SPECTEROPS

TALK

Rethinking Detection Engineering: **False Positives are Bad, False Negatives are Worse**

Jared Atkinson

November 20 10:00 - 11:00

SO-CON 2020

Binary Classification

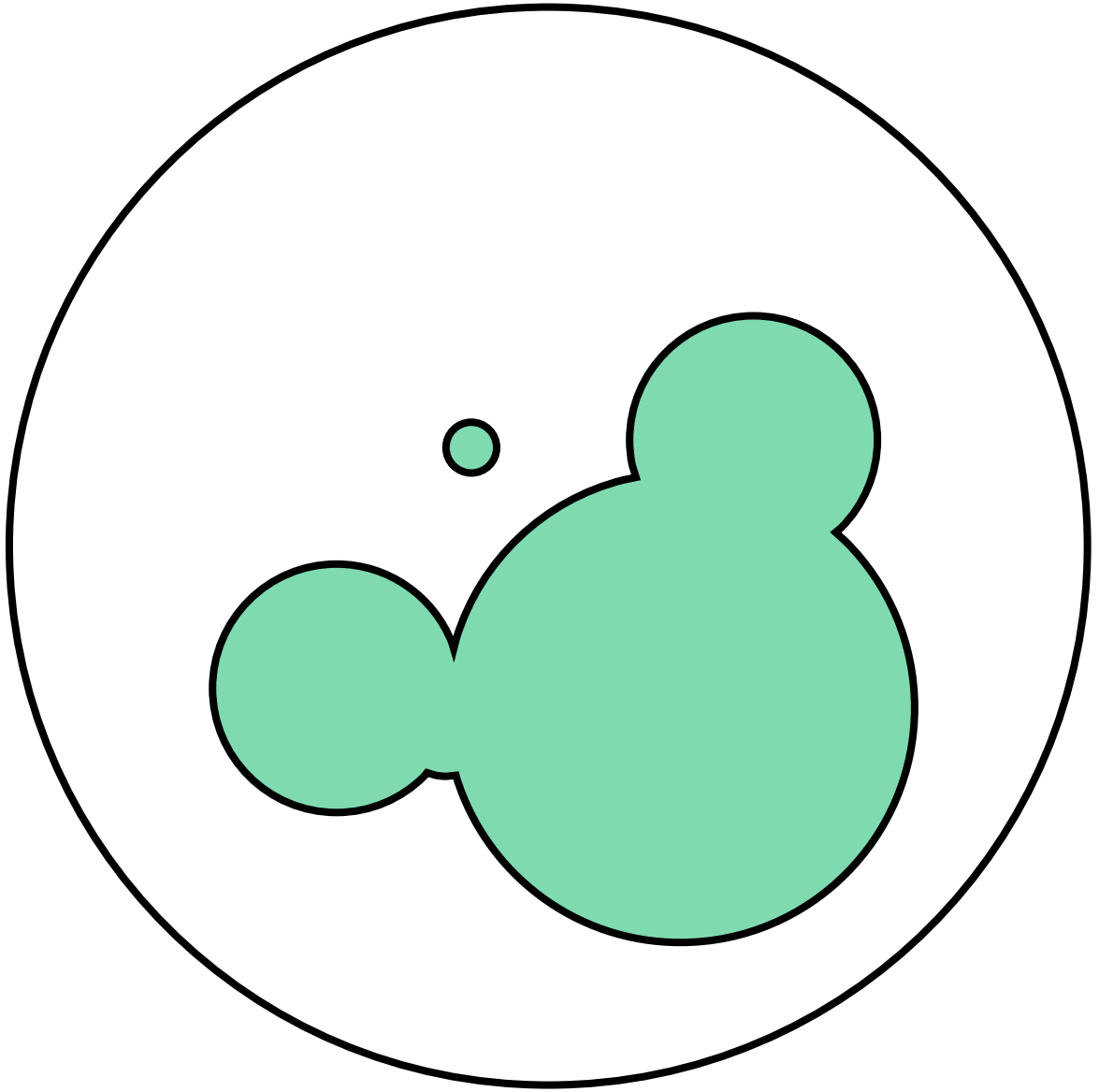
Binary classification is the task of classifying the elements of a set into two groups (positive or negative) on the basis of a classification rule. This is typically done with imperfect knowledge of the true state of the element which is why the result is considered a “prediction”.

Population

- A set of similar items or events which is of interest for some question or experiment.
- Example
  - All people tested for a disease
  - All telemetry collected from enterprise assets

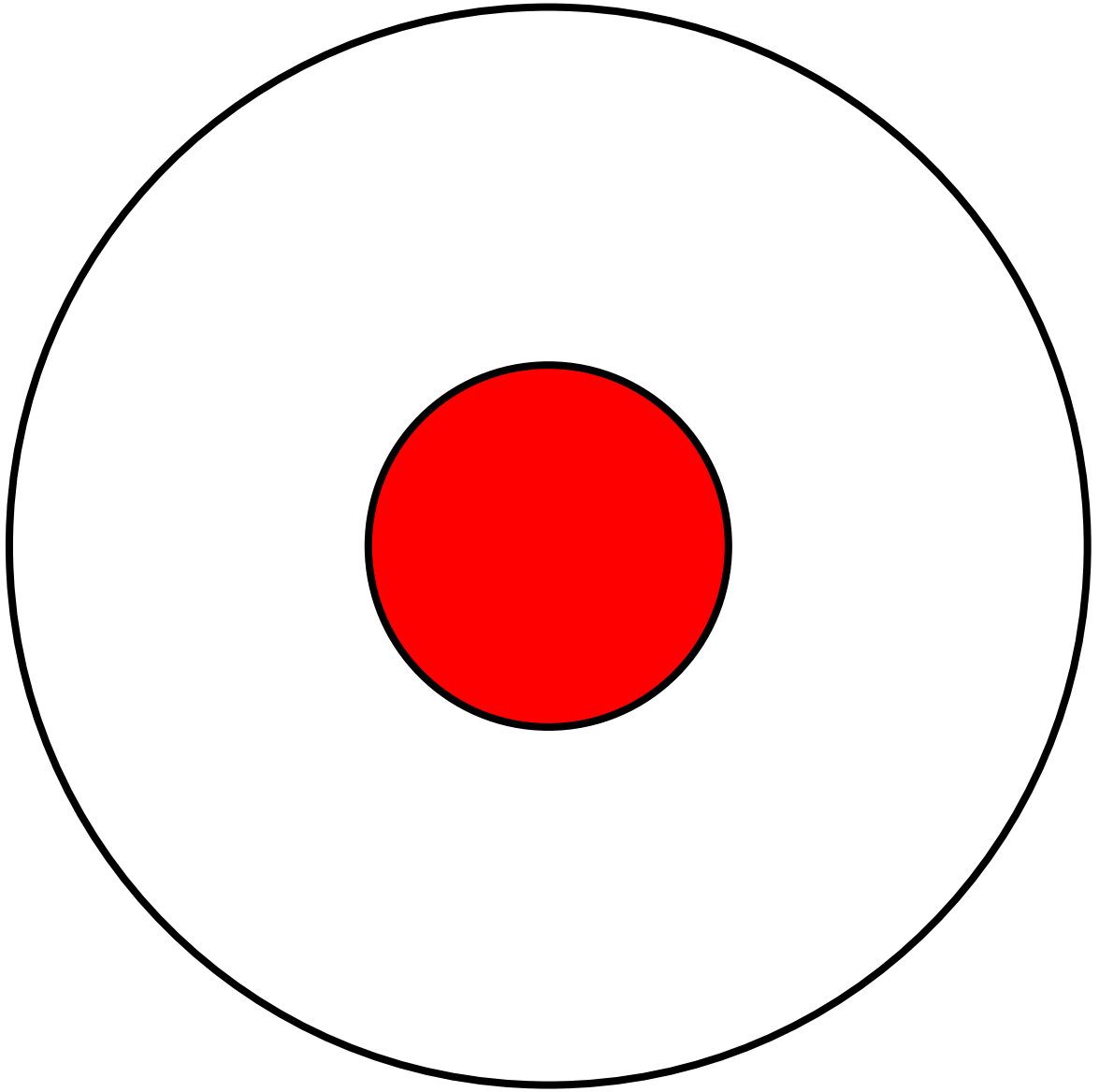
Classification Rule

- A procedure by which the elements of the population are each predicted to belong to one of the classes
  - In Binary Classification there are only two classes (positive and negative)
- Examples
  - People who test positive for the disease
  - Events that are classified as malicious services



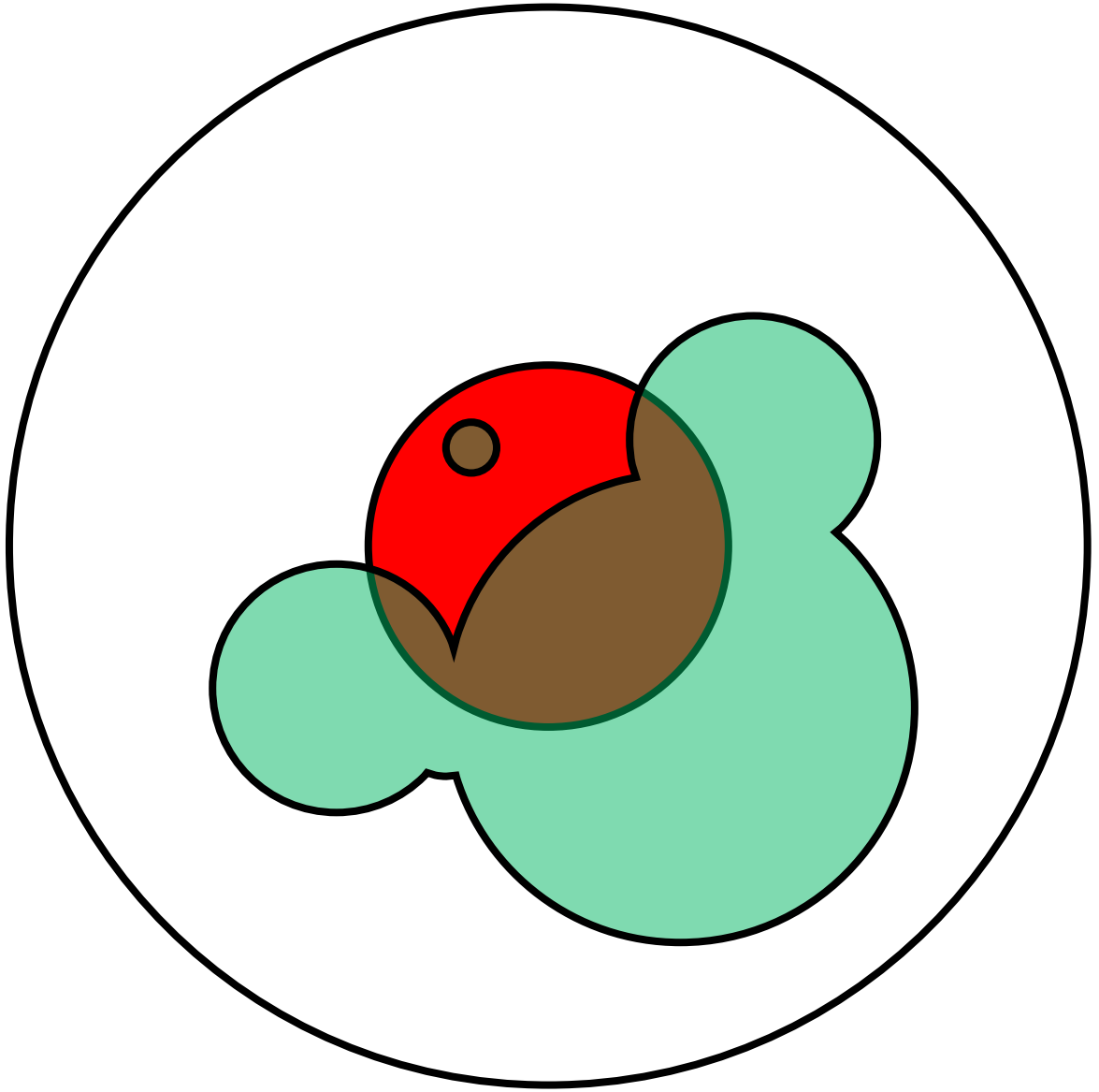
Condition Positive

- Represents the real number of positive events in the collected data
- Examples
  - The objective sub population of sick people (positive for disease)
  - The objective sub population of malicious events



