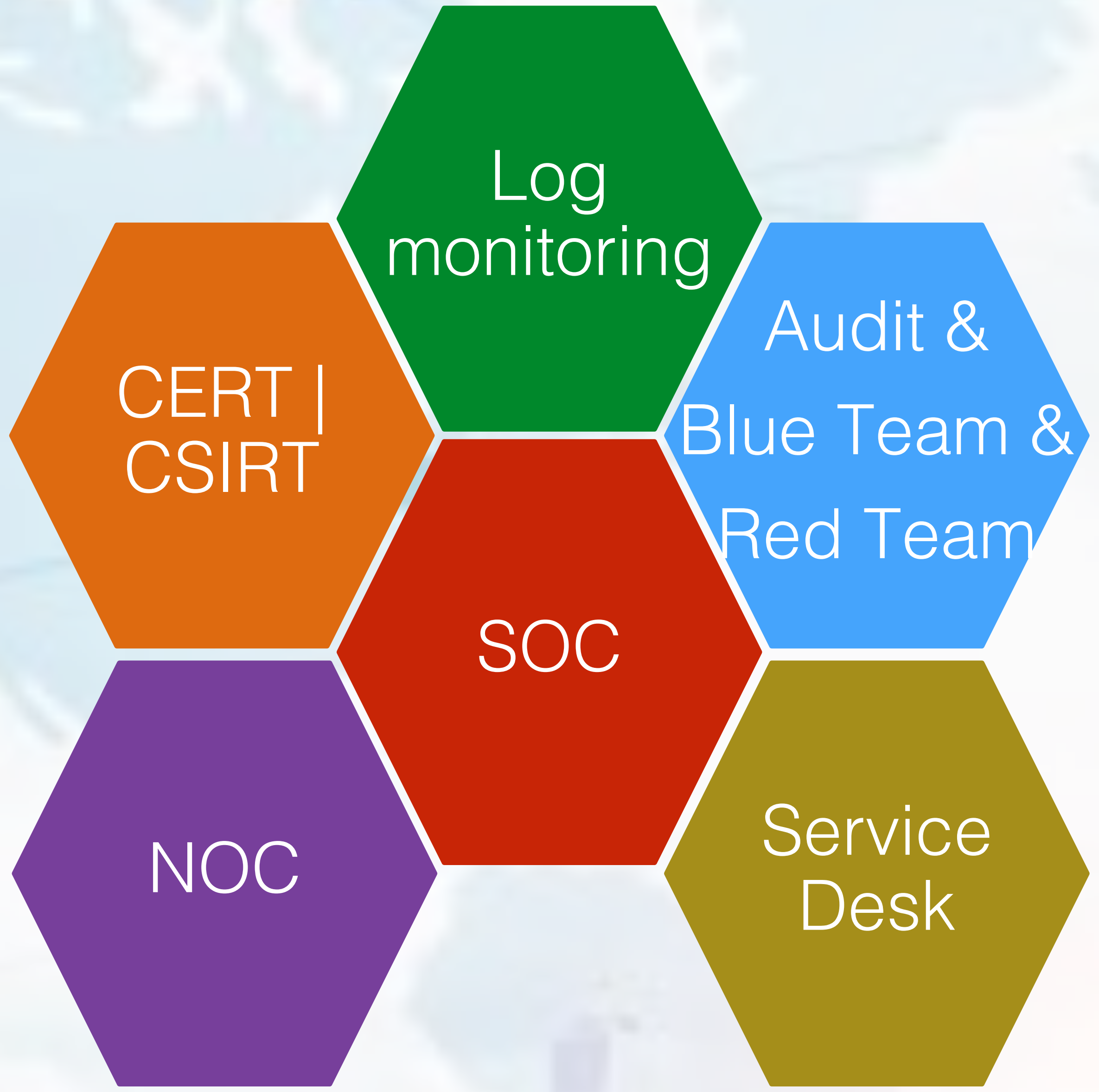
- “We are not a target” mentality
- “**Provides no value to the business**”

State of the Art

Relationship model – Strengthen the hive

Search
Advanced detection: What's not normal

Share
Collaboration and relations



Log monitoring

CERT | CSIRT

Audit & Blue Team & Red Team

SOC

NOC

Service Desk

Act
Advanced Incident Response to find, fix and defeat an adversary

Vital functions
Availability & Capacity

Route
Single Point of Contact

Protect
Continuous monitoring
Security management

State of the Art

Translation of natural evolution to market terms

SOC 1.0
Ac-hoc monitoring

- Disconnected teams
- Lack of proactivity
- Body-Shopping
- Expensive underused technologies

SOC 2.0
Sharing

- Network knowledge exchange (FIRST, Trusted Introducer…)
- Continuous improvement procedures
- Security technicians
- Away from business
- Multi geographic

SOC 3.0
Intel & Data Analytics

- Audit & improvement
- Innovation with available data (intel, big data)
- DevOps
- Security experts
- Close to business

SOC 4.0
Proactive Threat Hunting

- Adaptive defense
- Industry Threat Intelligence
- Produce quality data
- Security strategists
- Involved in business

3. SOC 4.0

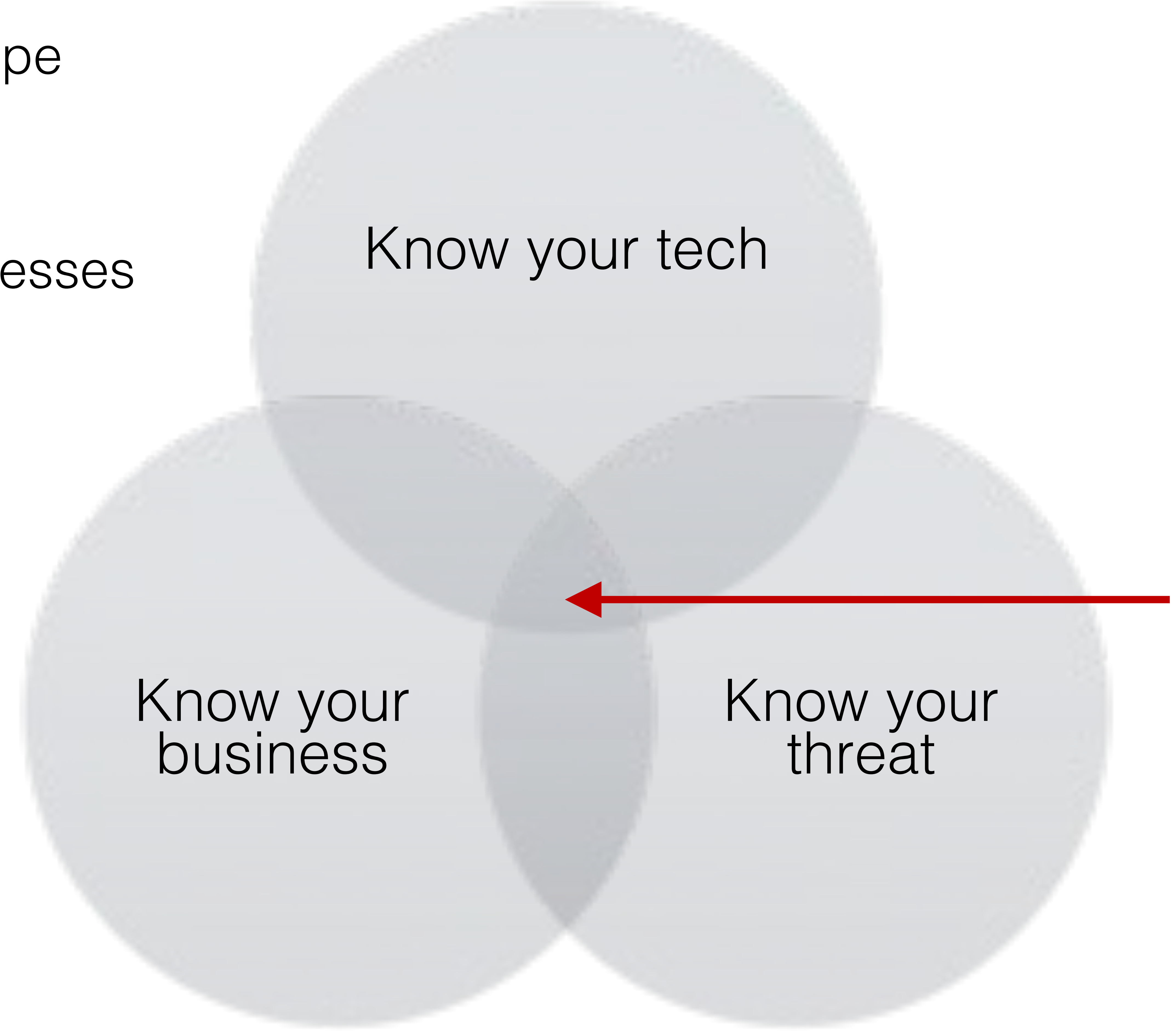
SOC 4.0

Deer or lion? Advanced cyber attacks can go unnoticed for a long period of time

SOC 4.0

Focus on you…

- Your business really is unique:
  - Different threat landscape
  - Different tech stack
  - Different business processes



Hunting means:

- Understanding your business-specific threats and motivations
- Understanding your tech stack and blind spots
- Understanding the business and what's normal

