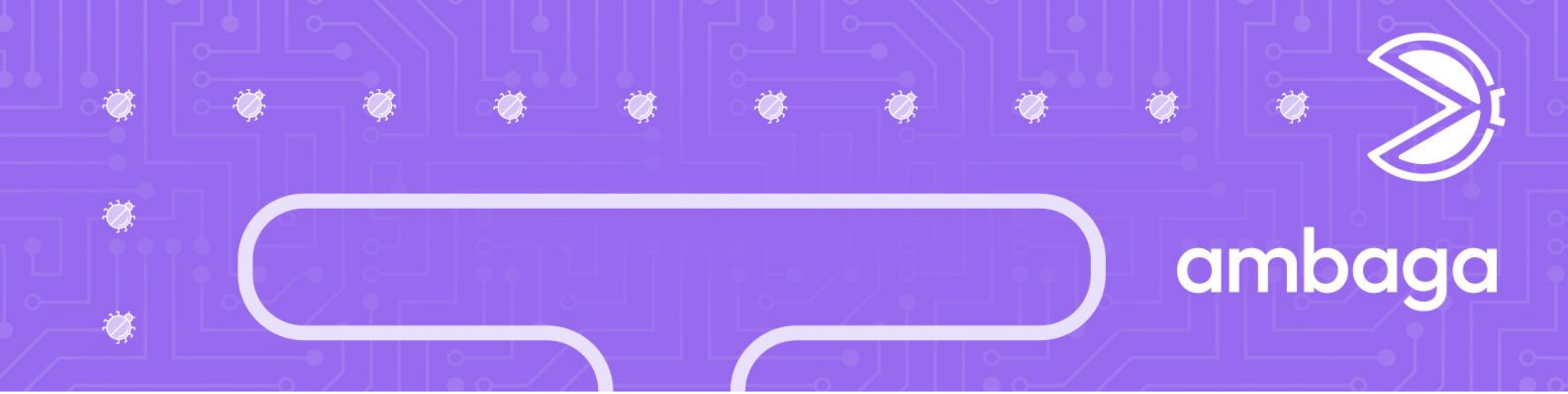
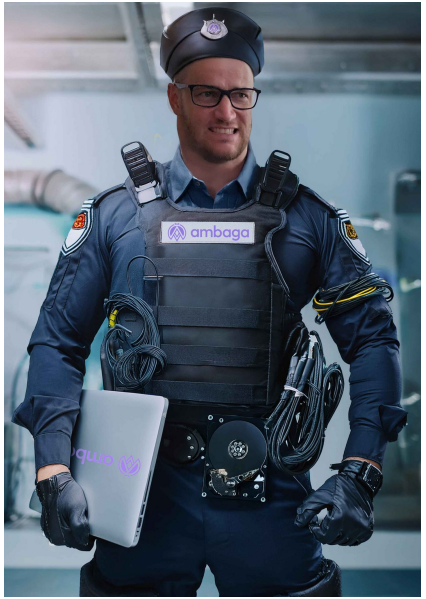


Detection and Response, hverjum er ekki drull!

ambaga

- Bergsteinn Karlsson
- Lögreglan
- Syndis - Origo - Syndis
  - Security Engineer
  - Team Lead
- Lacework
  - Senior Security Engineer
- Ambaga
  - Co-Founder



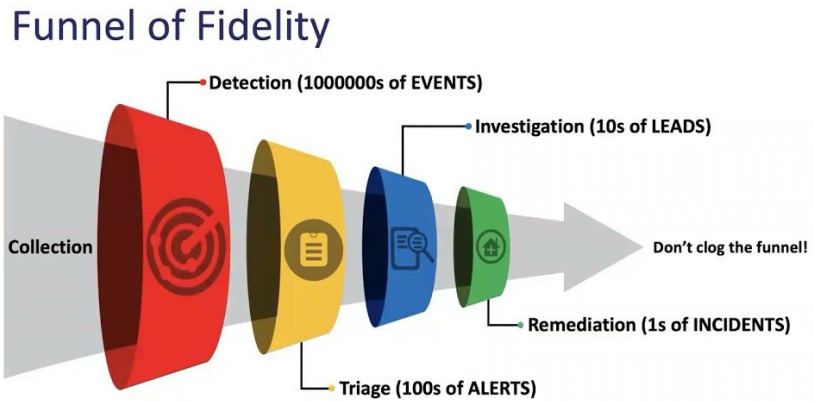
Vöktun og Viðbrögð (Detection and Response)