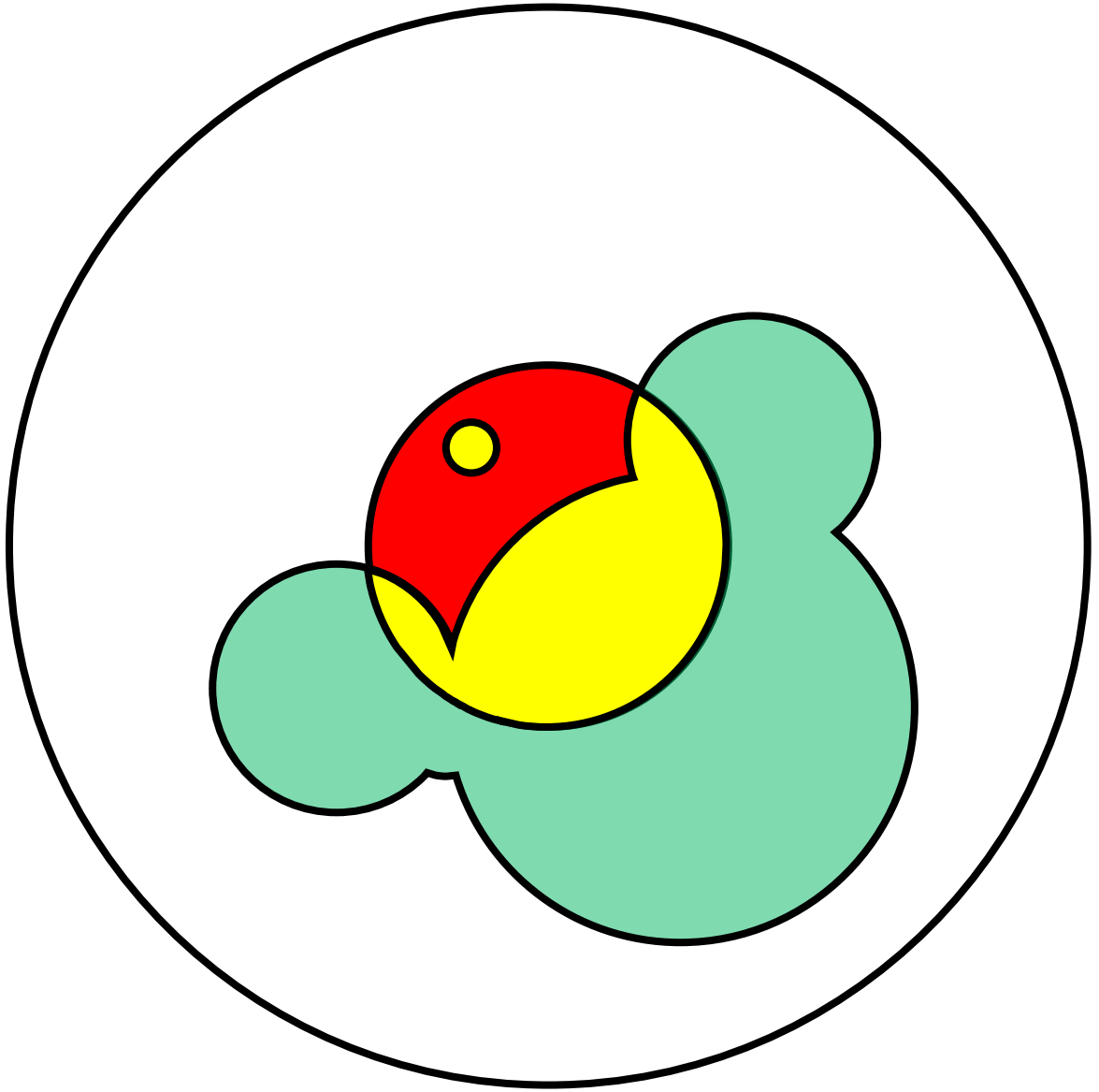
Condition Positive

- Represents the real number of positive events in the collected data
- Examples
  - The objective sub population of sick people (positive for disease)
  - The objective sub population of malicious events
- Two possible predictions:
  - True Positive
  - False Negative



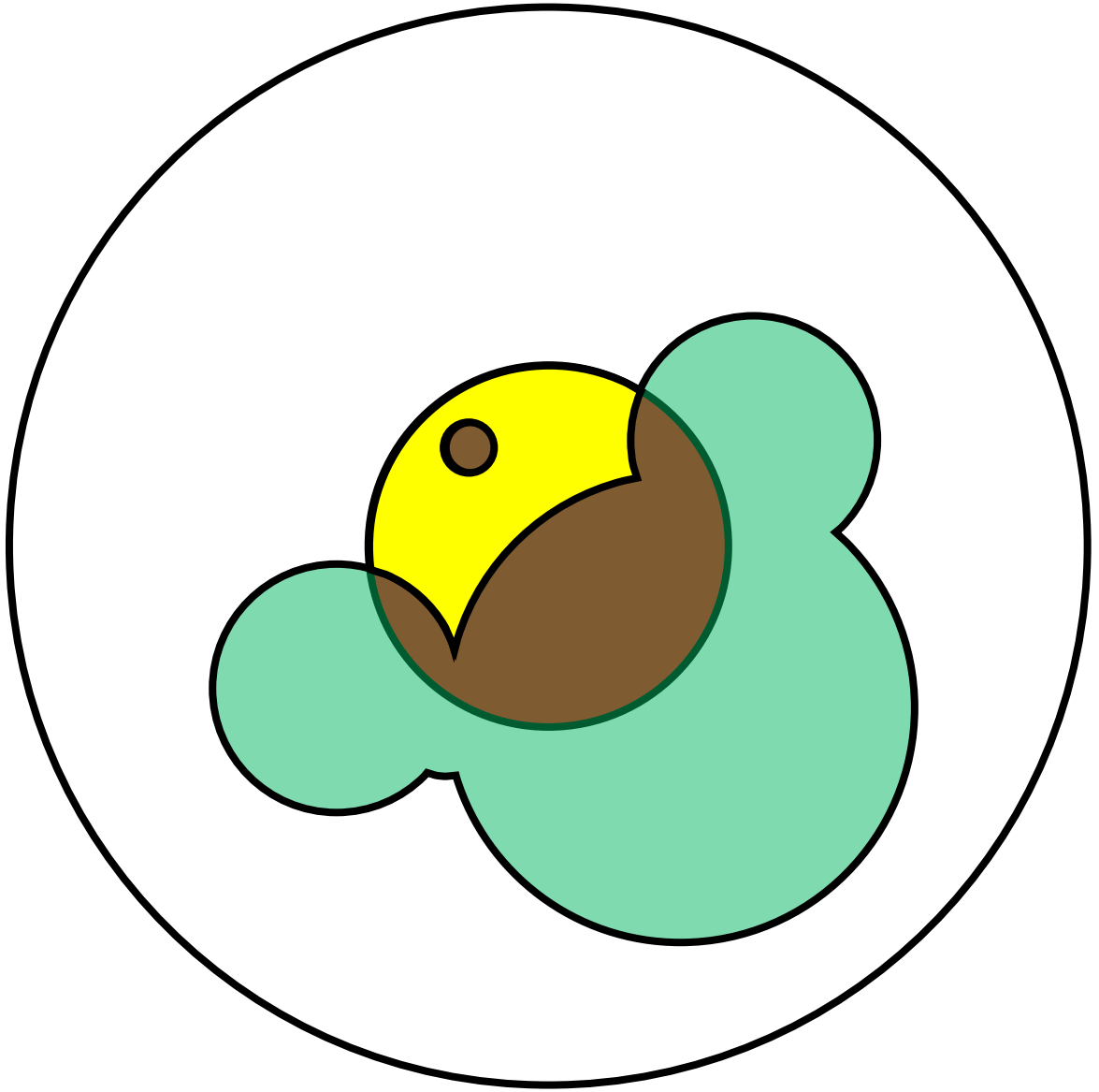
True Positives (TP)

- Positive events that are classified as positive
- Examples
  - Sick people correctly identified as sick
  - Malicious services correctly identified as malicious



False Negatives (FN)

- Positive events that are classified as negative
- Examples
  - Sick people incorrectly identified as healthy
  - Malicious services incorrectly identified as benign
- Problem
  - False Negatives fail silently
  - Risk is implicitly assumed



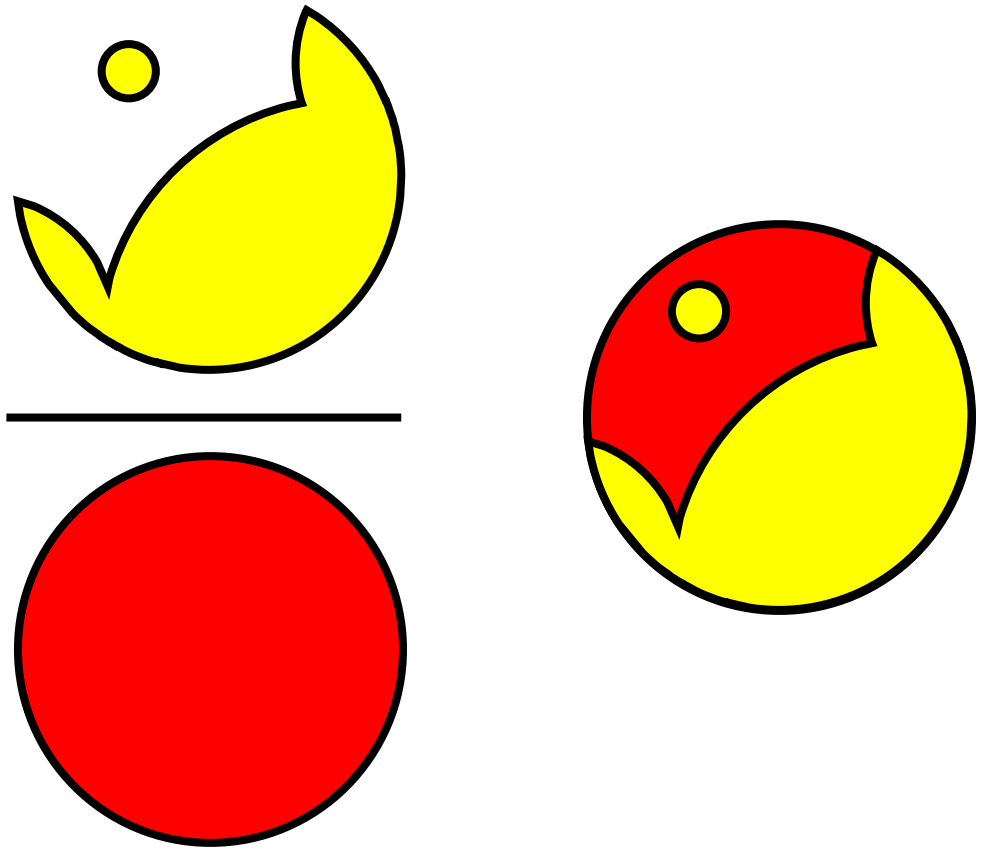
Sensitivity

- Measures the ability of the test to correctly detect events that meet the condition
- How likely are you to identify sick people as being sick?

$$\text{sensitivity} = \frac{\text{number of true positives}}{\text{number of true positives} + \text{number of false negatives}}$$

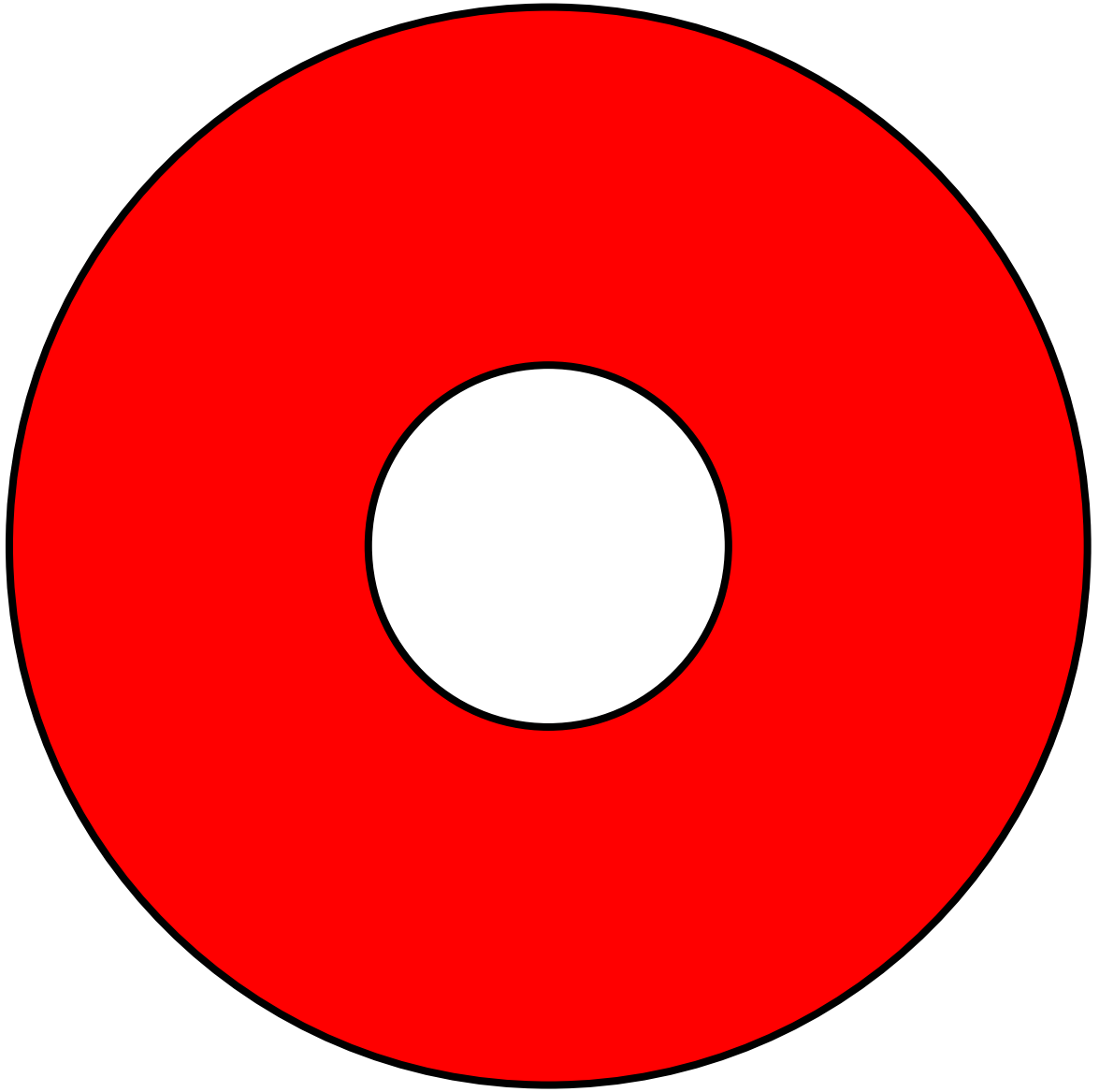
$$= \frac{\text{number of true positives}}{\text{total number of sick individuals in population}}$$

$$= \text{probability of a positive test given that the patient has the disease}$$