SOC 4.0

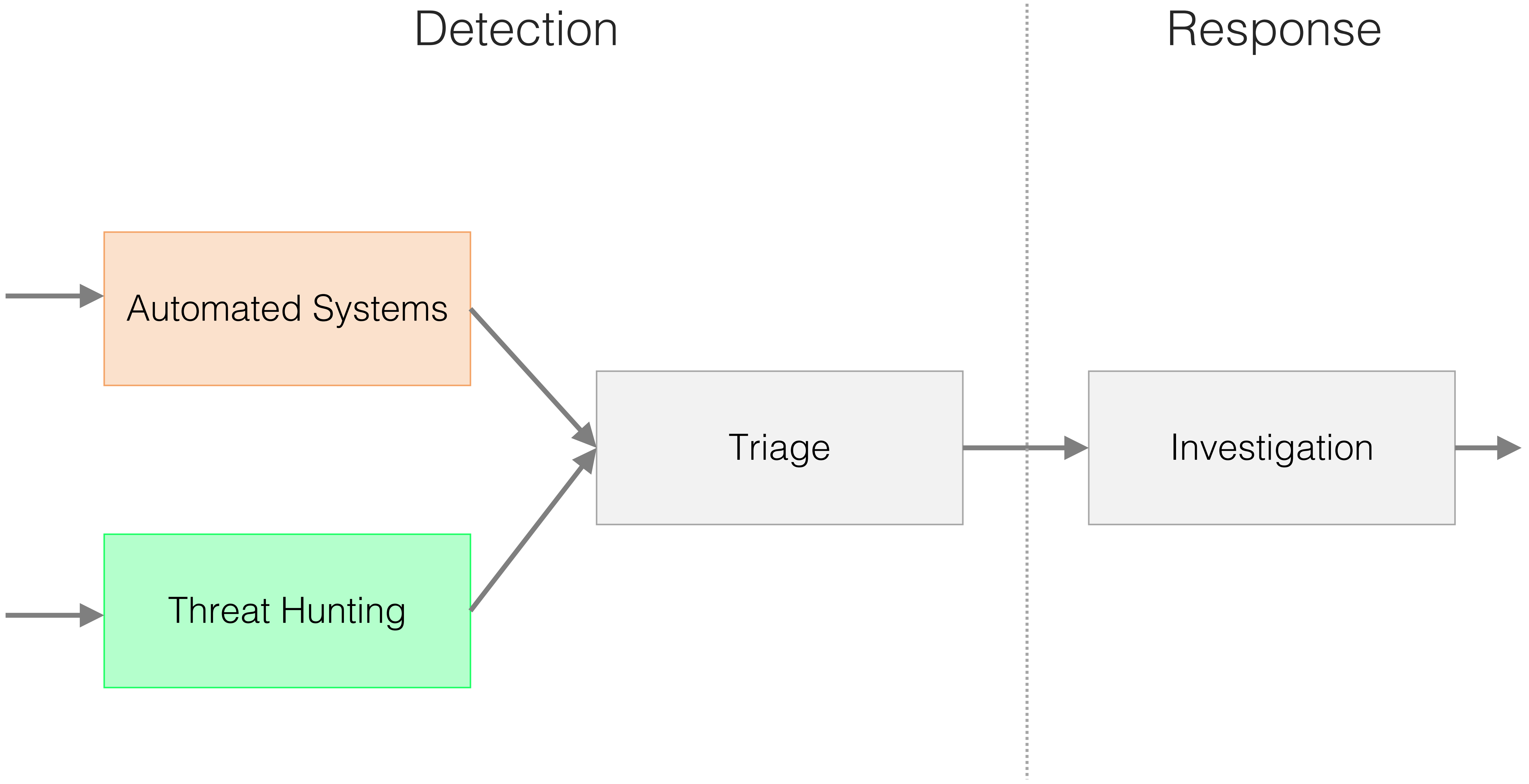
Threat = Capability + Intent + Opportunity

SOC 4.0

Embedded in your SOC: Hunting vs. Alerting – Hunting is a pre-investigation activity

Threat hunting is threat detection that is driven by a person. This concept is analogous to, but also the opposite and complement of, a concept familiar to many who practice in the IR domain: threat detection that is driven by an automated system, such as IDS/IPS or SIEM.

Automated systems and threat hunting are parallel inputs to the triage/investigation process

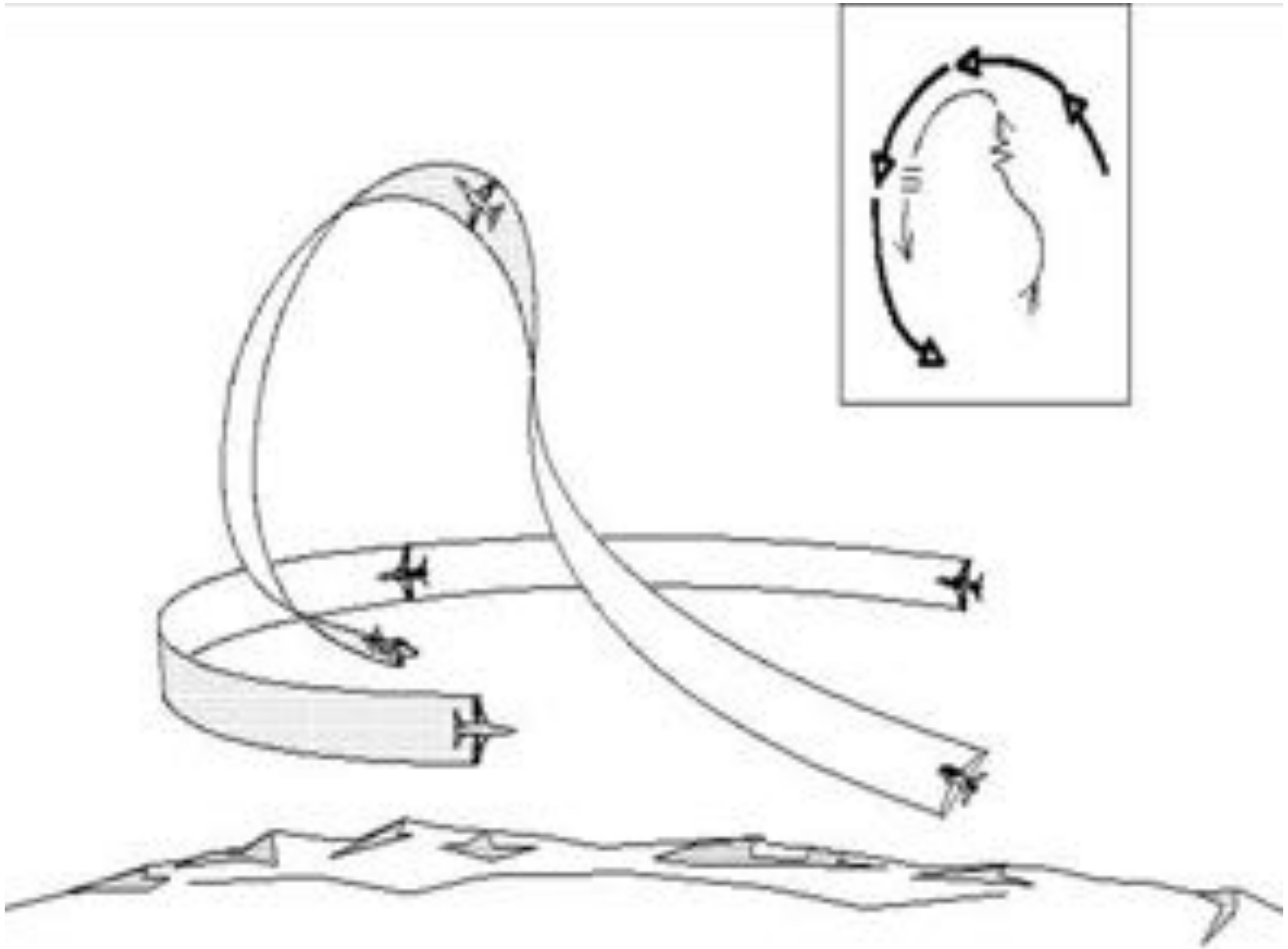


Threat hunting has (at least) two high-level goals:

- Identify attackers operating unseen in a network
- Improve automated threat detection systems

SOC 4.0

Hunting culture – OODA loop



Col John Boyd

Time is the dominant parameter. The pilot who goes through the OODA cycle in the shortest time prevails because his opponent is caught responding to situations that have already changed.

SOC 4.0

OODA loop: People, processes an technology TOGETHER

Intelligence phase

Execution phase

Observe
Old School
Orient
Decide
Act
Old School
Implicit Guidance & Control
Implicit Guidance & Control
Visibility & Real Time Information
Data from Network & Endpoints
Outside Information
Unfolding Interaction
Observations
Feed Forward
Cyber Kill Chain
Business Needs
Critical Controls
Defense Lifecycle
NIST Framework
Analysis/Synthesis
Diamond model
Common Criteria
Past Experience
PCI Standards
Feed Forward
Decision (Hypothesis)
Feed Forward
Action (Test)
Unfolding Interaction With Environment
Feedback
Feedback
Feedback

Sources:

- https://resources.sei.cmu.edu/asset_files/TechnicalReport/2015_005_001_444963.pdf

4. Strategic Threat “Thinking”

Proactive Threat Hunting

Strategic Threat “Thinking”

Needle in a haystack – Threat hunting is not a single state but a progression

- Searching for adversaries **without a particular indicator**.
- Proactively and iteratively searching through networks and IT assets to detect and respond to advanced **threats that evade traditional rule**– or signature–based security solutions.
- Combines the use of threat intelligence, analytics, and automated security tools **with human smarts**.
- Identify solid evidence indicating the presence or residual activity of attackers.
- Documentation leads to organizational **knowledge that must be shared** with SOC, Engineers, and others….
- **Continuous** improvement of your prevention and detection coverage

Strategic Threat “Thinking”

How? High level steps…

1. **Hypothesis**: Identify what to hunt for

2. Identify and collect **data needed** to carry out the hunt

3. Identify most **effective method(s)** of processing data

4. Apply method(s) to data, iterating based on **quality of results**

5. **Triage** results for detection and **investigation**

Strategic Threat “Thinking”

The program – How you get there

Starts with Visibility

Requires skilled, experienced analysts, engineers, and incident responders

Tools and Automation are important

Metrics are important

Training is critically important

Data aggregated can produce actionable intelligence

Strategic Threat “Thinking”

Relevant logs, but it’s much more than a SIEM

- Top relevant log sources
  - DHCP server
  - VPN server
  - 802.1x auth
  - DNS server
  - NAT gateway (firewall)
  - Email
  - Proxy
  - Active Directory
- Netflows
- ?

