



MC2MC

**EXCEPTIONAL DETECTIONS IN YOUR
MICROSOFT SECURITY STACK**

PresenterInfo | project About

Gianni Castaldi

Supporting customers and their security products

Improving the usage of existing security products

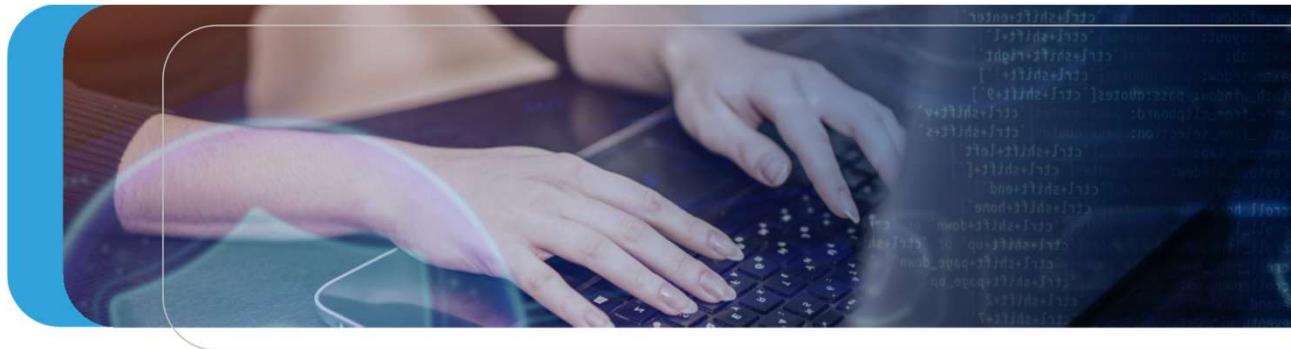
Implementing security new products

Background as an IT Administrator



TODAYS USE CASE

During an incident response we found out that a user clicked on a phishing link in an E-mail. Clicked on the URL and entered their credentials. After entering their credentials, the adversary got access to the user's account.



```
C:\WINDOWS\system32\cmd. X + V - □ X
[21:53:51] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[21:53:51] [inf] loading phishlets from: .\phishlets
[21:53:51] [inf] loading configuration from: C:\Users\GianniCastaldi\.evilginx
[21:53:51] [inf] blacklist: loaded 0 ip addresses and 0 ip masks

+-----+
| phishlet | status   | visibility | hostname      | unauth_url |
+-----+
| example  | disabled | visible   |               |
| microsoft365 | enabled | visible   | evilhacker.com |
+-----+

: lures

+-----+
| id    | phishlet | hostname | path          | redirector | redirect_url | paused | og   |
+-----+
| 0     | microsoft365 |           | /Z2lhbm5pQGt1... |           |             | ---   | --- |
| 1     | microsoft365 |           | /Z2lhbm5pQGt1... |           |             | ---   | --- |
+-----+

: lures get-url 1
https://login.evilhacker.com/Z2lhbm5pQGt1c3Rvd29ya3MuY29t
```

Emergency Password Change!! - Message (HTML)

File Message Help Tell me what you want to do

Share to Teams All Apps Find Zoom

Emergency Password Change!!

GC Gianni Castaldi
To: Gianni Castaldi

Wed 06/11/2024 21:57

Start your reply all with: This is not working. Completed. This link does not work. Feedback

Dear recipient,

Please reset your password as soon as possible.

Go to: <https://login.evilhacker.com/Z2lhbm5pQGt1c3Rvd29ya3MuY29t>

Kind regards,

Not a Hacker

© Kust

Page / 5

[Install software](#)

Good evening

Apps

Outlook	OneDrive	Word	Excel	PowerPoint	OneNote	SharePoint	Teams	Viva	Engage
Power Automate	Loop	Clipchamp	Learning	Project	Bookings	Kaizala	Whiteboard	Insights	To Do
Power Pages	Power Apps	Forms	Sway	Visio	Lists	Stream	Connections	Planner	Calendar
People	Power BI	Delve	Add-Ins						

```
C:\WINDOWS\system32\cmd. X + - □ × by Kuba Gretzky (@mrgretzky) version 3.3.0  
[21:53:51] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)  
[21:53:51] [inf] loading phishlets from: .\phishlets  
[21:53:51] [inf] loading configuration from: C:\Users\GianniCastaldi\.evilginx  
[21:53:51] [inf] blacklist: loaded 0 ip addresses and 0 ip masks  


| phishlet     | status   | visibility | hostname       | unauth_url |
|--------------|----------|------------|----------------|------------|
| example      | disabled | visible    |                |            |
| microsoft365 | enabled  | visible    | evilhacker.com |            |

  
: lures  


| id | phishlet     | hostname | path             | redirector | redirect_url | paused | og  |
|----|--------------|----------|------------------|------------|--------------|--------|-----|
| 0  | microsoft365 |          | /Z2lhbm5pQGt1... |            |              |        | --- |
| 1  | microsoft365 |          | /Z2lhbm5pQGt1... |            |              |        | --- |

  
: lures get-url 1  
https://login.evilhacker.com/Z2lhbm5pQGt1c3Rvd29ya3MuY29t  
  
[22:00:53] [imp] [0] [microsoft365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0 (127.0.0.1)  
[22:00:53] [inf] [0] [microsoft365] landing URL: https://login.evilhacker.com/Z2lhbm5pQGt1c3Rvd29ya3MuY29t  
[22:01:57] [+++] [0] Password: [REDACTED]  
[22:01:57] [+++] [0] Username: [gianni@kustoworks.com]  
[22:01:57] [+++] [0] Username: [gianni@kustoworks.com]  
[22:05:23] [+++] [0] Custom: [mfaAuthMethod] = [PhoneAppNotification]  
[22:05:23] [+++] [0] Username: [gianni@kustoworks.com]  
[22:05:23] [+++] [0] all authorization tokens intercepted!  
:
```