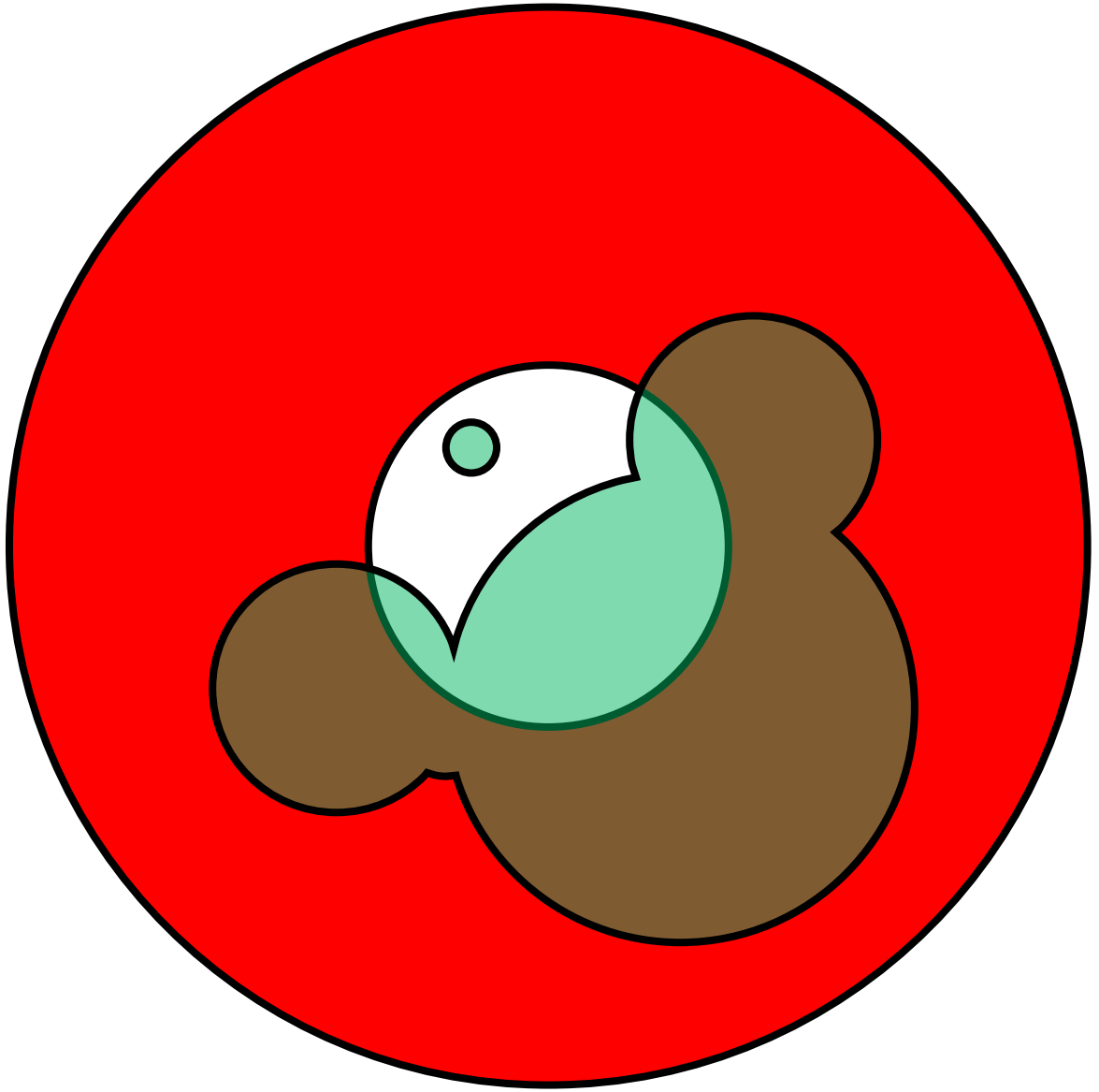
Condition Negative

- Represents the real number of negative events in the collected data.
- Examples
  - The objective sub population of healthy people (negative for disease)
  - The objective sub population of benign events



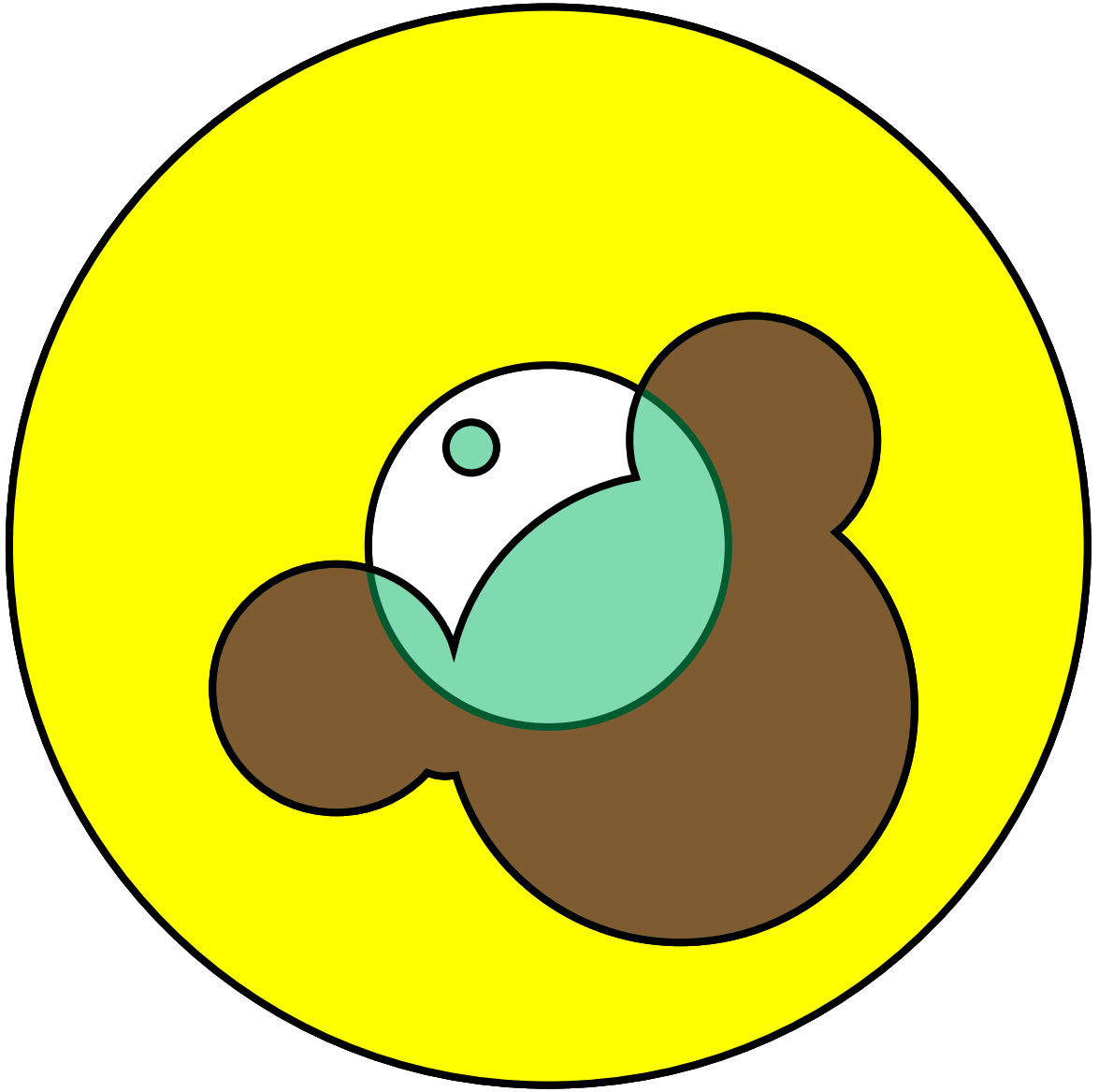
Condition Negative

- Represents the real number of negative events in the collected data.
- Examples
  - The objective sub population of healthy people (negative for disease)
  - The objective sub population of benign events
- Two possible predictions:
  - True Negative
  - False Positive



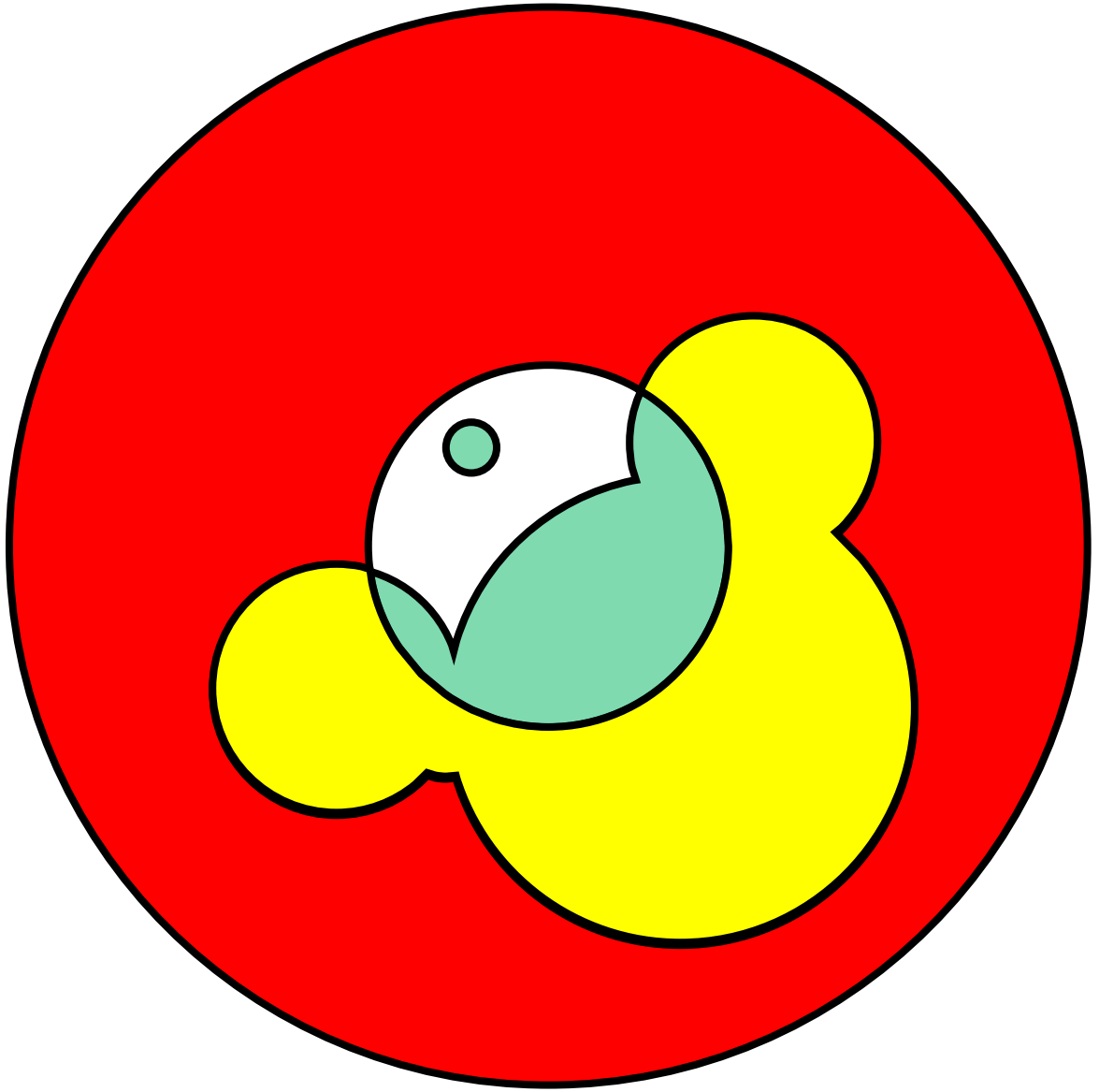
True Negatives (TN)

- Negative events that are classified as negative
- Examples
  - A healthy person correctly identified as healthy
  - A benign service correctly identified as benign



False Positives (FP)

- Negative events that are classified as positive
- Examples
  - Healthy people incorrectly identified as sick
  - Benign services incorrectly identified as malicious
- Problem
  - False Positives fail noisily
  - Triage and Investigation resources may be diverted from actual malicious activity