Strategic Threat “Thinking”

Define a realistic scope

Visibility

- To know the environment and acquire new focuses
- **Be specific**: Endpoint, perimeter Internet, business area…
- Manage your investment – time
- The process shall document where the information is, its uses and keep it up to date

- Add endpoint visibility
- Utilize the tools you have (SIEM, Sandbox, IDS/IPS/HIDS, Behavioral analyzers, DNS, proxy…)
- Find ”context” in every alert
- Custom alerts for your environment

Strategic Threat "Thinking"

Perhaps we need to remove the blinkers from our eyes – manage flood risk

Visibility

- Log **quality**: they can stretch the reality but not make the impossible possible.
- The endpoint will always contain the biggest footprint of malicious activity.

- We need analytical tools to manage this type & amount of data.

Strategic Threat "Thinking"

What we would like to have…

Strategic Threat “Thinking”

It is the integration of tools and people that leads to effective threat hunting

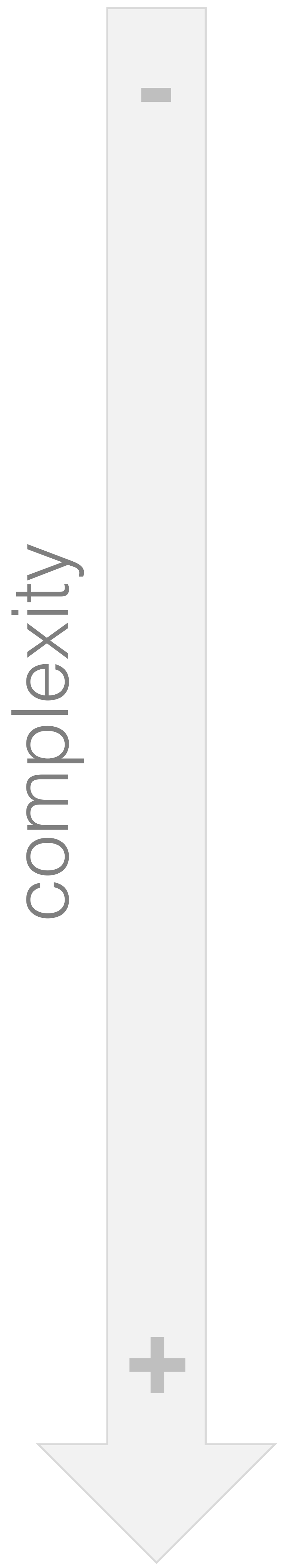
IOC? Yes, but… They understand the underline threat landscape and the organization well enough to **ask the right questions** and find the right answers

- There will always be a need for instincts
- There will always be a need for passion
- There will always be a need for curiosity

Strategic Threat “Thinking”

Transform into improve hunting in real time

Tools & Automation



- Blacklist / Whitelist
- Procedural action: Reset credential, isolate a host, block ip…
- Improve triage criteria
- Rule creation / customization
- Enrichment feed
- Retrospective behavioural check (fraud-style)
- Additional valuable information production
  - Tool or product set up (single)
  - Tool or product installation (global, i.e. endpoints)
  - Workflow orchestration
- Collateral actions (adaptive defence)

grep, head, tail, sed, awk…

ELK suit

Powershell

Volatility

Logs, logs & logs (Sagan, Graylog…)

BRO

Python

Tcpdump

Nmap

Sigcheck

YARA

Wireshark

Snort

Sysinternal Sysmon

NetFlow

MISP

APIs: Virustotal, PassiveDNS…

Strategic Threat "Thinking"

We need a methodology

Strategic Threat “Thinking”

Measurable

Metrics

Programme's ROI

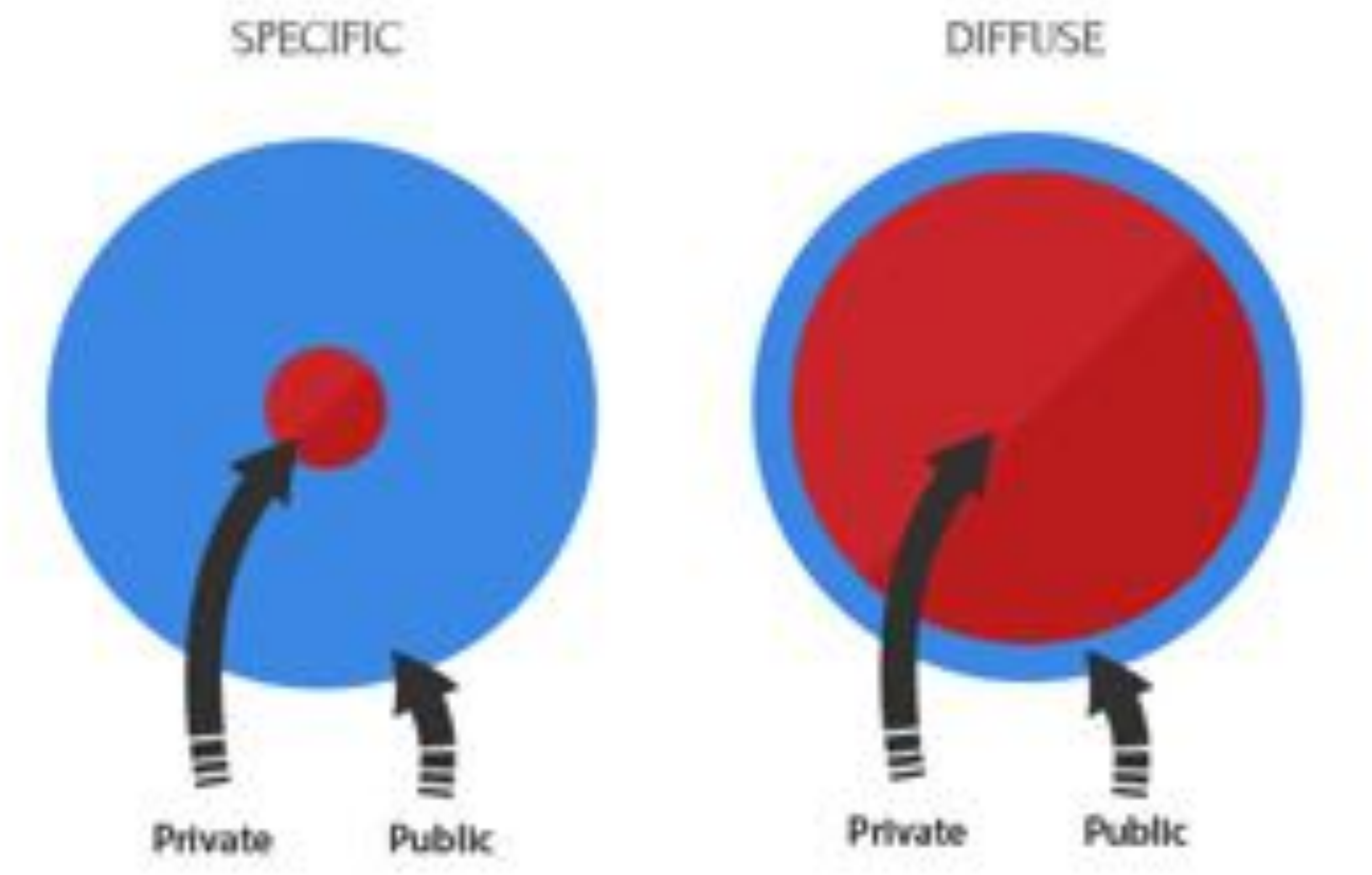
- Time to detect malicious activity
- # of campaigns being tracked
- # of IOCs discovered
- # of new breaches detected based on those IOCs
- # of rules created on the SIEM (or other tools) as a result of this findings
- Finding categorisation: weak / wrong configurations, vulnerabilities, malware, intrusions…

Strategic Threat “Thinking”

Produce & consume specific data

- Produce your own intelligence – It’s must be a result of Threat Hunting

- Focus on TTP (*Tactics, Tecniques & Procedures*) rather than IOCs
- Be specific – Industry Intelligence



Strategic Threat “Thinking”

Audience

Some polls…

- How many people have done threat hunting before in an environment?

- Done by your own or do you have an stablished program?

  - Recurrent & promoted by you organization

5. TH Approaches

Proactive Threat Hunting

Continuously adapt to adversary tactics

- Finding a specific threat is only one of the goals of hunting. The other goal is to build persistent defenses that continuously adapt to adversary tactics. You do not hunt only to find new incidents; **you also hunt to find new ways of finding new incidents**.

- There are some interesting **commercial products which will help** you with the process.

- 3 major **believes** to trigger hunting. Based on:
  - Anomalies
  - Hypotheses
  - Third-party sources, including threat intelligence.