Agenda



Introduction to
Detection
Engineering



Fundamentals of
Detection Engineering



Kusto Query
Language (KQL)



Practical Applications
and Best Practices



Agenda



Introduction to
Detection
Engineering



Fundamentals of
Detection Engineering



Kusto Query
Language (KQL)



Practical Applications
and Best Practices



Introduction to Detection Engineering



Introduction to Detection Engineering



Brief definition

Introduction to Detection Engineering



Brief definition



Importance in modern
cybersecurity

Introduction to Detection Engineering



Brief definition



Importance in modern
cybersecurity



Overview of roles and
responsibilities



© KustoWorks 2024

ROLES IN DETECTION ENGINEERING



ROLES IN DETECTION ENGINEERING



Detection Engineer



ROLES IN DETECTION ENGINEERING



Detection Engineer



Threat Hunter



ROLES IN DETECTION ENGINEERING



Detection Engineer



Threat Hunter



Incident Responder



ROLES IN DETECTION ENGINEERING



Detection Engineer



Threat Hunter



Incident Responder



SOC Analyst





Agenda



Introduction to
Detection
Engineering



Fundamentals of
Detection Engineering



Kusto Query
Language (KQL)



Practical Applications
and Best Practices



Agenda



Introduction to
Detection
Engineering



Fundamentals of
Detection Engineering



Kusto Query
Language (KQL)