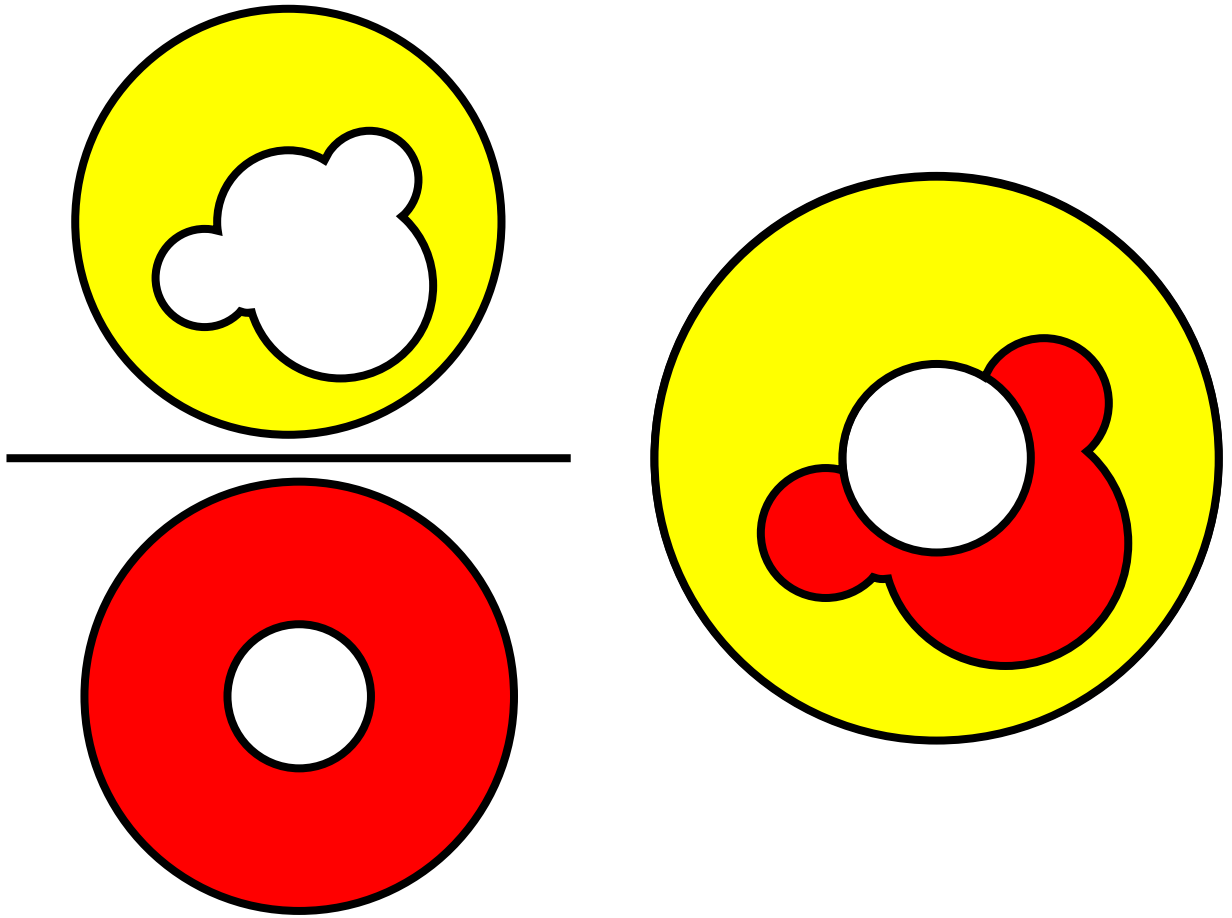
Specificity

- Measures the ability of the test to correctly reject events that do not meet the condition
- How likely are you to identify healthy people as being healthy?

$$\text{specificity} = \frac{\text{number of true negatives}}{\text{number of true negatives} + \text{number of false positives}}$$

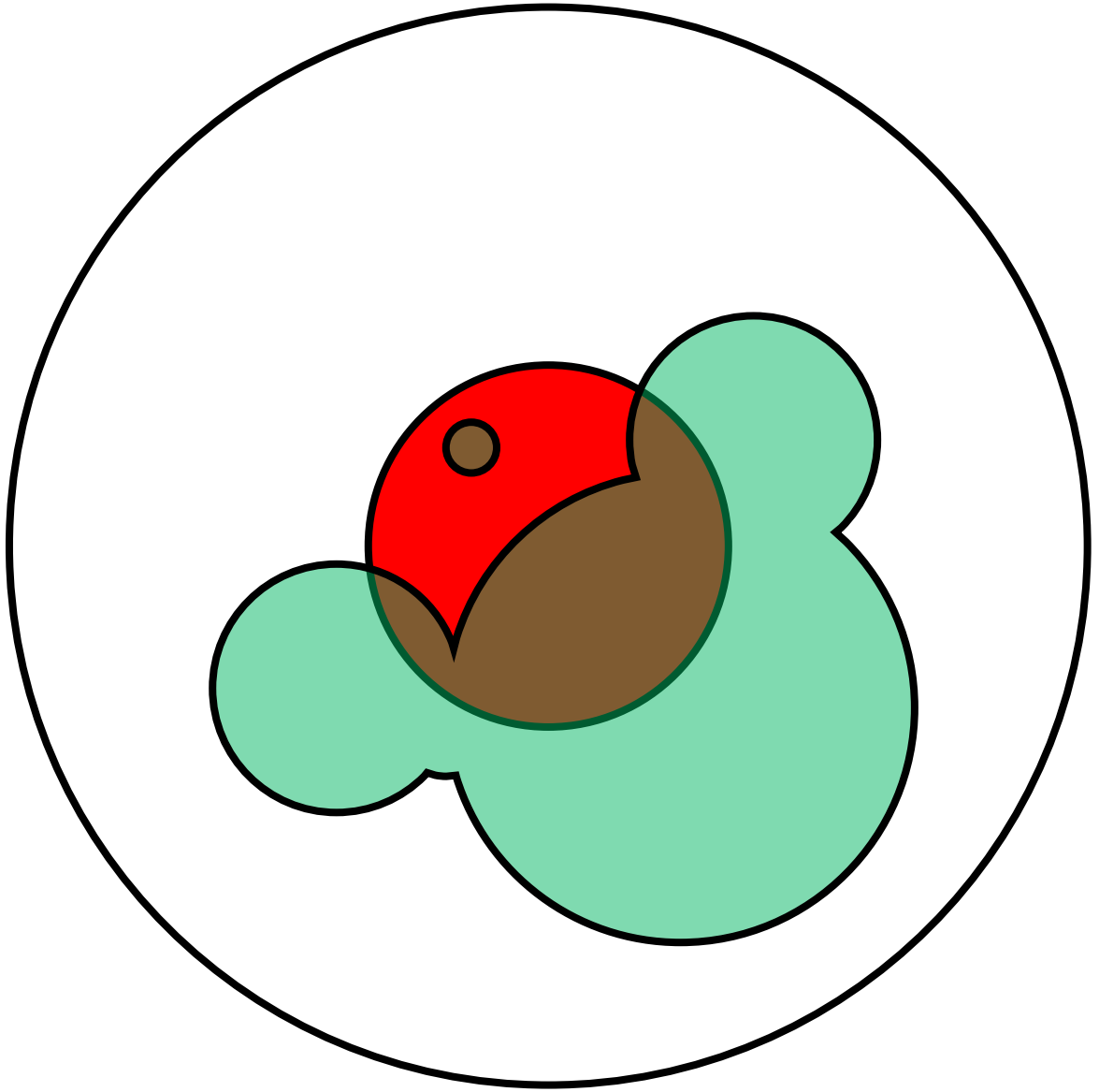
$$= \frac{\text{number of true negatives}}{\text{total number of well individuals in population}}$$

$$= \text{probability of a negative test given that the patient is well}$$



FP Reduction Problem

- False Positives are tangible while Fales Negatives are invisible
- Triage and Investigation resources are “wasted” on FPs
- **Problem** – Analysts often work to reduce FPs (specificity) without considering the effect on FNs (sensitivity)



Common Detection Routine

For this example, we will discuss a layered detection in the context of addressing the Service Creation attack technique. This technique can be used by attackers to achieve persistence, privilege escalation, and/or lateral movement.

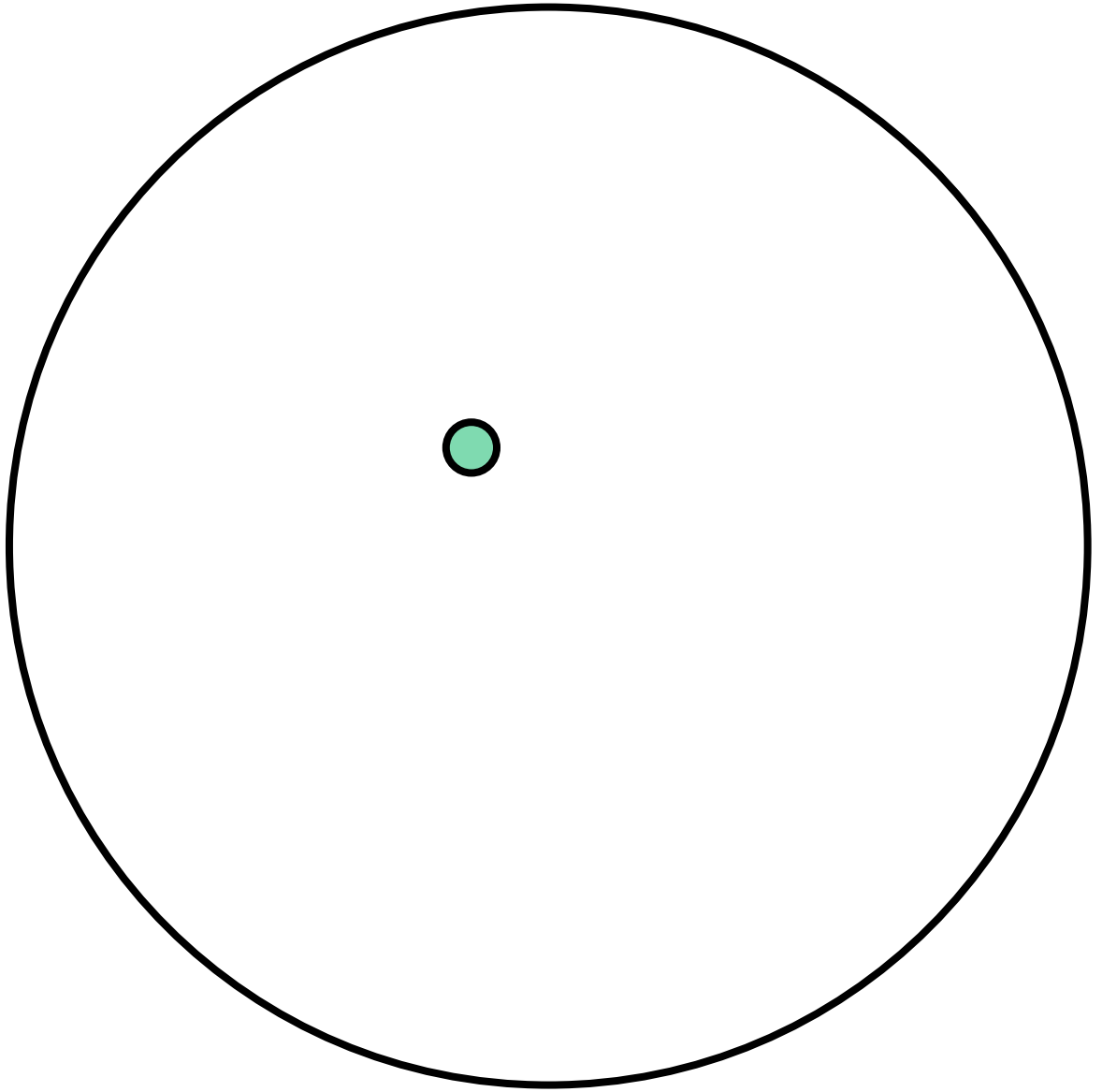
Telemetry

- Telemetry provides analysts with perspective/context of activity that is occurring within the environment.
- Constrained resources forces analysts to find ways to identify telemetry that is more likely to be security relevant (Detection).

Precise Detection

- High Specificity (Low FP/High FN)
- Reduces detection, triage, and investigation burden
- Increases potential risk from FNs

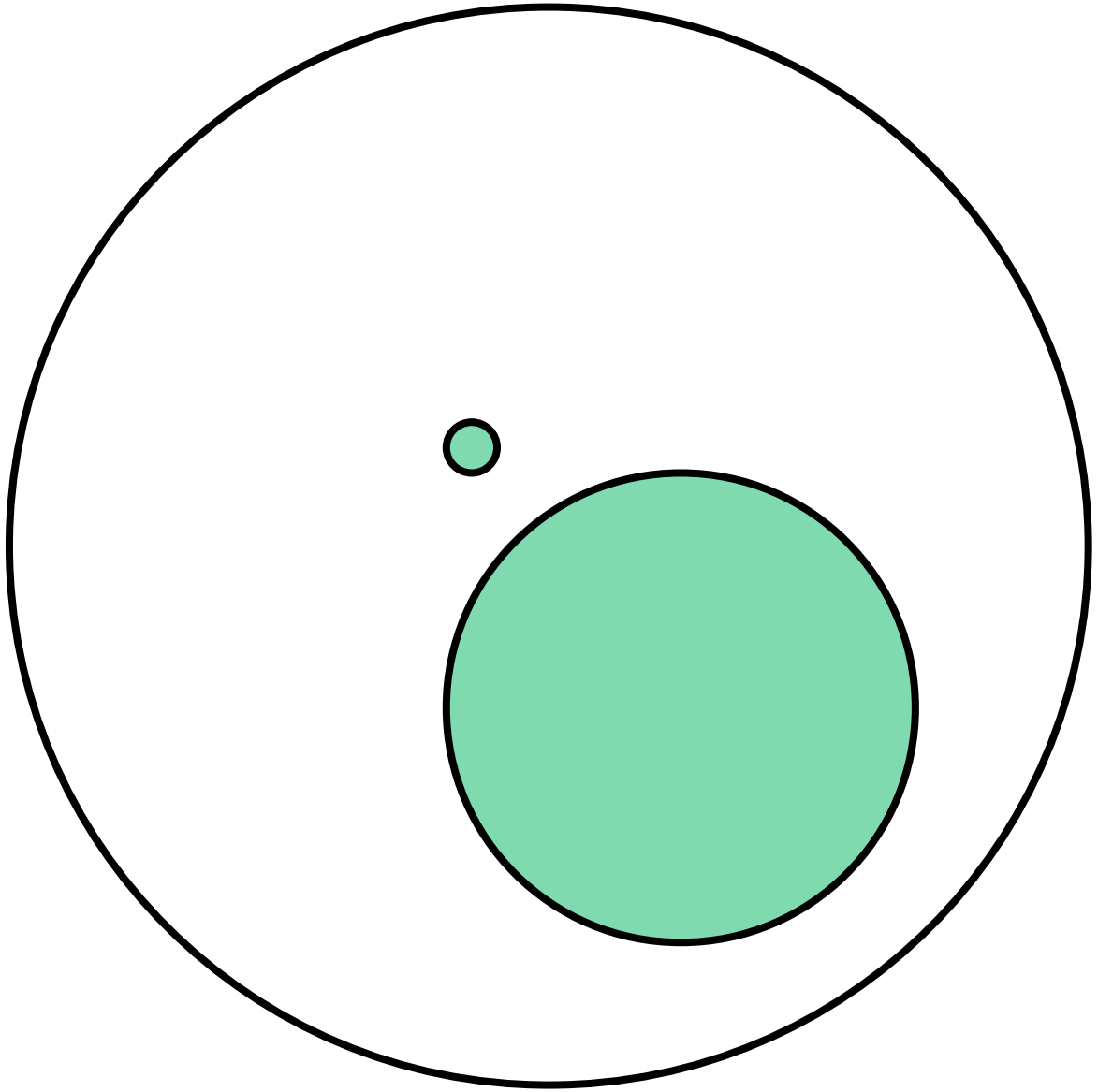
- Alert on services with a specific display name (MalSvc).
- All alerts generated via this detection are likely to be malicious.