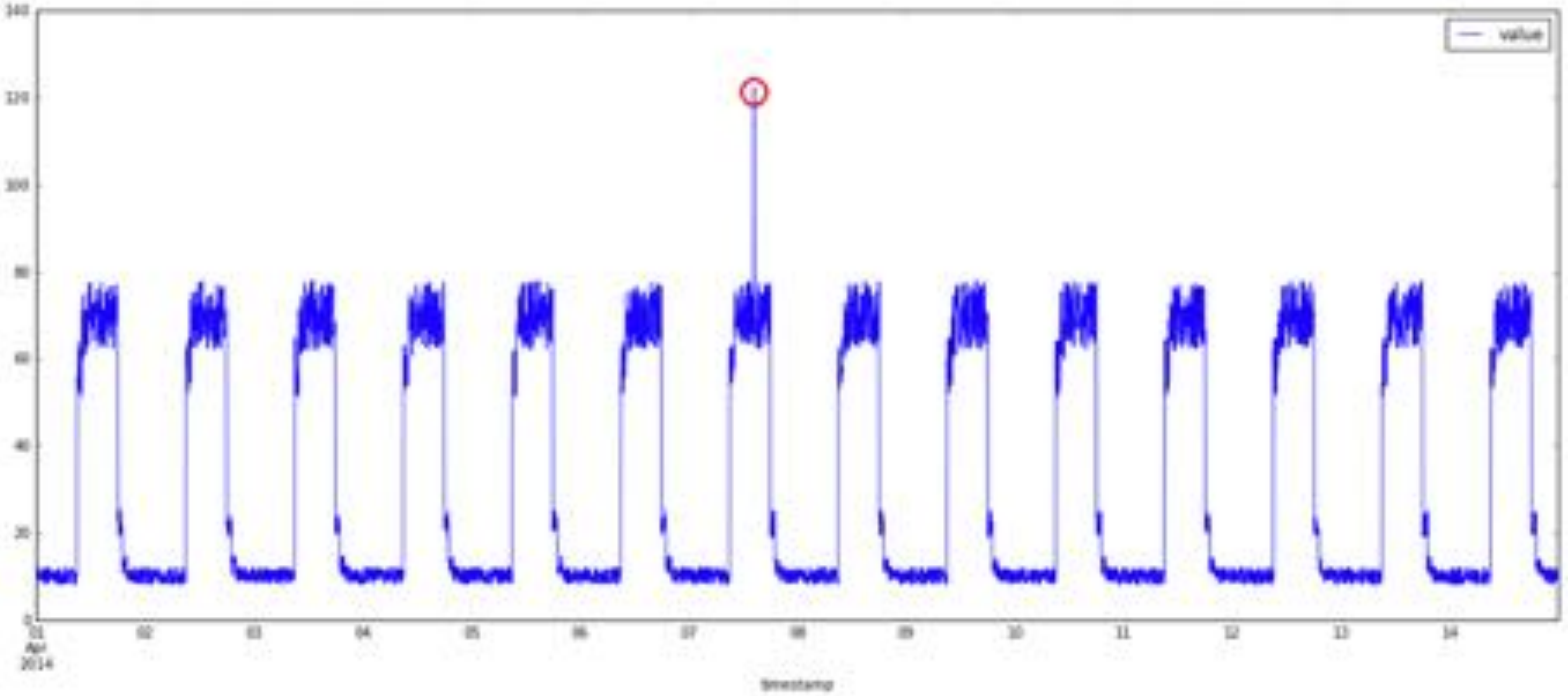
- Here, we present **3 complementary concept approaches** for Threat Hunting:
  1. Data Centric hunting
  2. DFIR style hunting
  3. Deception based hunting

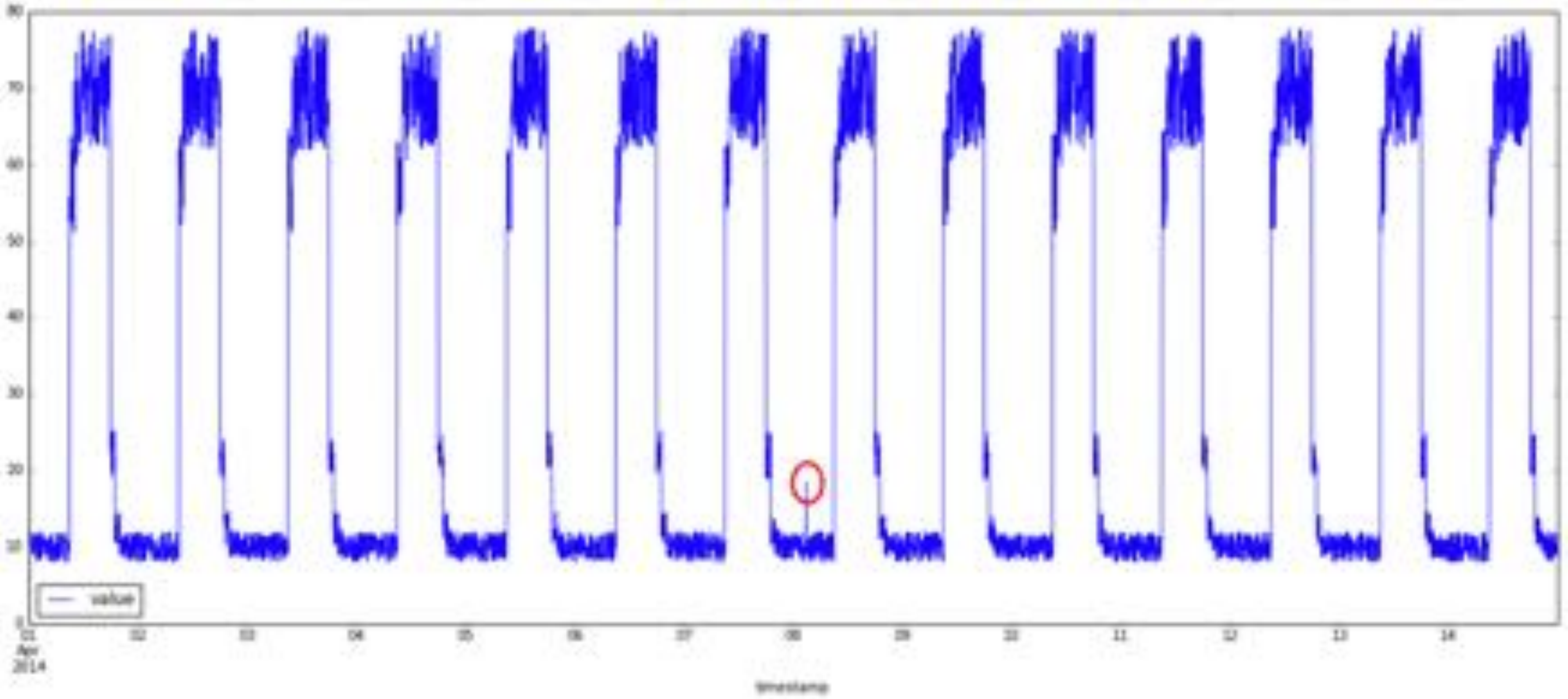
1. Data Centric Hunting

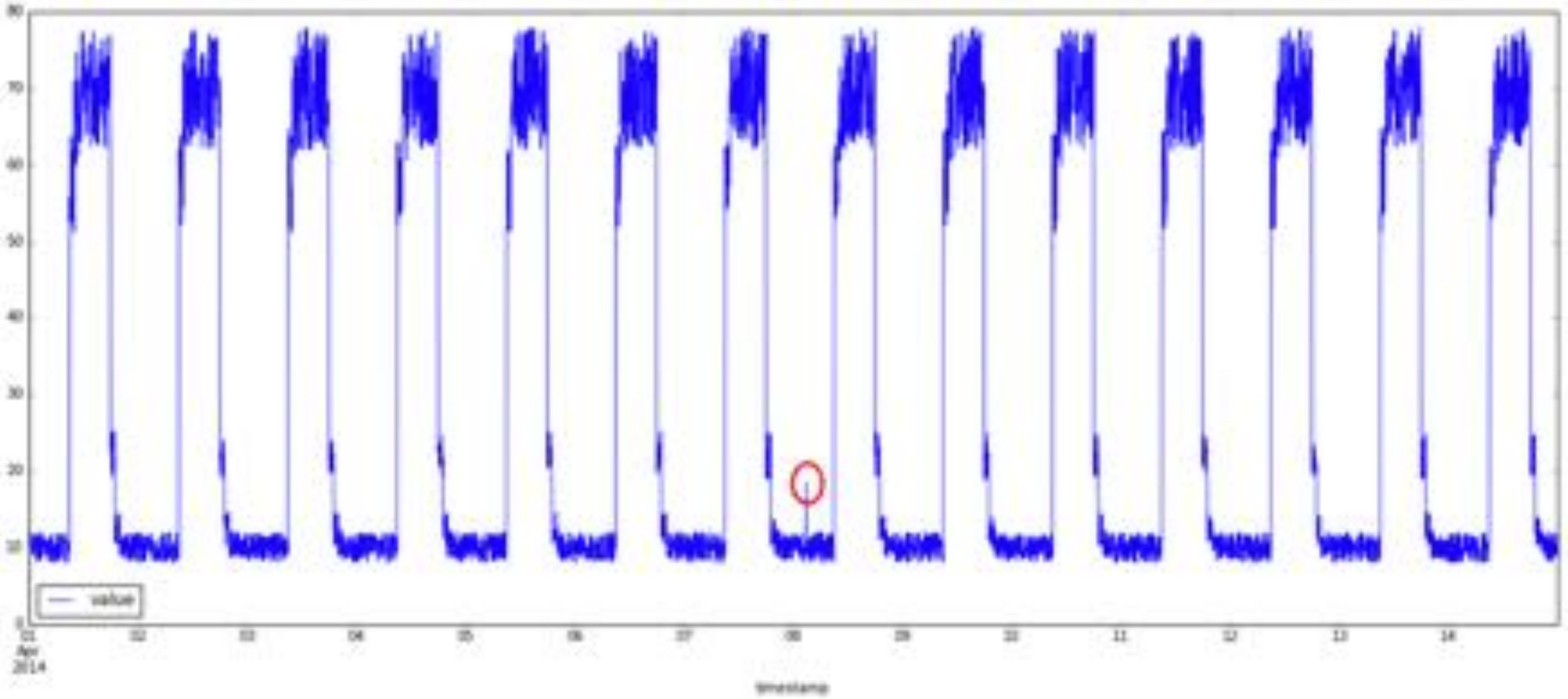
- Ingesting or querying the existing logs from a SIEM or log management solution and outputting flags on certain malicious behaviors and events that require a closer look by an analyst
- It merely applies analytics to existing stores of data and logs. Modern intrusion detection systems and EDR tools collect significantly more data and logs than they generate alerts on, so searching against this data set and correlating behavior over time can be very effective in identifying breaches that went unnoticed.
- A subcategory of security monitoring is emerging from this area called User and Entity Behavior Analytics (UEBA)