Practical Applications
and Best Practices



FUNDAMENTALS OF DETECTION ENGINEERING



Tools



Detection engineering process



Signal Detection Theory

TOOLS



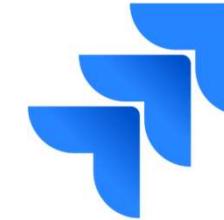
Excel



OneNote

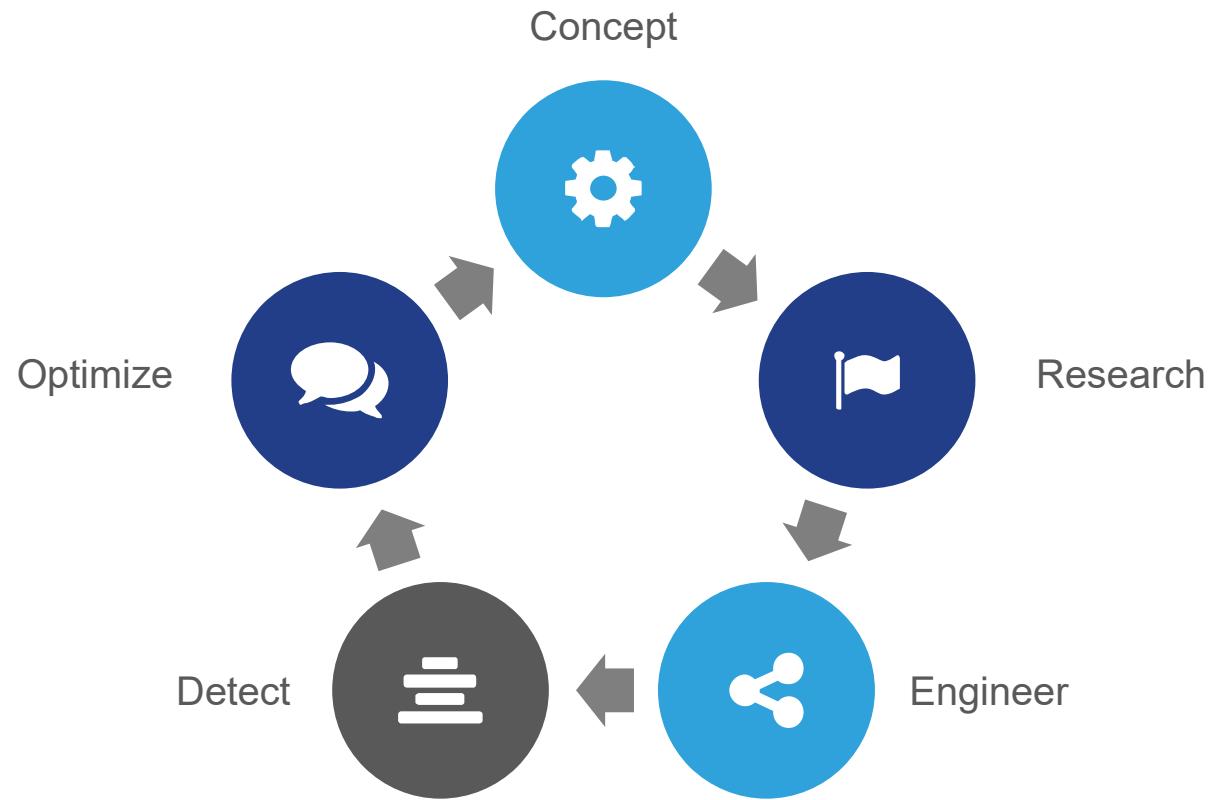


Azure DevOps



Jira

PROCESS



CONCEPT

Item	Description
Title	Name of the detection
Goal	Description of what we want to detect
Scope	What entities should be targeted by the detection
Detection source	What is the source of this detection
Data Source	What is the source of the data
Target Engine	Which engine is the detection made for

SOURCES

Business rules

Incidents

Malware

Offensive Tools & research

Red Team

Threat hunting

Threat Intelligence



CONCEPT

Item	Description
Title	Successful Login Post-URL Click Detection
Goal	Identify successful logins that occur shortly after a user clicks a URL in a phishing email, indicating potential account compromise
Scope	All users
Detection source	Incidents
Data Source	Microsoft Defender XDR
Target Engine	Microsoft Defender XDR

RESEARCH

Item	Description
Strategy Abstract	High level description of what we want to detect
Technical Context	Detailed description for responder to understand the detection
MITRE ATT&CK Tactic identifier	MITRE ATT&CK Tactic ie. Execution
MITRE ATT&CK Technique identifier	MITRE ATT&CK Technique ie.T1059.001
Feasibility	Yes/No
Severity	High Medium Low Informational
Artifacts	What are the items the detection should trigger on

RESEARCH

Item	Description
Strategy Abstract	Detect instances where a user successfully logs in shortly after clicking on a phishing URL from an email, indicating potential account compromise.
Technical Context	This detection identifies correlations between URL click events and subsequent login activities. It uses base64 encoding to match shortened user identifiers within URLs, then cross-references with login attempts within a 15-minute window.
MITRE ATT&CK Tactic identifier	Credential Access
MITRE ATT&CK Technique identifier	T1078 - Valid Accounts
Feasibility	Yes
Severity	High
Artifacts	UrlClickEvents: UrlChain AccountUpn

ENGINEER

Item	Description
Blind Spots and assumptions	Known gaps and assumptions
False Positives	Known false positives
Validation	How to generate a true positive
Version	What is the current version
Response	3-5 steps to investigate this
Additional Resources	References
Comments	Changelog
Suppressions	Which suppressions are made
Detection Logic	Logic

ENGINEER

Item	Description
Blind Spots and assumptions	When the E-mail is sent to a distribution list with a different domain it will not be detected
False Positives	Claude.ai registrations
Validation	Simulate a phishing scenario where a test user clicks a malicious URL and logs in within the specified time frame
Version	1.0
Response	Verify the login location and timing Check the associated email content for phishing indicators Confirm user activity with the impacted individual Isolate the account if suspicious activity is verified Review logs for further signs of compromise
Additional Resources	
Comments	Initial logic, awaiting feedback and tuning
Suppressions	
Detection Logic	KQL

DEPLOY

Item	Description
Deployable Object	[{}]



```
1  {
2    "displayName": "Successful Login Post-URL Click Detection",
3    "schedule": {
4      "nextRunDateTime": "2024-09-07T17:39:41.653333Z",
5      "period": "1H"
6    },
7    "isEnabled": true,
8    "detectionAction": {
9      "alertTemplate": {
10        "severity": "high",
11        "mitreTechniques": [],
12        "title": "Successful Login Post-URL Click Detection",
13        "recommendedActions": "Verify the login location and timing\nCheck the associated email content for phishing indicators\nConfirm user activity with the impacted individual\nIsolate the account if suspicious activity is verified\nReview logs for additional context",
14        "category": "CredentialAccess",
15        "description": "Identify successful logins that occur shortly after a user clicks a URL in a phishing email, indicating potential account compromise",
16        "impactedAssets": [
17          {
18            "@odata.type": "#microsoft.graph.security.impactedMailboxAsset",
19            "identifier": "accountUpn"
20          },
21          {
22            "@odata.type": "#microsoft.graph.security.impactedUserAsset",
23            "identifier": "accountUpn"
24          }
25        ],
26        "organizationalScope": null,
27        "responseActions": []
28      },
29    },
30    "lastRunDetails": {
31      "lastRunDateTime": "2024-09-07T16:39:41.653333Z",
32      "errorCode": null,
33      "status": "completed",
34      "failureReason": null
35    },
36    "createdBy": "gianni@kustoking.com",
37    "lastModifiedBy": "gianni@kustoking.com",
38    "@odata.context": "https://graph.microsoft.com/beta/$metadata#security/rules/detectionRules/$entity",
39    "queryCondition": {
40      "lastModifiedDateTime": null,
41      "queryText": "// Define the length for the encoded UPN substring\r\nlet EncodedUpnLength = 20;\r\n// Extract and transform data from UrlClickEvents\r\n\r\nlet ClickEvents = AccountUpnLower = tolower(AccountUpn)\r\n\r\nlet EncodedUpn = AccountUpn.substring(0, EncodedUpnLength);\r\nlet EncodedUpn = EncodedUpn.replace(/[^a-zA-Z0-9]/g, '');",
42    },
43    "lastModifiedDateTime": "2024-09-07T16:39:40.981483Z",
44    "detectorId": "5edb2469-2a8c-460c-b5c1-2468befcf49f7",
45    "id": "17016",
46    "createdDateTime": "2024-09-07T16:39:40.981483Z"
47  }
```