Broad Detection

- High Sensitivity (High FP/Low FN)
- Reduces potential risk of FNs
- Increases the burden of detection, triage, and investigation

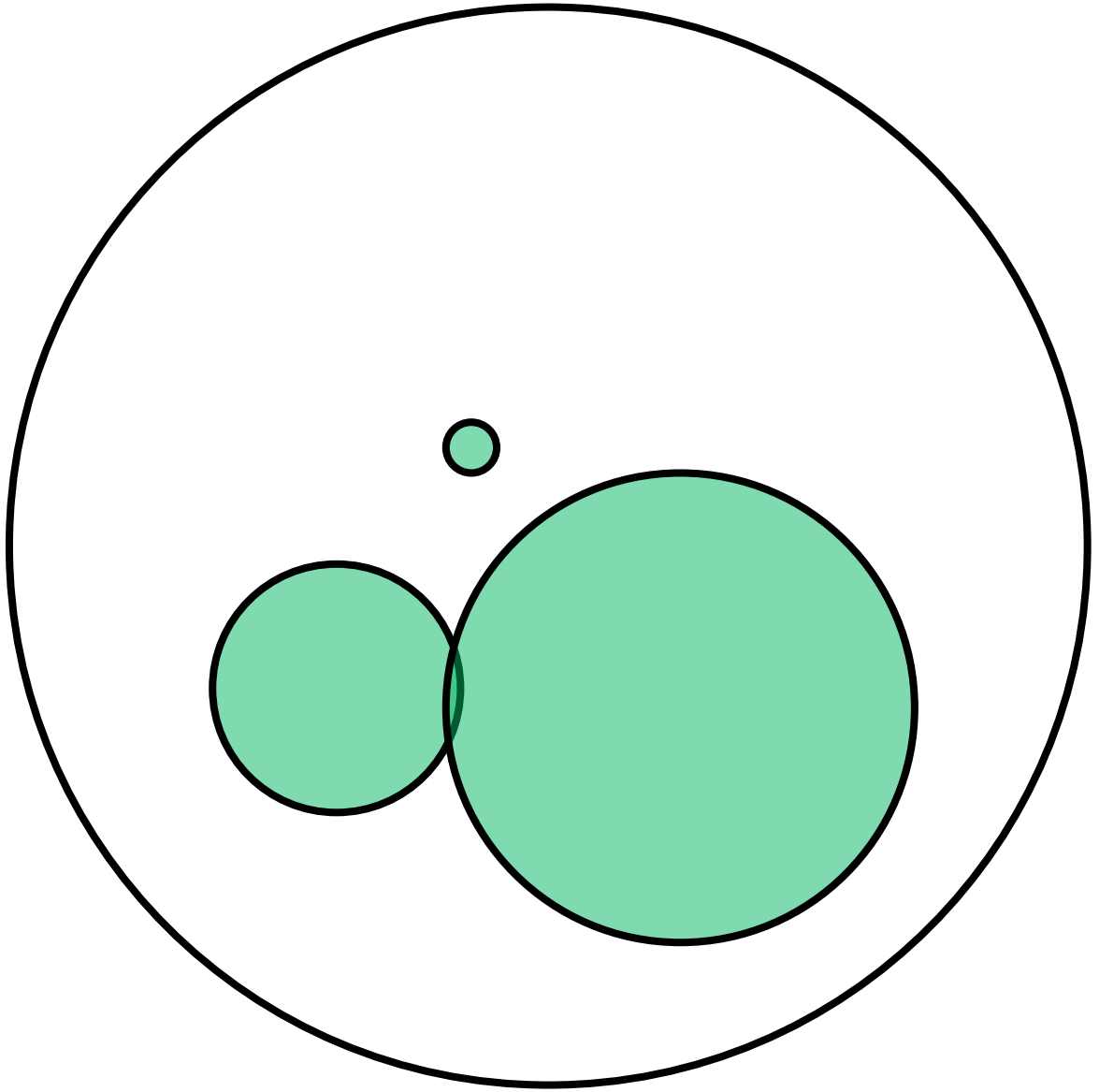
- Alert on services that are set to auto start on system boot up.
- This may be indicative of a service being created to establish persistence.



Inference

- Inductive Inference
  - Identify a feature that malicious events share and assume that is common among all malicious events.
- Deductive Inference
  - The process of reasoning from one or more statements (premises) to reach a logical conclusion.

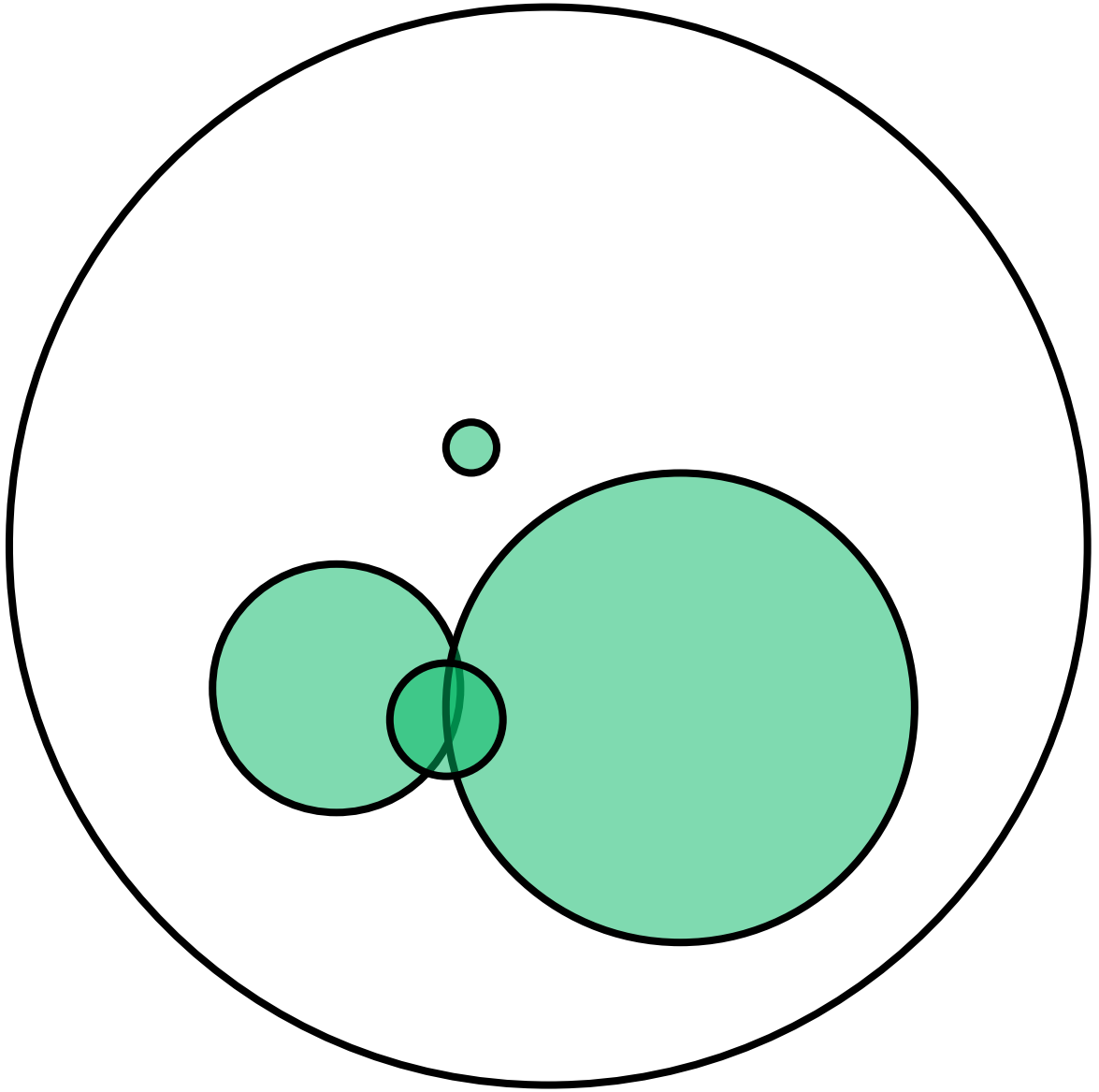
- Alert on services that were created by a process on a remote system.
- This may be representative of lateral movement.



Univariate Detections

- Rely on a single variable for detection.
- New detections do not inherently increase overall coverage.

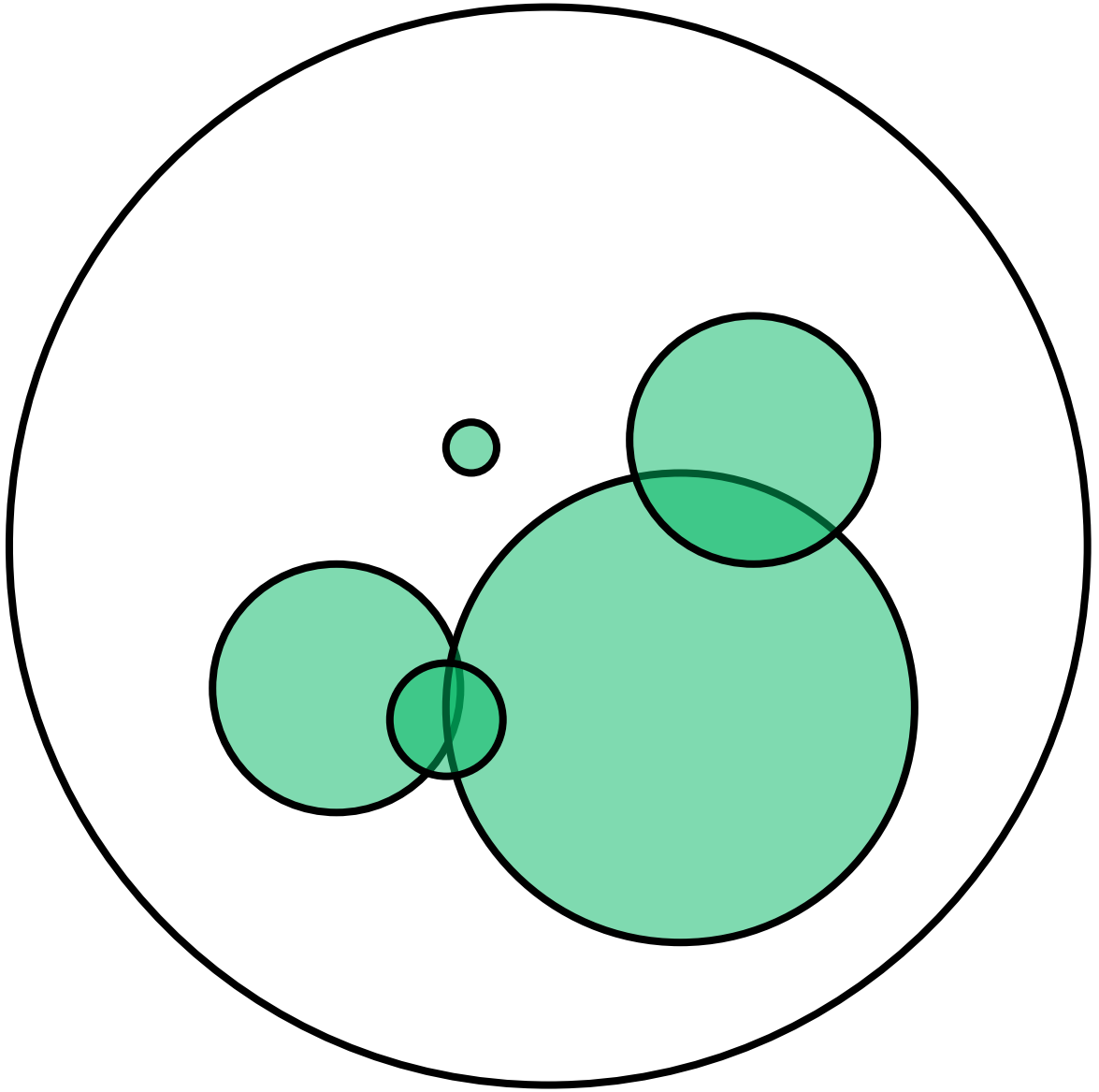
- Alert on services where the registry key was not created by services.exe (the SCM RPC server).
- This may represent service creation outside of the supported API.