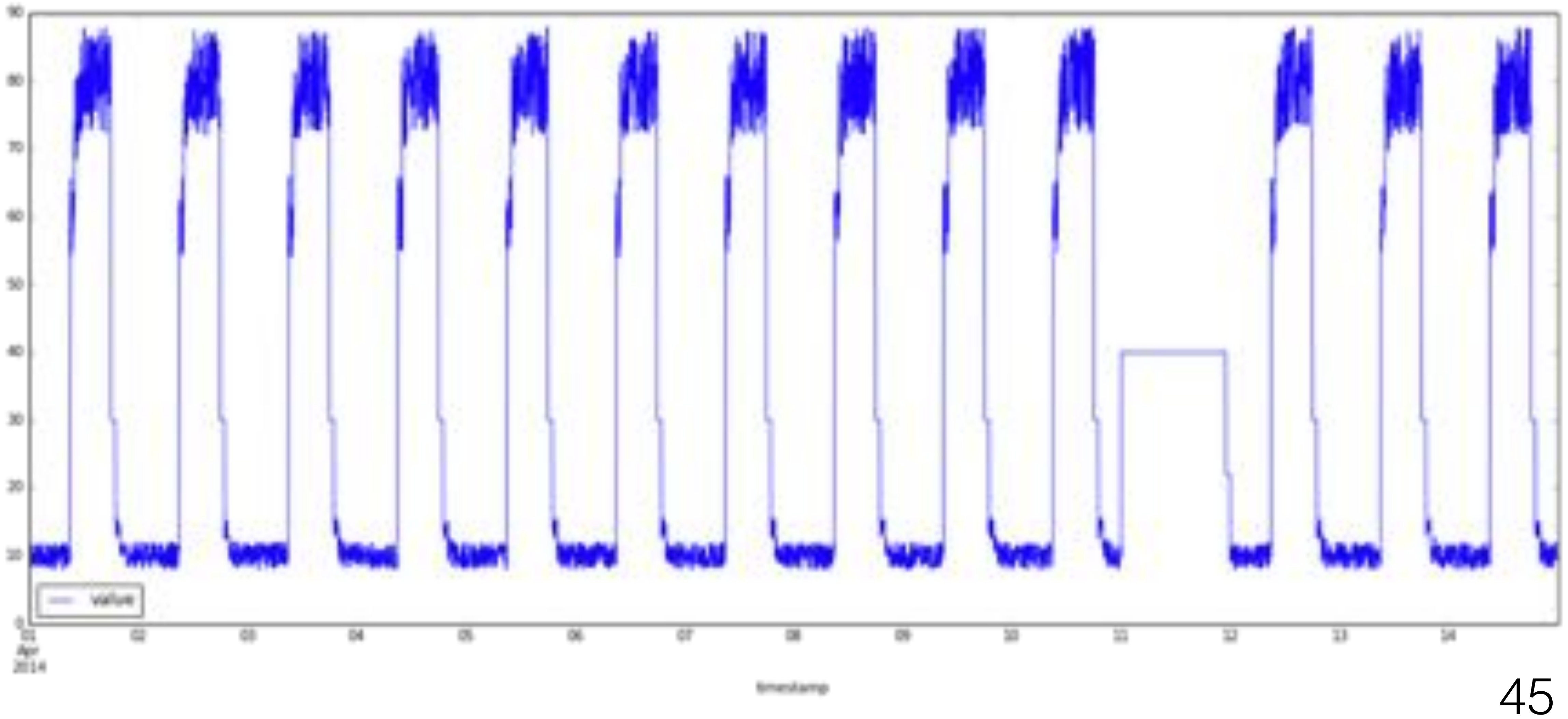
Threat Hunting – Data Centric Hunting

Anomaly detection – Statistics & AI



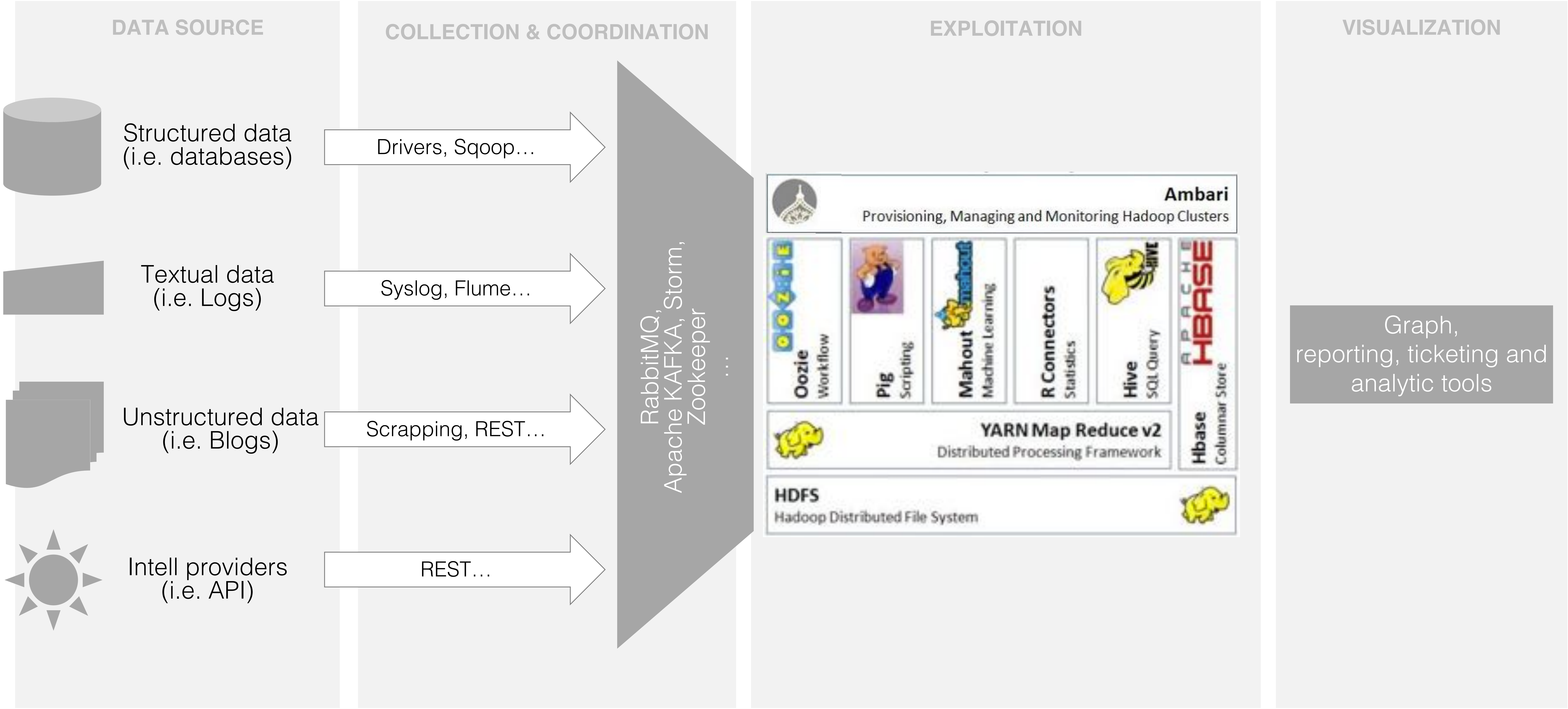






Threat Hunting – Data Centric Hunting

Architecture example



DATA SOURCE

COLLECTION & COORDINATION

EXPLOITATION

VISUALIZATION

Structured data (i.e. databases)

Drivers, Sqoop…

Textual data (i.e. Logs)

Syslog, Flume…

Unstructured data (i.e. Blogs)

Scrapping, REST…

Intell providers (i.e. API)

REST…

RabbitMQ, Apache KAFKA, Storm, Zookeeper …

Graph, reporting, ticketing and analytic tools

Threat Hunting – Data Centric Hunting

Analytical Process

1. **Select a question to answer**
2. Identify the data that matters
3. Reduce the data to a manageable amount
4. Structure the problem (clean the data, categorize, normalize, articulate)
5. Conduct formal analysis (data mining, statistics, machine learning)
6. Conduct exploration / visualization (root cause analyze and remove)
7. Confirm findings and present results