OPTIMIZATION

Item	Description
Change Log	What changes are made
Notables	What are the findings of the reviews



OPTIMIZATION

Item	Description
Change Log	Added filtering
Notables	Low false positive rate after adding filtering



Item	Description
Title	Name of the detection
Goal	Description of what we want to detect
Scope	What entities should be targeted by the detection
Detection source	What is the source of this detection
Data Source	What is the source of the data
Target Engine	Which engine is the detection made for
Strategy Abstract	High level description of what we want to detect
Technical Context	Detailed description for responder to understand the detection
MITRE ATT&CK Tactic identifier	MITRE ATT&CK Tactic ie. Execution
MITRE ATT&CK Technique identifier	MITRE ATT&CK Technique ie.T1059.001
Feasibility	Yes/No
Severity	High Medium Low Informational
Artifacts	What are the items the detection should trigger on
Blind Spots and assumptions	Known gaps and assumptions
False Positives	Known false positives
Validation	How to generate a true positive
Version	What is the current version
Response	3-5 steps to investigate this
Additional Resources	References
Comments	Changelog
Suppressions	Which suppressions are made
Detection Logic	Logic
Deployable Object	[{}]
Change Log	What changes are made
Notables	What are the findings of the reviews



Signal Detection Theory

OVERVIEW

	Response present	Response absent
Signal present	True positive	False negative
Signal absent	False positive	True negative



IMPORTANT VARIABLES

A large blue circle containing the text "Criterion".

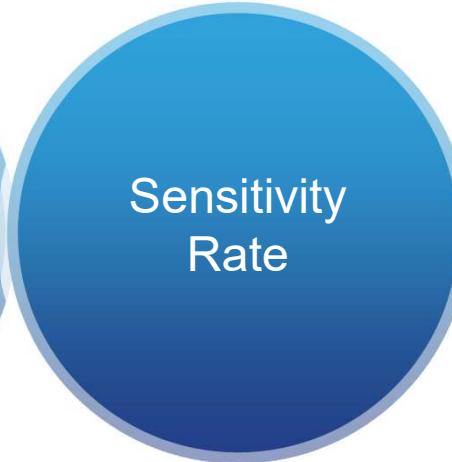
Criterion

A large blue circle containing the text "Hit Rate".

Hit Rate

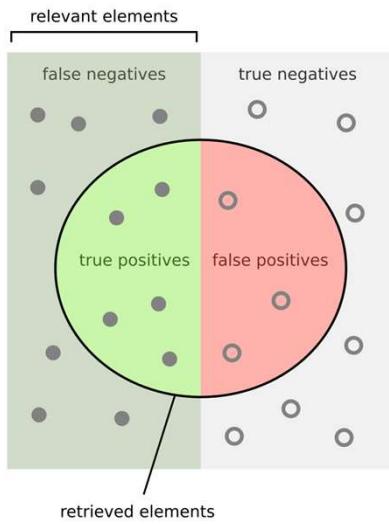
A large blue circle containing the text "False Positive Rate".

False Positive Rate

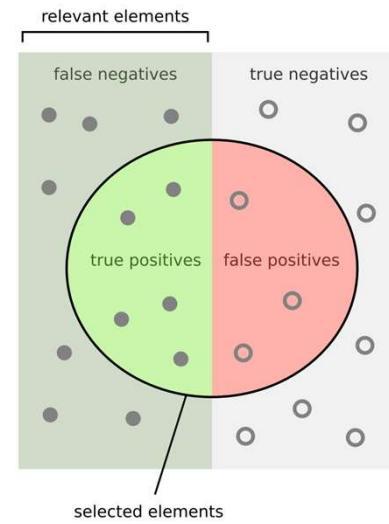
A large blue circle containing the text "Sensitivity Rate".