Layered Detections

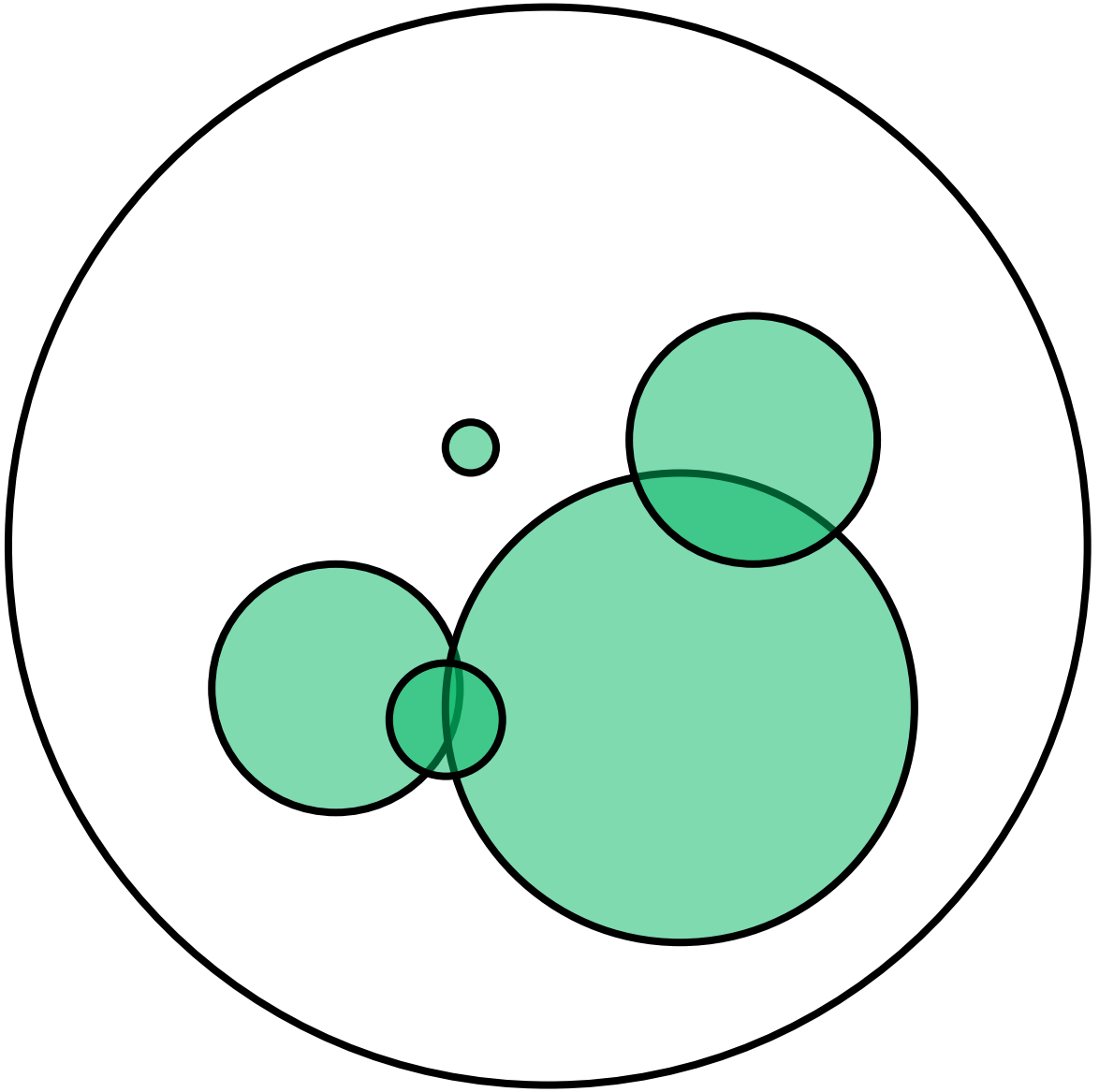
- Add additional detections that balance specificity and sensitivity to build a comprehensive approach.

- Alert on services that execute unsigned binaries.
- This may represent a service that is not part of an approved enterprise application.



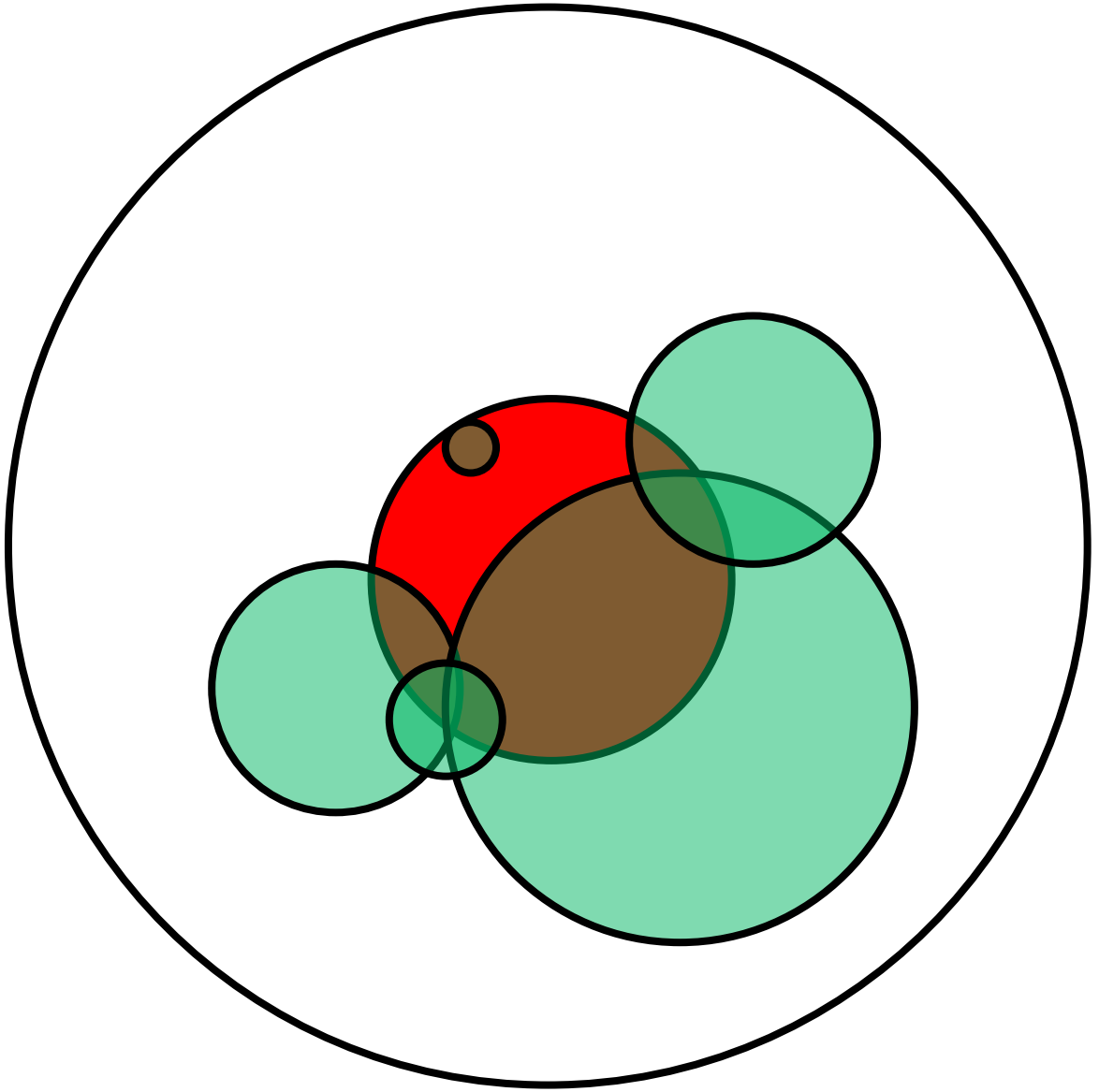
Uncertainty

- A state of limited knowledge where it is impossible to exactly describe the existing state, a future outcome, or more than one possible outcome.
- Analysts often don’t review events that were not the subject of an alert/alarm.



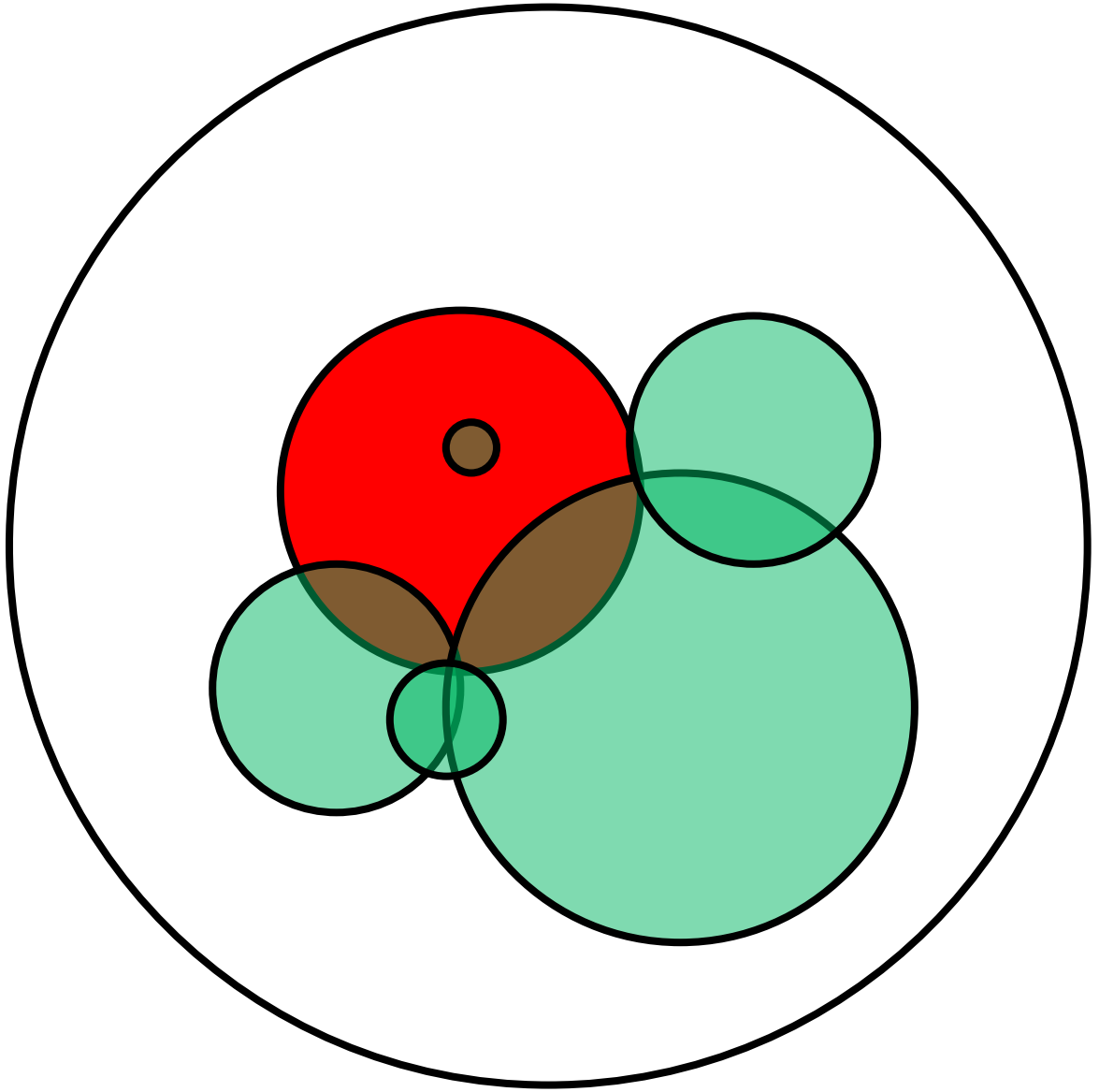
Uncertainty

- A state of limited knowledge where it is impossible to exactly describe the existing state, a future outcome, or more than one possible outcome.
- Analysts often don’t review events that were not the subject of an alert/alarm.



Uncertainty

- A state of limited knowledge where it is impossible to exactly describe the existing state, a future outcome, or more than one possible outcome.
- Analysts often don’t review events that were not the subject of an alert/alarm.



Jean Piaget

Swiss psychologist best known for his theory of cognitive development in children.