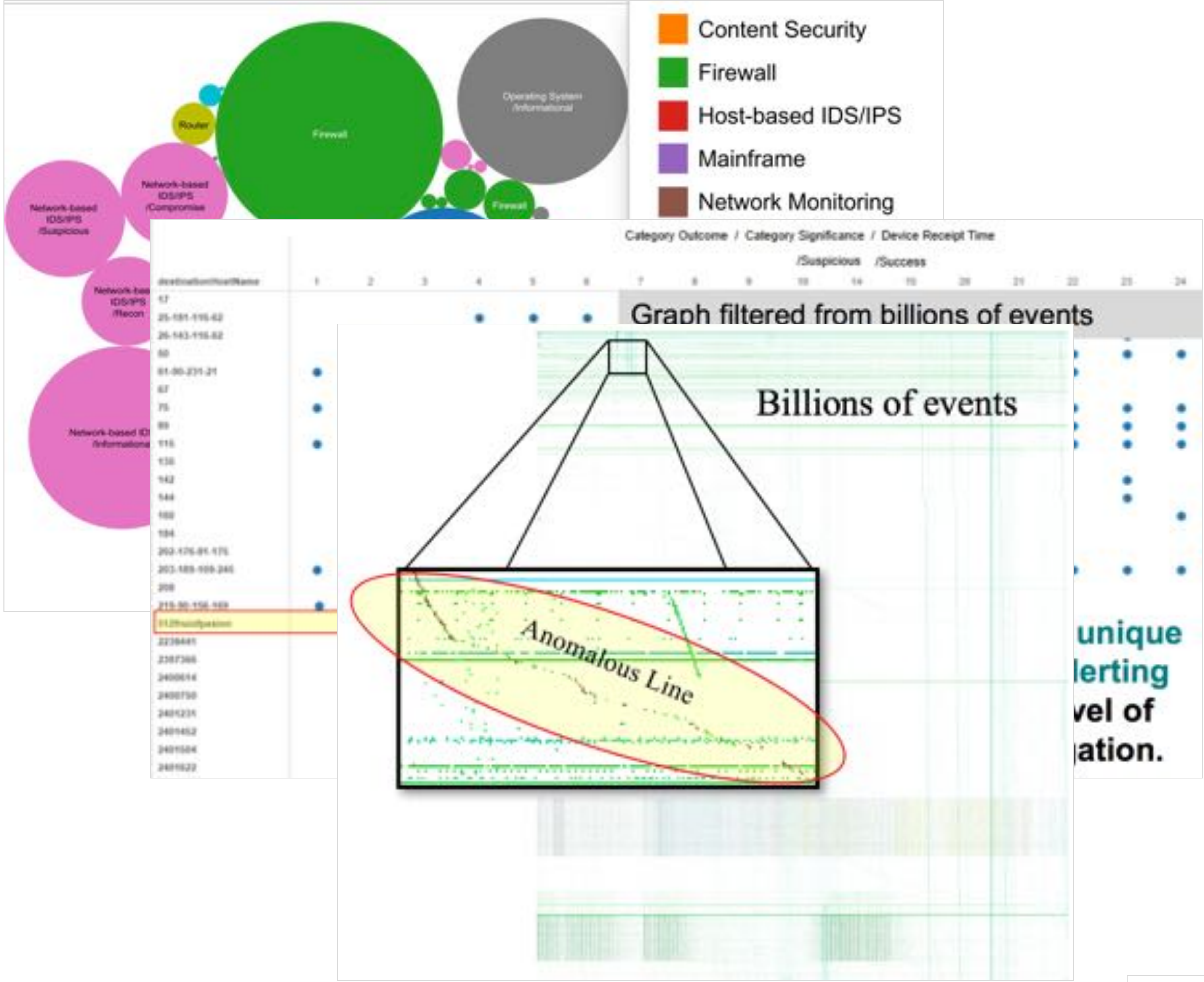
Threat Hunting – Data Centric Hunting

An example – 5 Hunt Team Use Cases

- Eg 1: Proportionality

- Eg 2: Uniqueness

- Eg 3: Stealthy activity



Sources:

- Joshua Stevens' (Hewlett-Packard) presentation at RSA Conference 2015

Threat Hunting – Data Centric Hunting

Conclusions

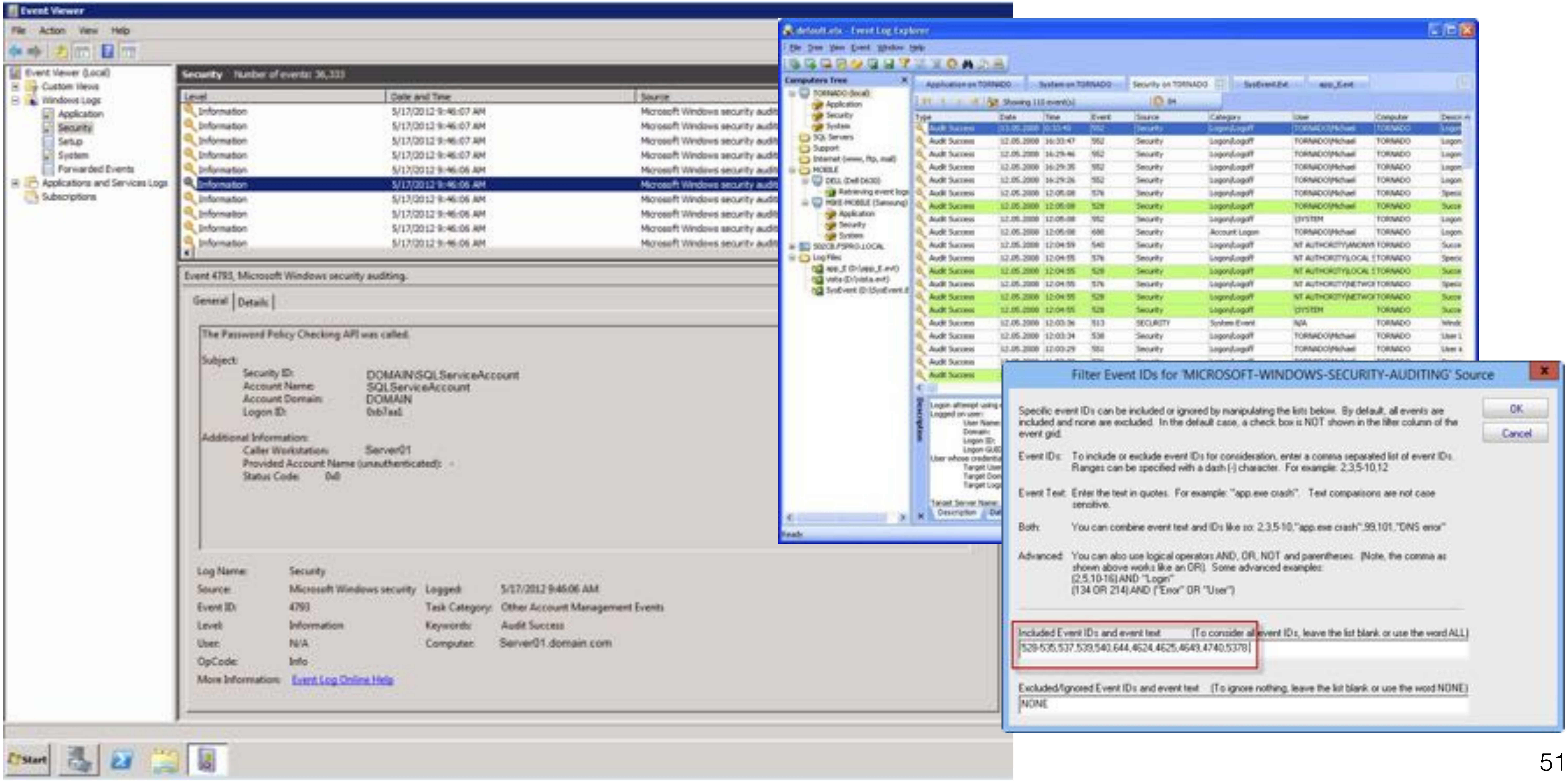
	Data-centric
Advantages	• Looking at the data over time to glean additional context • Non invasive • Modern intrusion detection systems and EDR tools collect significantly more data and logs than they generate alerts on
Disadvantages	• High skillset requirement • The existing sensors must also be mature • Require collecting and storing vast amounts of security/IT events and logs • Only appropriate to an internal SOC

/2. Digital Forensics and Incident Response (DFIR) style hunting

- **It’s an evolution of Digital Forensics and Incident Response (DFIR) with the key difference being proactive application and scale**
- The best way to detect the adversary is by learning from them
- Hunting on the Endpoint uses host/endpoint forensic information and artefacts to discover threats or artefacts indicative of compromised systems.
- Uses host/endpoint forensic information and artefacts to discover threats or artefacts indicative of compromised systems
- This is different from the behaviour analysis techniques used by your Endpoint Detection and Response (EDR) or User Behaviour Analytics (UBA) products
- SOC detects adversary behaviour ←→ DFIR observes and tracks adversary behaviour

Threat Hunting - DFIR

Looking for a needle in a haystack



Event Viewer

Security   Number of events: 36,333

Level	Date and Time	Source
Information	5/17/2012 9:46:07 AM	Microsoft Windows security audit
Information	5/17/2012 9:46:07 AM	Microsoft Windows security audit
Information	5/17/2012 9:46:07 AM	Microsoft Windows security audit
Information	5/17/2012 9:46:07 AM	Microsoft Windows security audit
Information	5/17/2012 9:46:06 AM	Microsoft Windows security audit
Information	5/17/2012 9:46:06 AM	Microsoft Windows security audit
Information	5/17/2012 9:46:06 AM	Microsoft Windows security audit
Information	5/17/2012 9:46:06 AM	Microsoft Windows security audit
Information	5/17/2012 9:46:06 AM	Microsoft Windows security audit
Information	5/17/2012 9:46:06 AM	Microsoft Windows security audit