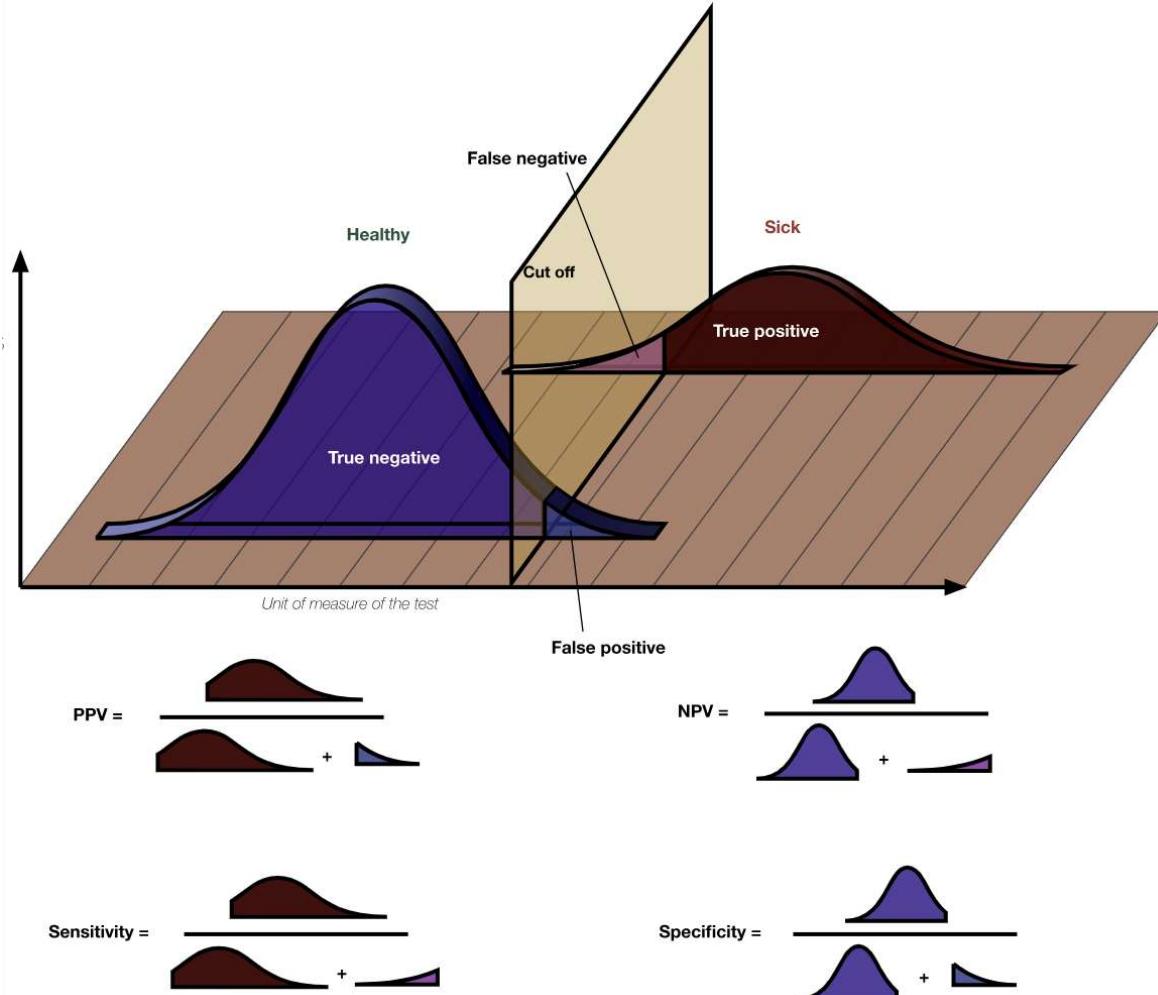
Sensitivity Rate

Precision Recall



Sensitivity Specificity





DO THE MATH

Hit Rate:

Correctly identified threats = 85

Threats that were missed = 15

False Positive Rate:

Safe activities incorrectly flagged = 20

Correctly identified safe activities = 80



THE GOOD

```
1 def calculate_rates(true_positives, false_positives, true_negatives, false_negatives):
2     # Calculate Hit Rate
3     hit_rate = true_positives / (true_positives + false_negatives)
4
5     # Calculate False Positive Rate
6     false_positive_rate = false_positives / (false_positives + true_negatives)
7
8     return hit_rate, false_positive_rate
9
10
11 # Example inputs
12 true_positives = 85 # Number of correctly identified threats
13 false_positives = 20 # Number of safe activities incorrectly flagged as threats
14 true_negatives = 80 # Number of correctly identified safe activities
15 false_negatives = 15 # Number of threats that were missed
16
17 # Calculate rates
18 hit_rate, false_positive_rate = calculate_rates(true_positives, false_positives, true_negatives, false_negatives)
19
20 print(f"Hit Rate: {hit_rate:.2f}")
21 print(f"False Positive Rate: {false_positive_rate:.2f}")
22
23 PS C:\Users\GianniCastaldi> & "C:/Program Files/Python311/python.exe" -m venv venvRate.py
24 Hit Rate: 0.85
25 False Positive Rate: 0.20
```

THE GOOD

```
1  from scipy.stats import norm
2
3  # Hit Rate
4  hit_rate = 0.85 # Hit rate of 85%
5  z_hit = norm.ppf(hit_rate) # Outputs approximately 1.04
6
7  # False Positive Rate
8  false_positive_rate = 0.20 # False positive rate of 20%
9  z_false_positive = norm.ppf(false_positive_rate) # Outputs approximately -0.84
10
11 # Calculate Sensitivity (d')
12 d_prime = z_hit - z_false_positive # Sensitivity calculation
13
14 # Function to classify Sensitivity (d')
15 def classify_sensitivity(d_prime):
16     if d_prime < 0.5:
17         return "Poor Sensitivity"
18     elif 0.5 <= d_prime < 1.0:
19         return "Fair Sensitivity"
20     elif 1.0 <= d_prime < 1.5:
21         return "Moderate Sensitivity"
22     elif 1.5 <= d_prime < 2.0:
23         return "Good Sensitivity"
24     else:
25         return "Excellent Sensitivity"
26
27 # Classification of d'
28 sensitivity_classification = classify_sensitivity(d_prime)
29
30 print("Z-score for Hit Rate:", z_hit)
31 print("Z-score for False Alarm Rate:", z_false_positive)
32 print("Sensitivity (d'):", d_prime)
33 print("Sensitivity Classification:", sensitivity_classification)
```