Stages of Cognitive Development

- Sensorimotor Stage
  - Children explore the world through movement and their senses
- Preoperational Stage
  - Children play and manipulate symbols while also becoming interested in why things work the way they do
- Concrete Operational Stage
  - Children can think logically, but are limited to what they can physically manipulate
- Formal Operational Stage
  - Children develop abstract thought and can think logically in their mind

Applying Piaget's Theory of Cognitive Development to Mathematics Instruction
https://files.eric.ed.gov/fulltext/EJ841568.pdf

Abstract Concept:
Clean Your Room

Formal Operational - Reasoning Skills

- Clarification
  - Identification and Analysis of the element of the problem to identify the information that is necessary to solve the problem
- Inference
  - Deductive Inference – Reasoning from general concepts to specific instances
  - Inductive Inference – Extract similarities and difference between specific objects to arrive at generalizations
- Evaluation
  - Using criteria to judge the adequacy of a problem solution which leads to forming a hypothesis about future events
- Application
  - Involves connecting concepts to real-life situations

Applying Piaget's Theory of Cognitive Development to Mathematics Instruction
https://files.eric.ed.gov/fulltext/EJ841568.pdf

Building a Solution

Dr. Anton Chuvakin
On Threat Detection Uncertainty

- Improve Alert Triage
  - Improve the efficiency of decision making or outsource to a 3rd party
- Use Multi-Stage Detections
  - Produce a noisy signal that has automation to gather additional context and help increase certainty
- Split Bad From Interesting
  - Differentiate precise/brittle signal and noisy signal into separate processes requiring different levels of resources

https://medium.com/anton-on-security/on-threat-detection-uncertainty-7eac9b22adb6

Detection Process

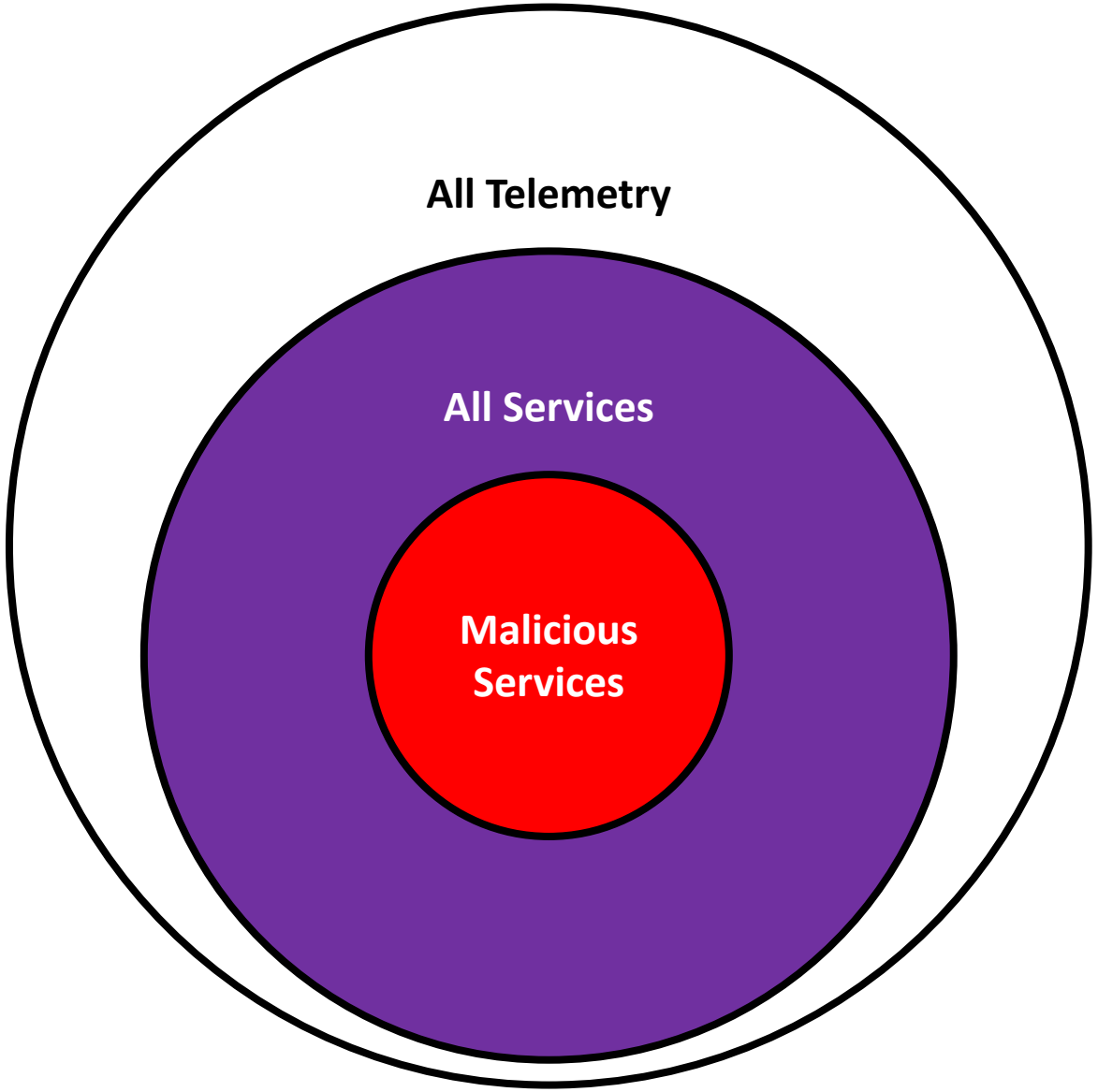
1. Identify Base Condition
2. Capture Base Instances
3. Identify Contextual Factors
4. Add Necessary Context
5. Evaluate Multivariate Detection
6. Tune

Identify Base Condition

Determine the condition that must be fulfilled by all positive events. Is it possible to identify something that every malicious service must have in common? This allows for filtered population (relative to all collected events) but minimizes the likelihood of false negatives (at this point).

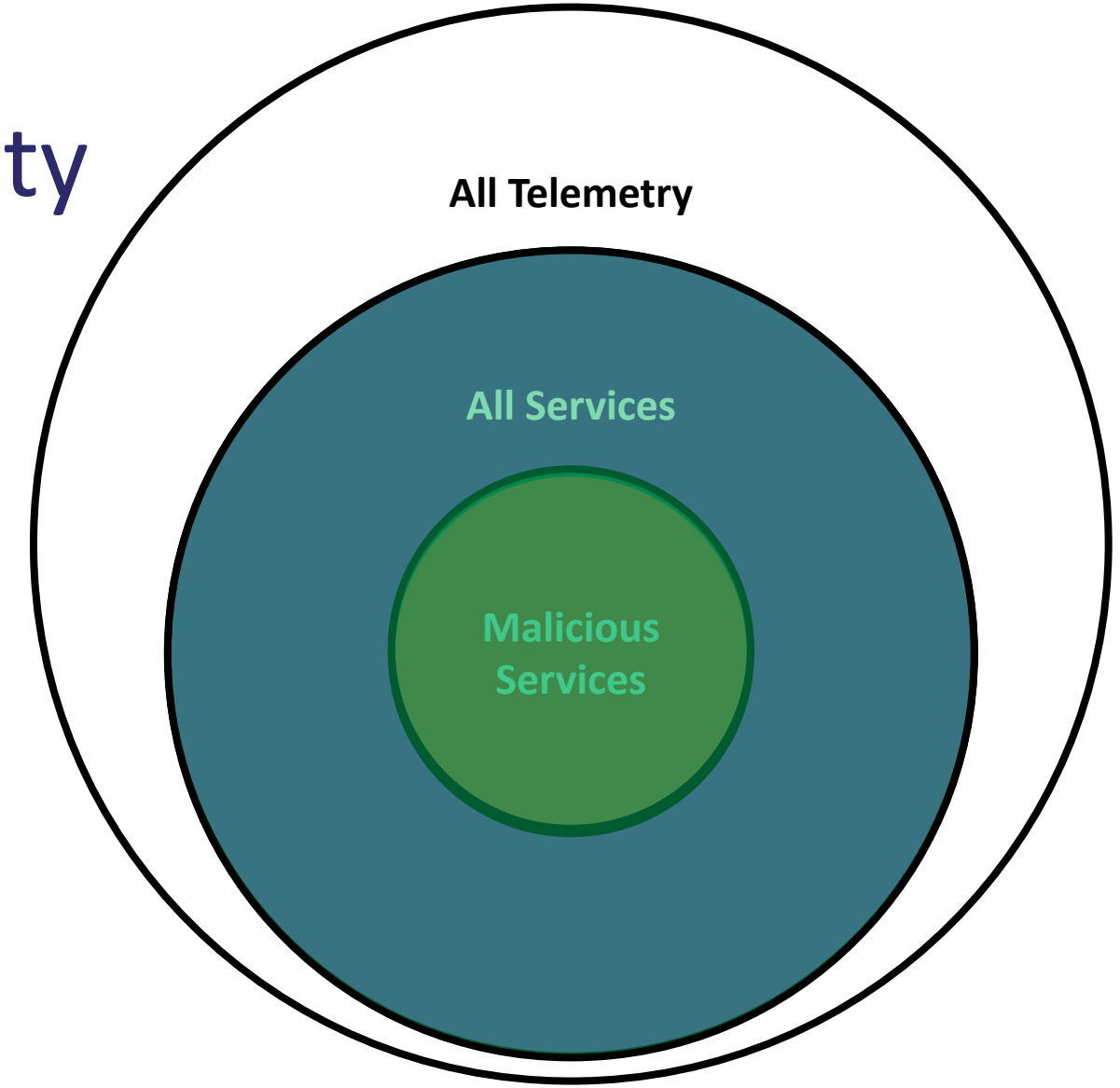
Telemetry Hierarchy

- All Telemetry – represents the collection of all events collected from the enterprise as a means of understanding the activity occurring within
- All Services – represents the collection of all services (malicious or benign) that are installed on monitored assets in the enterprise
- Malicious Services – represents the collection of services that are installed by threat actors for nefarious purposes



Start with High Sensitivity

- Uses the multi-stage detection approach
- All malicious services (subset) must also be services (superset)
- Detection service creation is the “base condition” for detecting malicious service creation
- Accounts for the uncertainty of the positive condition



Capture Base Instances

Identify a specific event the indicates the base condition. Is this event currently captured, and if so, what is the best way to capture it? This capture should include all true condition events, but because specificity is low it will include many false positives.

Services are Stored in the Registry

Database of Installed Services

05/31/2018 • 2 minutes to read •

The SCM maintains a database of installed services in the registry. The database is used by the SCM and programs that add, modify, or configure services. The following is the registry key for this database: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**.

This key contains a subkey for each installed service and driver service. The name of the subkey is the name of the service, as specified by the CreateService function when the service was installed by a service configuration program.

An initial copy of the database is created when the system is installed. The database contains entries for the device drivers required during system boot. The database includes the following information about each installed service and driver service:

https://docs.microsoft.com/en-us/windows/win32/services/database-of-installed-services

Considerations for Selecting a Base Event

- Initial Contextual Details
  - Security 4697
    - Name, File Name, Service Type, Start Type
  - Sysmon 12
    - Name and Registration Process
- Capture Mechanism
  - Security 4769 (SCM API)
  - Sysmon 12 (Registry Key Creation)

Windows Security Event ID 4697
SecurityId : *S-1-5-21-2705517210-3166577-436293457-500*
AccountName : *ladmin*
AccountDomain : *bennett1*
LogonId : *0x43FB79*
ServiceName : *TYLIUHEYAWUNSMCLWIES*
ServiceFileName : *%COMSPEC% /C "%COMSPEC% /C start /b powershell -noP -sta -w 1 -enc SQB...FgA*
ServiceType : *0x10*
ServiceStartType : *3*
ServiceAccount : *LocalSystem*

Sysmon Event ID 12
EventType : *CreateKey*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWIES*

Sysmon Event ID 12
EventType : *CreateKey*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES*

Rethinking Detection Engineering:

False Positives are Bad, False Negatives are Worse

Jared Atkinson

SO-CON 2020

Sysmon Event ID 12
EventType : *CreateKey*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES*

Composite
Name : *TYLIUHEYAWUNSMCLWTES*
RegistrationProcessImagePath : *C:\windows\system32\services.exe*

Rethinking Detection Engineering:

False Positives are Bad, False Negatives are Worse

Jared Atkinson

SO-CON 2020

Identify Contextual Factors

In many case, the base event provides limited context. Does additional context exist, and if so, how can it be collected/correlated? For instance, a service name is likely not sufficient context to determine if the service is malicious.

Service Configuration API

Service Configuration

05/31/2018 • 2 minutes to read •

The system uses the configuration information to determine how to start the service. The configuration information also includes the service display name and its description. For example, for the DHCP service, you could use the display name "Dynamic Host Configuration Protocol Service" and the description "Provides internet addresses for computer on your network."

To modify the configuration information for a service object, a configuration program uses the **ChangeServiceConfig** or **ChangeServiceConfig2** function. For an example, see Changing a Service Configuration.

To retrieve the configuration information for a service object, the configuration program uses the **QueryServiceConfig** or **QueryServiceConfig2** function. For an example, see Querying a Service's Configuration.

The **ChangeServiceConfig2** and **QueryServiceConfig2** service configuration functions support the use of triggers to control service start.

https://docs.microsoft.com/en-us/windows/win32/services/service-configuration

ChangeServiceConfigA function (winsvc.h)

12/05/2018 • 7 minutes to read

Changes the configuration parameters of a service.

To change the optional configuration parameters, use the ChangeServiceConfig2 function.