Event 4793, Microsoft Windows security auditing.

```
The Password Policy Checking API was called.

Subject:
        Security ID:            DOMAIN\SQLServiceAccount
        Account Name:           SQLServiceAccount
        Account Domain:         DOMAIN
        Logon ID:               0xb7aa1

Additional Information:
        Caller Workstation:     Server01
        Provided Account Name (unauthenticated): -
        Status Code:    0x0
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/17/2012 9:46:06 AM
Event ID:	4793	Task Category:	Other Account Management Events
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	Server01.domain.com
OpCode:	Info		
More Information:	Event Log Online Help		

default.elx - Event Log Explorer

Showing 115 event(s)

Type	Date	Time	Event	Source	Category	User	Computer	Descr
Audit Success	13.05.2008	0:33:40	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	16:33:47	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	16:29:46	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	16:29:35	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	16:29:26	552	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	12:05:08	576	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Speci
Audit Success	12.05.2008	12:05:08	528	Security	Logon/Logoff	TORNADO\Michael	TORNADO	Succe
Audit Success	12.05.2008	12:05:08	552	Security	Logon/Logoff	SYSTEM	TORNADO	Logon
Audit Success	12.05.2008	12:05:08	680	Security	Account Logon	TORNADO\Michael	TORNADO	Logon
Audit Success	12.05.2008	12:04:59	540	Security	Logon/Logoff	NT AUTHORITY\ANONYM	TORNADO	Succe
Audit Success	12.05.2008	12:04:55	576	Security	Logon/Logoff	NT AUTHORITY\LOCAL S	TORNADO	Speci
Audit Success	12.05.2008	12:04:55	528	Security	Logon/Logoff	NT AUTHORITY\LOCAL S	TORNADO	Succe
Audit Success	12.05.2008	12:04:55	576	Security	Logon/Logoff	NT AUTHORITY\NETWOR	TORNADO	Speci
Audit Success	12.05.2008	12:04:55	528	Security	Logon/Logoff	NT AUTHORITY\NETWOR	TORNADO	Succe
Audit Success	12.05.2008	12:04:55	528	Security	Logon/Logoff	SYSTEM	TORNADO	Succe
Audit Success	12.05.2008	12:03:36	513	SECURITY	System Event	N/A	TORNADO	Windc
Audit Success	12.05.2008	12:03:34	538	Security	Logon/Logoff	TORNADO\Michael	TORNADO	User L
Audit Success	12.05.2008	12:03:29	551	Security	Logon/Logoff	TORNADO\Michael	TORNADO	User i
Audit Success								
Audit Success								

Filter Event IDs for 'MICROSOFT-WINDOWS-SECURITY-AUDITING' Source

Specific event IDs can be included or ignored by manipulating the lists below. By default, all events are included and none are excluded. In the default case, a check box is NOT shown in the filter column of the event grid.

Event IDs: To include or exclude event IDs for consideration, enter a comma separated list of event IDs. Ranges can be specified with a dash (-) character. For example: 2,3,5-10,12

Event Text: Enter the text in quotes. For example: "app.exe crash". Text comparisons are not case sensitive.

Both: You can combine event text and IDs like so: 2,3,5-10,"app.exe crash",99,101,"DNS error"

Advanced: You can also use logical operators AND, OR, NOT and parentheses. (Note, the comma as shown above works like an OR). Some advanced examples:
(2,5,10-16) AND "Login"
(134 OR 214) AND ("Error" OR "User")

Included Event IDs and event text (To consider all event IDs, leave the list blank or use the word ALL)
528-535,537,539,540,644,4624,4625,4649,4740,5378

Excluded/Ignored Event IDs and event text (To ignore nothing, leave the list blank or use the word NONE)
NONE

Threat Hunting - DFIR

What is normal?

- “**Normal**” is unique to a particular organization
- Unfamiliarity with “normal” leads to extremely ineffective response

- What if you knew…
  - Running processes
  - Process privileges
  - Network activity
  - Kernel drivers
  - Persistence mechanisms
  - Scheduled tasks
  - Services

Threat Hunting - DFIR

Baseline

Are we…

- Logging the correct type of data and event IDs
- What's needed on all type of systems
- Forwarding log data to our our SIEM
  - What about workstations?
- Is enabled PowerShell module logging?
- Seeing this events in our SIEM
- Correlating events to anomalous activity

Threat Hunting - DFIR

Check check check [1/3]

1. Are abnormal user accounts being used? Are user accounts being added locally?

2. Do Windows processes have (*lsass, svchosts, csrss…*) have strange parents? Winlogon and LSASS injection. Detect rare thread injections to *svchost* (Service host)

3. Are IE, Acrobat, Word, Notepad… spawning child processes? Monitor browser and Office processes that have suspicious executables (*cmd, Powershell, csript.exe, wscript.exe, rundll32.exe,…*) as child process on workstations.