THE GOOD

Z-Hit: =NORM.S.INV(B1)

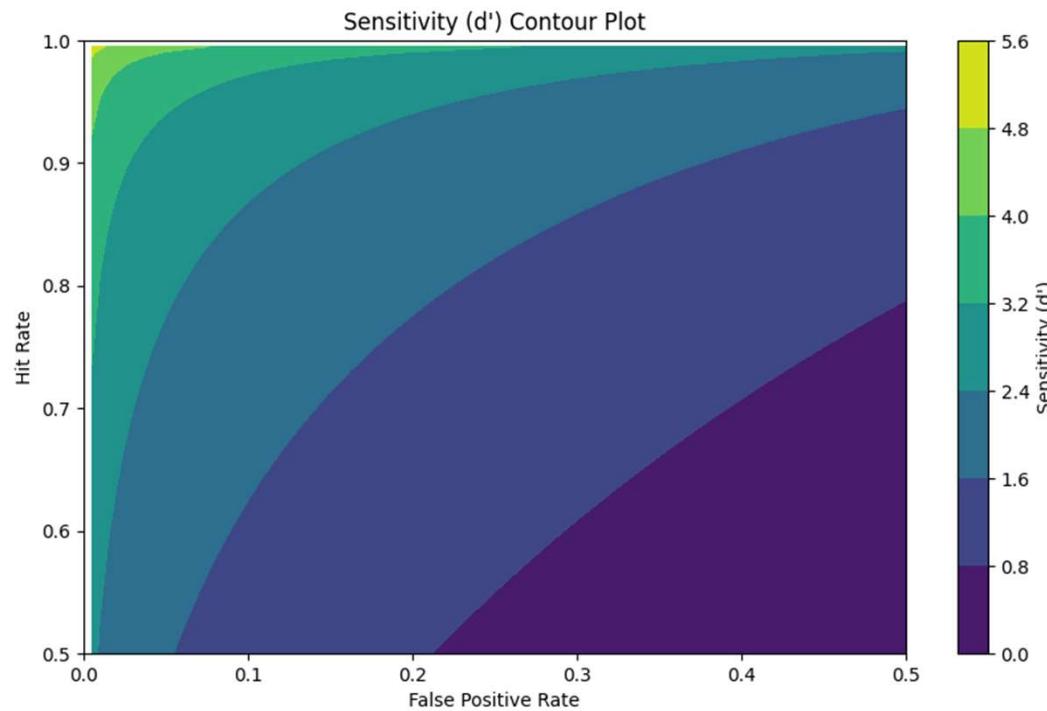
Z-FP: =NORM.S.INV(B2)

d': =B4-B5

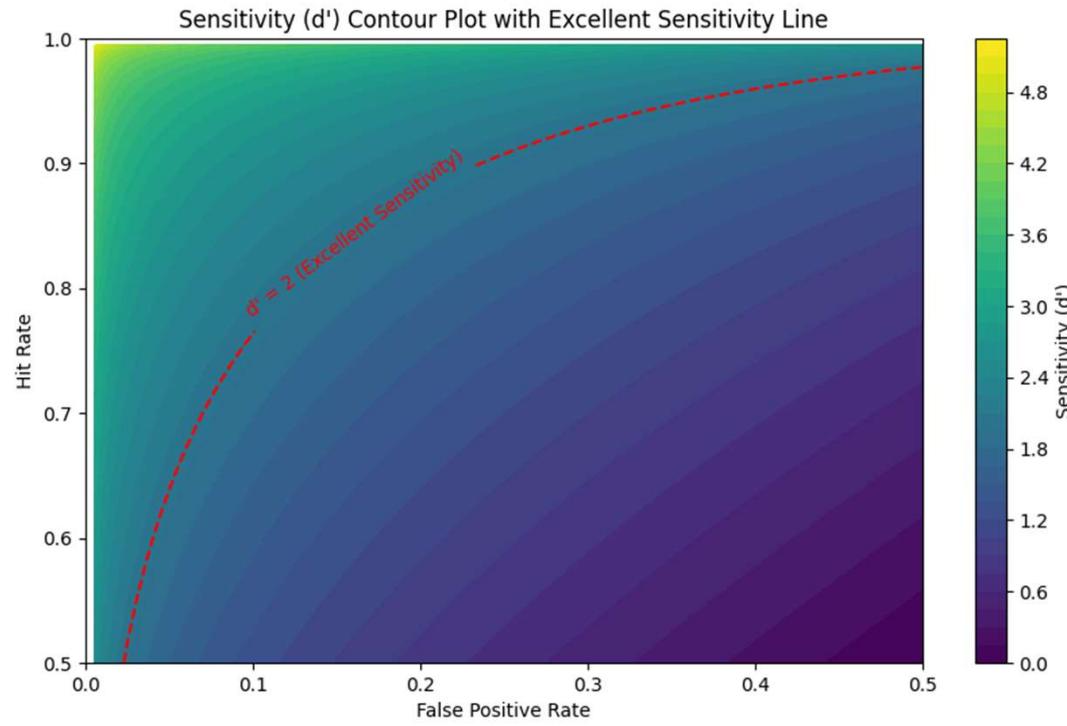
```
=IF(B7 < 0,5; "Poor Sensitivity";
  IF(B7 < 1; "Fair Sensitivity";
    IF(B7 < 1,5; "Moderate Sensitivity";
      IF(B7 < 2; "Good Sensitivity";
        "Excellent Sensitivity"))))
```