Syntax

C++ Copy

```
BOOL ChangeServiceConfigA(
  SC_HANDLE hService,
  DWORD     dwServiceType,
  DWORD     dwStartType,
  DWORD     dwErrorControl,
  LPCSTR    lpBinaryPathName,
  LPCSTR    lpLoadOrderGroup,
  LPDWORD   lpdwTagId,
  LPCSTR    lpDependencies,
  LPCSTR    lpServiceStartName,
  LPCSTR    lpPassword,
  LPCSTR    lpDisplayName
);
```

- Service Type
- Start Type
- Error Control
- Binary Path Name
- Load Order Group
- Tag Id
- Dependencies
- Service Start Name
- Password
- Display Name

https://docs.microsoft.com/en-us/windows/win32/api/winsvc/nf-winsvc-changeserviceconfiga

Add Necessary Context

Adding Initial Context

Sysmon12
EventType : *CreateKey*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES*

Start
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\Start*
Details : *DWORD (0x00000003)*

ImagePath
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\ImagePath*
Details : *%%COMSPEC%% /C "%%COMSPEC%% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell"*

Adding Initial Context

Sysmon12
EventType : *CreateKey*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES*

Start
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\Start*
Details : *DWORD (0x00000003)*

ImagePath
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\ImagePath*
Details : *%%COMSPEC%% /C "%%COMSPEC%% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell"*

Composite
Name : *TYLIUHEYAWUNSMCLWTES*
RegistrationProcessImagePath : *C:\windows\system32\services.exe*
StartType : *Manual (0x00000003)*
ImagePath : *%%COMSPEC%% /C "%%COMSPEC%% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell"*

Adding Remaining Context

Sysmon12
EventType : *CreateKey*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES*

DeleteFlag
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.923*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\DeleteFlag*
Details : *DWORD (0x00000001)*

ObjectName
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\ObjectName*
Details : *LocalSystem*

Start
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\Start*
Details : *DWORD (0x00000003)*

ImagePath
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\ImagePath*
Details : *%%COMSPEC%% /C "%%COMSPEC%% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell"*

Type
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\Type*
Details : *DWORD (0x00000010)*

ErrorControl
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTESrrorControl*
Details : *DWORD (0x00000000)*

DisplayName
EventType : *SetValue*
UtcTime : *2020-09-17 18:55:15.592*
ProcessGuid : *{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId : *624*
Image : *C:\windows\system32\services.exe*
TargetObject : *HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\DisplayName*
Details : *TYLIUHEYAWUNSMCLWTES*

Rethinking Detection Engineering:
False Positives are Bad, False Negatives are Worse
Jared Atkinson

SO-CON 2020

Adding Remaining Context

Composite	
Name	*TYLIUHEYAWUNSMCLWTES*
RegistrationProcessImagePath	*C:\windows\system32\services.exe*
StartType	*Manual (0x00000003)*
ImagePath	*%%COMSPEC%% /C "%%COMSPEC%% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell"*
ObjectName	*LocalSystem*
Type	*Win32OwnProcess (0x00000010)*
ErrorControl	*No Error (0x00000000)*
DisplayName	*TYLIUHEYAWUNSMCLWTES*
DeleteFlag	*Deleted (0x00000001)*

Sysmon12	
EventType	*CreateKey*
UtcTime	*2020-09-17 18:55:15.592*
ProcessGuid	*{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId	*624*
Image	*C:\windows\system32\services.exe*
TargetObject	*HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES*

DeleteFlag	
EventType	*SetValue*
UtcTime	*2020-09-17 18:55:15.923*
ProcessGuid	*{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId	*624*
Image	*C:\windows\system32\services.exe*
TargetObject	*HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\DeleteFlag*
Details	*DWORD (0x00000001)*

ObjectName	
EventType	*SetValue*
UtcTime	*2020-09-17 18:55:15.592*
ProcessGuid	*{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId	*624*
Image	*C:\windows\system32\services.exe*
TargetObject	*HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\ObjectName*
Details	*LocalSystem*

Start	
EventType	*SetValue*
UtcTime	*2020-09-17 18:55:15.592*
ProcessGuid	*{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId	*624*
Image	*C:\windows\system32\services.exe*
TargetObject	*HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\Start*
Details	*DWORD (0x00000003)*

ImagePath	
EventType	*SetValue*
UtcTime	*2020-09-17 18:55:15.592*
ProcessGuid	*{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId	*624*
Image	*C:\windows\system32\services.exe*
TargetObject	*HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\ImagePath*
Details	*%%COMSPEC%% /C "%%COMSPEC%% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell"*

Type	
EventType	*SetValue*
UtcTime	*2020-09-17 18:55:15.592*
ProcessGuid	*{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId	*624*
Image	*C:\windows\system32\services.exe*
TargetObject	*HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\Type*
Details	*DWORD (0x00000010)*

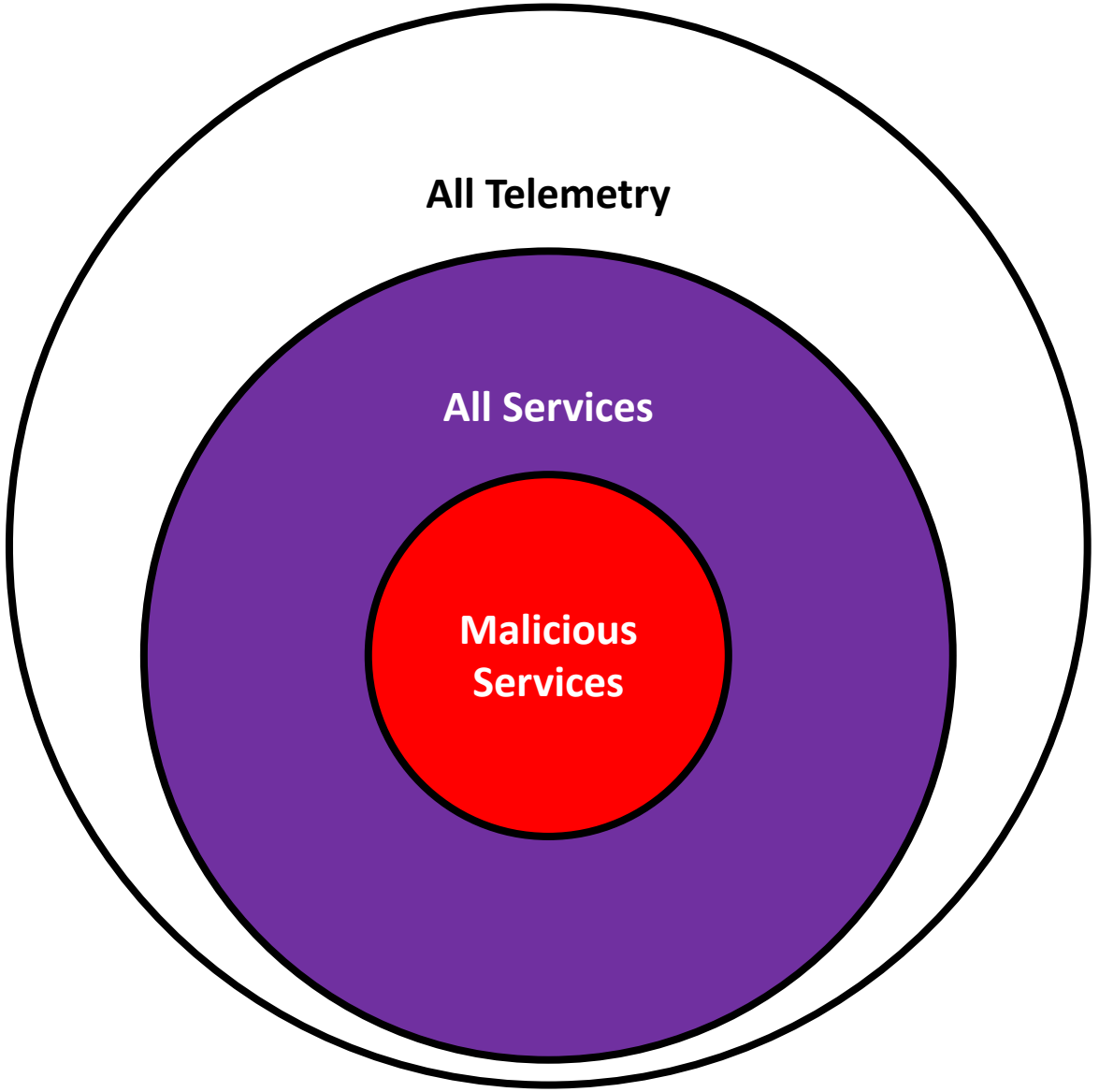
ErrorControl	
EventType	*SetValue*
UtcTime	*2020-09-17 18:55:15.592*
ProcessGuid	*{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId	*624*
Image	*C:\windows\system32\services.exe*
TargetObject	*HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTESrrorControl*
Details	*DWORD (0x00000000)*

DisplayName	
EventType	*SetValue*
UtcTime	*2020-09-17 18:55:15.592*
ProcessGuid	*{3D95CCDA-9158-5D41-0000-0010C1590000}*
ProcessId	*624*
Image	*C:\windows\system32\services.exe*
TargetObject	*HKLM\System\CurrentControlSet\Services\TYLIUHEYAWUNSMCLWTES\DisplayName*
Details	*TYLIUHEYAWUNSMCLWTES*

Evaluate Multivariate Detection

Threat Factors

- Registration Process
- Start Type (Auto)
- Service Type (Own Process)
- Service Name (Machine Generated)
- Service Binary
- Service Binary Path
- Remote Creation
- Requesting Process
- User



Jon Hencinski
@jhencinski

How do you measure #SOC quality? 🤔

1. ISO 2859-1 (#AQL) to determine sample size
2. #Python #Jupyter notebook to perform random selection
3. Check sheet to spot defects
4. Process runs every 24 hrs
5. (Digestible) #Metrics to improve

How'd we get there? Story in /thread

10:40 AM · Apr 26, 2020 · Twitter Web App

Jon Hencinski @jhencinski · Apr 26

My mental model for #SOC QC is two key activities:

1. QA | Focus: *Prevent* defects | Ex: Email notifications for those really spooky alerts

2. QC | Focus: *Find* defects | Ex: Let's review closed alerts

You likely already have a *ton* of QA built in.

But is there any QC?

Jon Hencinski @jhencinski · Apr 26

What next?

We went out and researched QC in manufacturing and landed on ISO 2859-1.

TL;DR ➡️ You make things (your lot), AQL tells you have many you should inspect.

Let's say your team handles 600 alerts per day (lot size).

You should inspect 32 (sample size).

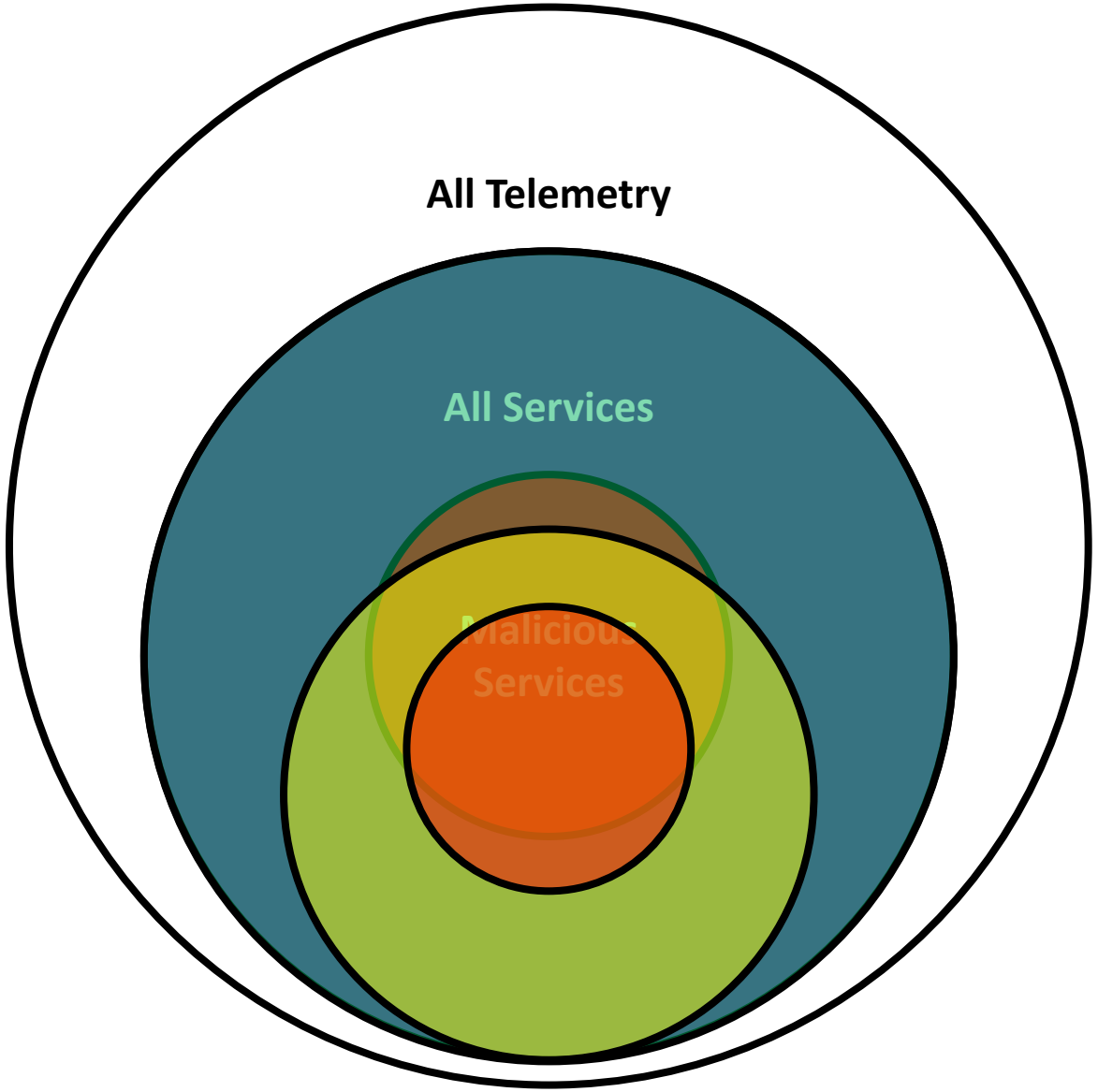
https://twitter.com/jhencinski/status/1254465280367083521?s=20

Rethinking Detection Engineering:
False Positives are Bad, False Negatives are Worse
Jared Atkinson

SO-CON 2020

Prioritization

- Uses the multi-stage detection approach
- All malicious services (subset) must also be services (superset)
- Detection service creation is the “base condition” for detecting malicious service creation
- Accounts for the uncertainty of the positive condition



Tune

www.specterops.io
@specterops
info@specterops.io