4. Analyze network connections for non-browsers executables with abnormal number of connections to Internet. I.e. are Office applications making outbound connections?

5. Are several fields being modified by a single process?

Threat Hunting - DFIR

Check check check [2/3]

6. Identification of suspicious file names (*i.e. *dump*, *hash*, *password*, single character*). Detect Malware based on the fact that it often uses short names (few letters)

7. Identify the use of utilities preferred by attackers (*i.e. at.exe, rar.exe, psexec.exe, psexesvc.exe, wmic.exe, powershell.exe, cscript.exe, wscript.exe, mofcomp.exe, scrcons.exe, csc.exe w/ installutil.exe*)

8. Identify binaries run from suspicious paths (*i.e. c:\temp, c:\wmpub, c:\Windows\addins, C:\users, C:\PerfLogs, /tmp*)

9. Look for evidence of file description mismatch.

10. Scheduled Tasks Example: Look for evidence of malicious "AT" job files

11. Also, Microsoft signed image loads (*IEExec, InstallUtil.exe, Regsvr32.exe, Rundll32,exe…*)

Sources:

- https://raw.githubusercontent.com/subTee/ApplicationWhitelistBypassTechniques/master/TheList.txt

Threat Hunting - DFIR

Check check check [3/3]

12. Image (DLLs) and driver loads
13. Is ftp or robocopy being used?
14. Are processes executing that don’t have a .exe or .src extension?
15. Monitor some relevant commands: *whoami, net user, useradd, userdel, useraccount (WMIC), Get-NetIPConfiguration (PowerShell), hostname, ipconfig / ifconfig, nicconfig (WMIC), …*
16. Detect long PowerShell commands that most probably will include obfuscated malicious code by length of command. A similar query searches for the presence of Invoke-Expression or IEX or Download strings
17. Monitor the execution of Windows Management Instrumentation Command-line on endpoints (WMIC.exe)
18. Detect suspicious execution of rundll[32].exe when the command line contains path to User Profile and the parent command line is browser

Threat Hunting

Pros & Cons

	Endpoint (DFIR-style)
Advantages	• There are some data points that can be checked that are not, collected by monitoring tools • This approach even works for less mature organizations that don’t have complete visibility or enough centralized retention of data/logs
Disadvantages	• More invasive as it collects forensic information from each host • Focused in workstations. Complex in infrastructure devices or devices running non-standard operating systems (i.e. switches, printers, etc.)

3. Deception

- “It’s all about the data.”
- While data is important, the *quality* of the data is more important than the quantity

BOLOGN
Carlsberg

Cyber Security Deception

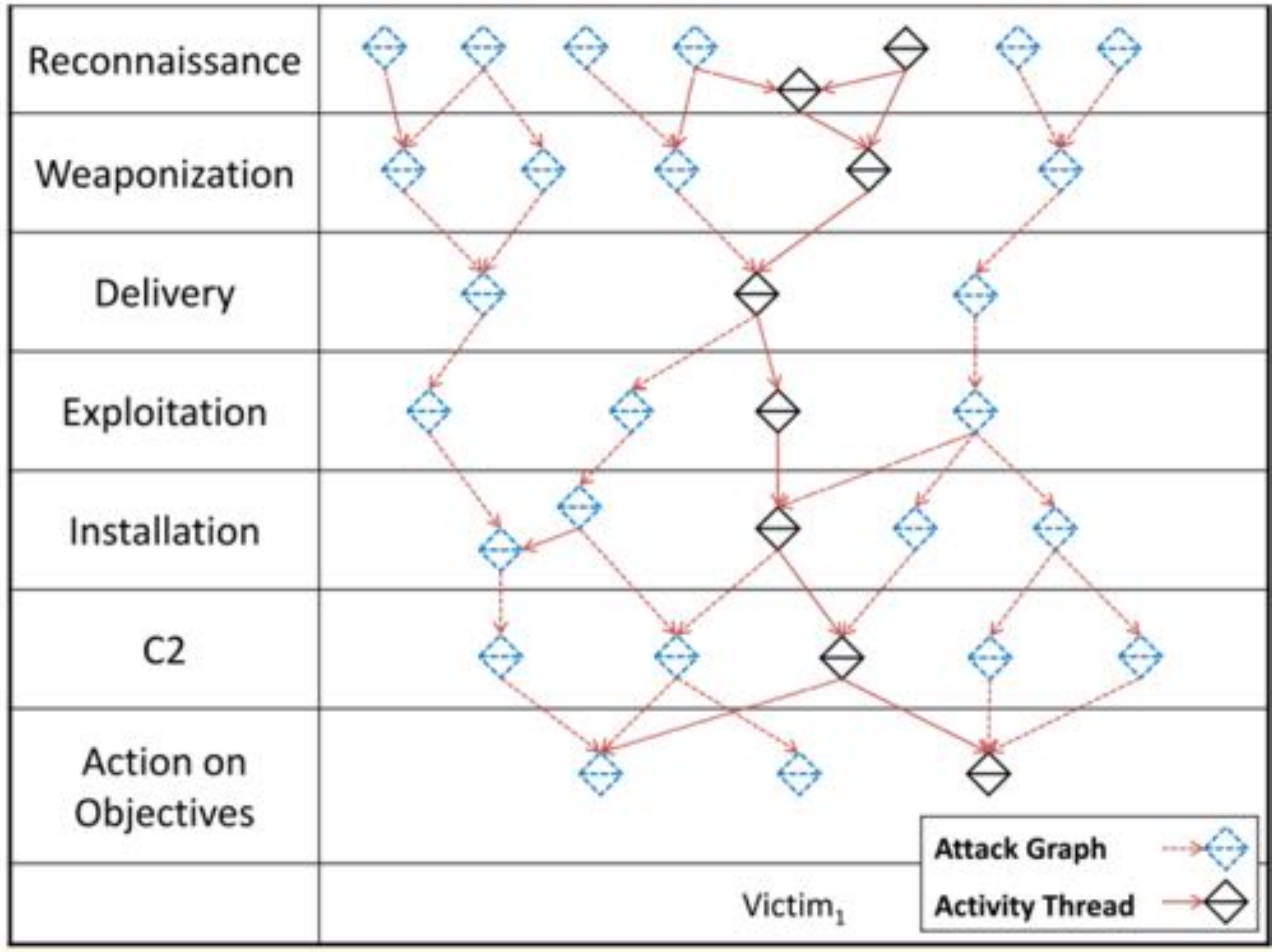
Design the Activity-Attack Graph

- Actors may be motivated by a variety of factors
- A proportion of them will decide to act on that motivation, become an adversary, choose a target and goal and then work towards it

❑ Identify the tipping point

❑ Discern between

- A global attacker
- A persisting attacker
- Those who have internal knowledge

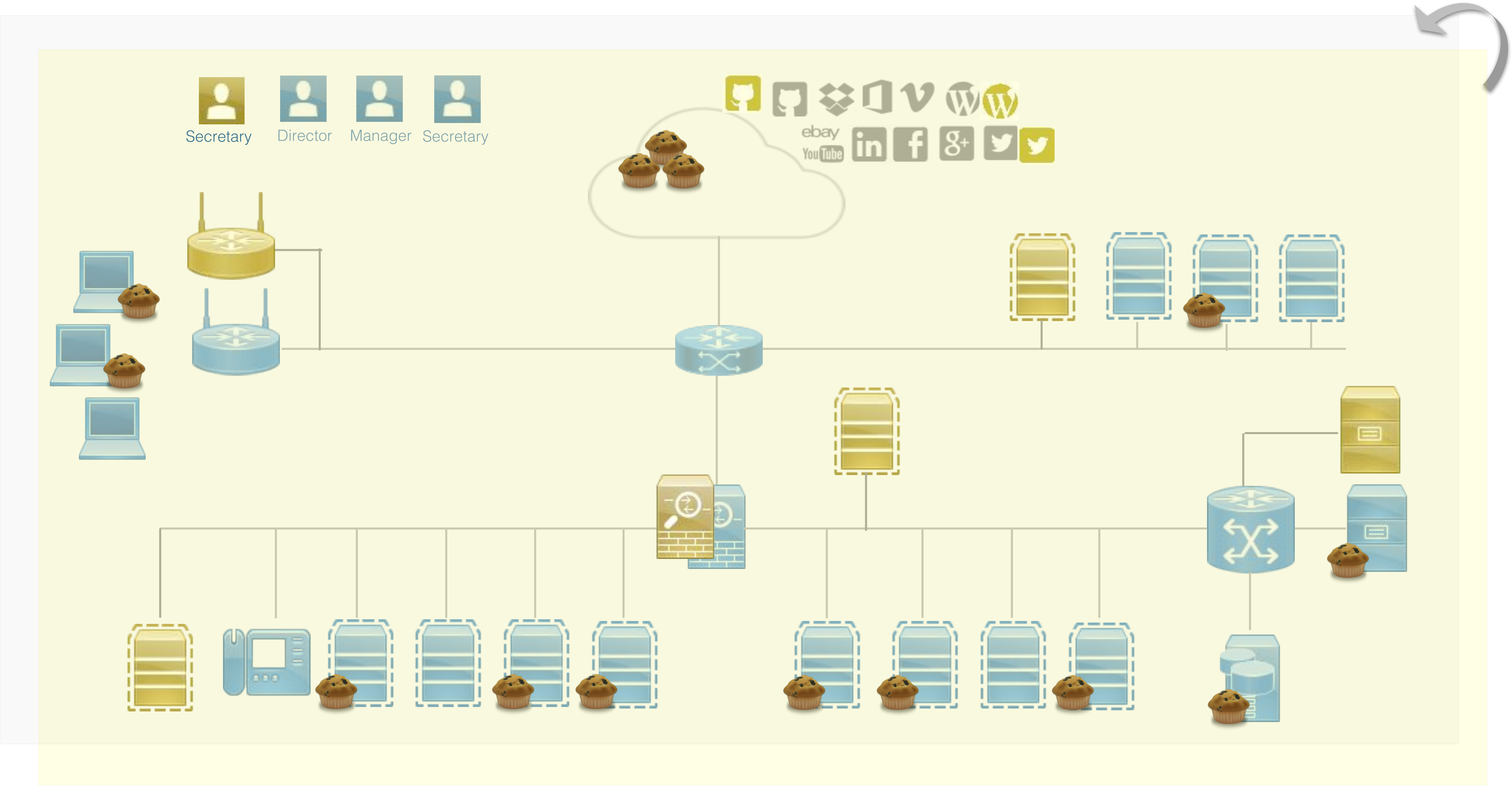


Sources:

- Cognitive Active Cyber Defense: Finding Value Through Hacking Human Nature (Peter Cooper)

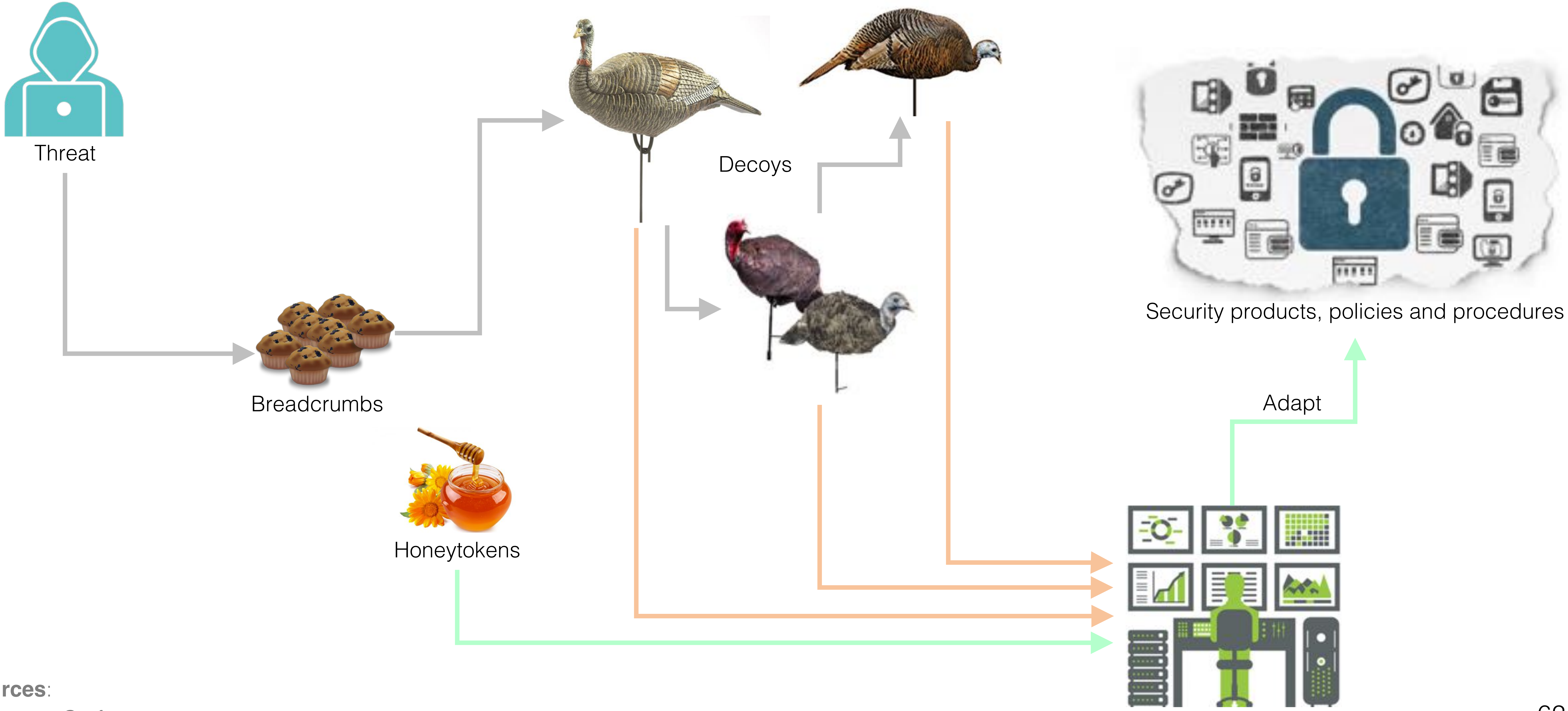
Cybersecurity Deception Operations

Stereoscopic 3D



Cybersecurity Deception Operations

Plan and integrate deception



Sources:
- CounterCraft

Threat Hunting

Pros & Cons

	Deception
Advantages	• No requirement for signatures • You are detecting effects of the adversary; that has nothing to do with their tools, techniques, or exploits. • Zero false positives
Disadvantages	• Infrastructure requirement to replicate critical services • Effectiveness is very difficult, if not impossible, to measure.

6. Conclusions

Conclusions

To sum up…

- Being one step ahead of hackers is at least challenging
  - Establish a trusted relationship with inside / outside SOCs, CERTs, IRTs, NOCs…
  - Manage your team’s “burn-out syndrome”. Engage Your Team Daily
  - From good to better

- Provide “Value”. Turn weaknesses into business opportunities
- Tips: Common Sense && Experience && Solid Management Strategies
- Visibility is the key

Conclusions

To sum up…

- Be proactive – don’t wait for someone else to notify you of a compromise
- Evolve – Create new dynamics – Use new approaches
- Promote a Hunting Mindset

- Hunting, in order to scale, must document and automate “normal” for the benefit of the entire organization
- Hunting output must be “formatted” into a consumable capability for daily operations

- Make it ”expensive” for adversaries to attack you
- Threat Hunting as a Service

Eskerrik asko!

Thank you!

EUSKALHACK