THE GOOD



THE GOOD



THE BAD

A screenshot of a Kusto Query Editor interface. At the top, there are buttons for 'Run' (highlighted in blue), 'Time range : Custom', 'Limit : 1000', and a dropdown for 'KQL mode'. Below the header is a code editor containing the following Kusto Query Language (KQL) script:

```
1 SecurityIncident
2 | summarize
3   Total      = count(),
4   Empty      = countif(isempty(Classification)),
5   BenignPositive = countif(Classification == "BenignPositive"),
6   Undetermined = countif(Classification == "Undetermined"),
7   TruePositive = countif(Classification == "TruePositive"),
8   FalsePositive = countif(Classification == "FalsePositive")
9
```

The results section shows a table with the following data:

Total	Empty	BenignPositive	Undetermined	TruePositive	FalsePositive
36604	18087	15549	1731	1158	79

Run Time range: Custom Limit : 1000 KQL mode

```

1 SecurityIncident
2 | summarize
3     Total      = count(),
4     Empty      = countif(isempty(Classification)),
5     BenignPositive = countif(Classification == "BenignPositive"),
6     Undetermined = countif(Classification == "Undetermined"),
7     TruePositive = countif(Classification == "TruePositive"),
8     FalsePositive = countif(Classification == "FalsePositive") by Title, bin(TimeGenerated,30d), Severity
9 | extend PrecisionPercentage = round(
10    (TruePositive*1.00 / (TruePositive + FalsePositive + BenignPositive))
11    ,2
12   )*100
13 | extend Precision = case(
14    PrecisionPercentage >= 80, "High",
15    PrecisionPercentage between (50 .. 80), "Medium",
16    "Low")
17 | project-away Empty, BenignPositive, Undetermined, TruePositive, FalsePositive
18

```

Results Chart Add bookmark

Title ↑	TimeGenerated [UTC]	Severity	Total	PrecisionPercentage	Precision
> 'AskToolbar' unwanted software was detected during a scheduled scan on one endpoint	12/17/2023, 12:00:00.000 AM	Informational	5	0	Low
> 'CandyOpen' unwanted software was prevented on one endpoint	11/17/2023, 12:00:00.000 AM	Informational	3	100	High
> 'CustomCertEnterpriseBlock' malware was prevented on one endpoint	6/14/2024, 12:00:00.000 AM	Informational	11	0	Low
> 'EICAR_Test_File' malware was detected on one endpoint	12/17/2023, 12:00:00.000 AM	Informational	3	100	High
> 'EICAR_Test_File' malware was prevented on one endpoint	3/16/2024, 12:00:00.000 AM	Informational	3	100	High
> 'Edrblok' hacktool was detected on one endpoint	8/13/2024, 12:00:00.000 AM	Low	1	NaN	Low
> 'Edrblok' hacktool was prevented on one endpoint	8/13/2024, 12:00:00.000 AM	Low	3	100	High
> 'ICBundler' unwanted software was prevented on one endpoint	11/17/2023, 12:00:00.000 AM	Informational	4	100	High
> 'InstallCore' unwanted software was prevented on one endpoint	12/17/2023, 12:00:00.000 AM	Informational	4	100	High
> 'MalUri' malware was prevented on one endpoint	2/15/2024, 12:00:00.000 AM	Informational	4	100	High

THE UGLY

A screenshot of a Kusto Query Editor interface. At the top, there are buttons for 'Run' (highlighted in blue), 'Time range : Custom', 'Limit : 1000', and a dropdown for 'KQL mode'. Below the toolbar is a code editor window containing the following Kusto Query Language (KQL) script:

```
1 SecurityIncident
2 | summarize
3     Total      = count(),
4     FalsePositive = countif(Classification == "FalsePositive")
5     by bin(TimeGenerated, 1d)
6 | extend Percentage=round((FalsePositive*1.00/Total),2)*100
7
```

The results section shows a table with four columns: 'TimeGenerated [UTC]', 'Total', 'FalsePositive', and 'Percentage'. The data is as follows:

TimeGenerated [UTC]	Total	FalsePositive	Percentage
> 6/25/2024, 12:00:00.000 AM	64	24	38
> 6/28/2024, 12:00:00.000 AM	44	8	18
> 7/17/2024, 12:00:00.000 AM	106	5	5
> 8/12/2024, 12:00:00.000 AM	57	2	4



Agenda



Introduction to
Detection
Engineering



Fundamentals of
Detection Engineering



Kusto Query
Language (KQL)



Practical Applications
and Best Practices



Agenda



Introduction to
Detection
Engineering



Fundamentals of
Detection Engineering



Kusto Query
Language (KQL)



Practical Applications
and Best Practices

KUSTO QUERY LANGUAGE (KQL)



Read Only
Query Language



Next
PowerShell



Used in a lot
of Microsoft Products

```
<summary>
Customer Master
</summary>
<remarks></remarks>
public class Customer
{
    private string pCustomerCode;
    private string pCustomerName;
    private string pAddress;
    private string pMobileNo;
    public string Customer
    {
        get { return pCustomerCode; }
        set { pCustomerCode = value; }
    }
}
```

^ Query

```
1 // Define the length for the encoded UPN substring
2 let EncodedUpnLength = 20;
3 // Extract and transform data from UrlClickEvents
4 UrlClickEvents
5 | extend AccountUpnLower = tolower(AccountUpn)
6 | extend EncodedUpn = base64_encode_tostring(AccountUpnLower)
7 | extend ShortUpn = substring(EncodedUpn, 0, EncodedUpnLength)
8 | extend AccountDomain = tostring(split(AccountUpnLower, "@")[-1])
9 | extend EncodedDomain = base64_encode_tostring(AccountDomain)
10 | extend DomainLength = strlen(EncodedDomain) - 8
11 | extend ShortDomain = substring(EncodedDomain, 4, DomainLength)
12 // Filter events where the URL chain contains the short UPN or domain
13 | where UrlChain contains ShortUpn or
14     UrlChain contains ShortDomain
15 // Join with IdentityLogonEvents on the lowercased UPN
16 | join kind=inner (
17     IdentityLogonEvents
18     | where LogonType in ("Login:login", "Login:reprocess", "SAS:BeginAuth")
19     | extend AccountUpnLower = tolower(AccountUpn)
20 ) on AccountUpnLower
21 // Calculate the time difference between events
22 | extend Delta = datetime_diff('minute', Timestamp, Timestamp1)
23 // Filter events where the time difference is between 0 and 15 minutes
24 | where Delta between (0 .. 15)
25 // Summarize to get the earliest event by NetworkMessageId
26 | summarize arg_min(Delta, *) by NetworkMessageId
27 // Join with EmailEvents on NetworkMessageId
28 | join EmailEvents on NetworkMessageId
```

The screenshot shows the Microsoft Defender interface for 'Successful Login Post-URL Click Detection'. The left sidebar includes sections for Home, Exposure management, Attack surface, Exposure insights, Secure score, Data connectors, Investigation & response (selected), Incidents & alerts (selected), Threat intelligence, Assets, Microsoft Sentinel, and Identities. The main content area displays a search bar, navigation links (Detection Rules, Successful Login Post-URL Click Detection), and a message indicating the alert is part of an incident involving one user. It shows details for user 'gianni' and 'Gianni Castaldi'. The 'What happened' section describes identifying successful logins shortly after a user clicks a URL in a phishing email. The 'Actions taken' section shows no actions taken. The 'Timeline' tab in the 'Related events' section shows an event from 11/6/2024 at 10:00:50 PM where a URL was clicked. The event details show the URL as https://login.evilhacker.com/Z2lhbm5pQGt1c3Rvd29ya3MuY29t and the Network message id as cb7c408e-ec3a-4430-29ec-08dcfea5b740. The right side of the screen provides an 'INSIGHT' summary for the alert, including classification (Not Set), assigned to (Unassigned), category (MITRE ATT&CK Techniques - Credential access), detection source (Custom detection), service source (Microsoft Defender XDR), and generation date (Nov 6, 2024 10:21:03 PM). There are also buttons for managing the alert and classifying it.



Agenda



Introduction to
Detection
Engineering



Fundamentals of
Detection Engineering



Kusto Query
Language (KQL)



Practical Applications
and Best Practices



Agenda



Introduction to
Detection
Engineering



Fundamentals of
Detection Engineering



Kusto Query
Language (KQL)



Practical Applications
and Best Practices



Best Practices and Common Pitfalls

Review detections every 6 months
Document your detections

Not having a classification framework
Not measuring detections



SUMMARY

CREDO

Formalize your detection engineering

Signal Detection Theory

Make your detections measurable

KQL

Optimize the performance



REFERENCES

<https://detect.fyi/a-research-driven-process-applied-to-threat-detection-engineering-inputs-1b7e6fe0412b>

<https://digitalcommons.usf.edu/etd/6728/>

https://www.wikipedia.org/wiki/Detection_theory

<https://www.kqlsearch.com>

<https://www.kqlcafe.com>



KustoCon

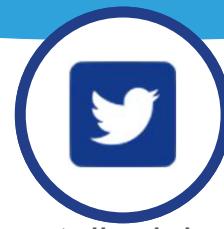
Learn | Share | Practice

November 8th, 2024

Thanks for
Watching



giannicastaldi



castello_johnny



gianni@kustoworks.com