- Hvaða vandamál erum við að reyna leysa?
- Nokkrir burðarveggir
- Söfnun (Logging)
  - Erfitt að tryggja yfirsýn
  - Gagnaflækja, hreiðrun
  - Hverju eigum við að safna og hvar?
- Vöktun (Detection)
  - Líma og binda snæri saman úr öllum áttum
  - Aðlaga að mismunandi útgáfum af sömu upplýsingum
  - Sér fyrirspurnarmál (QL) fyrir hvert Gagnasöfnunartól(SIEM)
- Viðvaranir og Bráðaflokkun (Alerting and Triaging)
  - Hvar? sms, email, Slack/Teams/MSN
  - Viðvörunar Streita/Óræðni (Alert Fatigue/Ambiguity)
  - Á ég að flokka þetta sem atvik?
- Viðbragð (Response)
  - Hvernig á ég að bregðast við og hvar er það skjalað?
  - Hver á að gera hvað og hvernig...
- Nú er komið upp atvik, hvernig leysum við það

ambaga

Trektin (Funnel of Fidelity)

- SpectreOps
  - BloodHound
- Hugmyndafræði í D&R
- Ekki stífla trektina
- Ómennskt að bregðast við öllum þessum upplýsingum handvirkt
- Gæði í hverju þrepi
- Kæruleysi í einhverju þrepi stíflar
- Markviss nálgun
  - Hjálpar við að greina flöskuhálsa



https://posts.specterops.io/introducing-the-funnel-of-fidelity-b1bb59b04036

ambaga

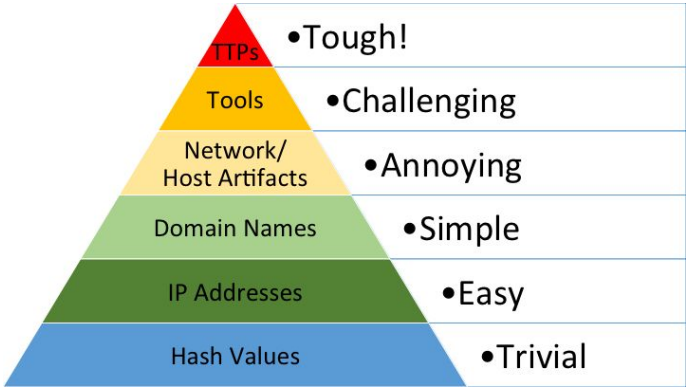
Söfnunarárátta (Log Management)

- Grunnstoð
- Miðlæg söfnun óháð uppruna gagna
- Ákvarða nauðsynleg gögn
  - tryggir nauðsynlegt samhengi
- Blindir blettir
  - fjármálasvið
- Varðveisla (Retention)
- Hjartsláttur (Heartbeat) reglulega
- Venjulegun (Normalization) á algengum gildum
  - datetime - ISO 8601 - UTC
  - IP, src_ip, dst_ip, port
  - hostname
  - Email
- Þetta er komið!

ambaga

Vöktun (Detection)

- Tryggja að þetta keyri - Hjartsláttur
- Harðgerðar - Skerða aðlögunarhæfni
- Stöðugt að vera vakandi fyrir nýjum árásum
- Locard's exchange principle
  - “Every contact leaves a trace”
- Pýramídi sársaukans, David Bianco
  - “Pýramígreni” Hjaltiminn
  - Viðvaranir sem valda sársauka
- Vá.. Trekt og Pýramídi... My brain hurts
- Fatatíska úlfsins: Finnbogi

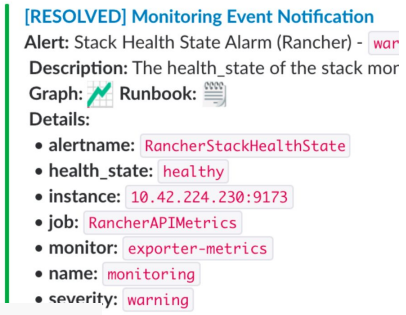


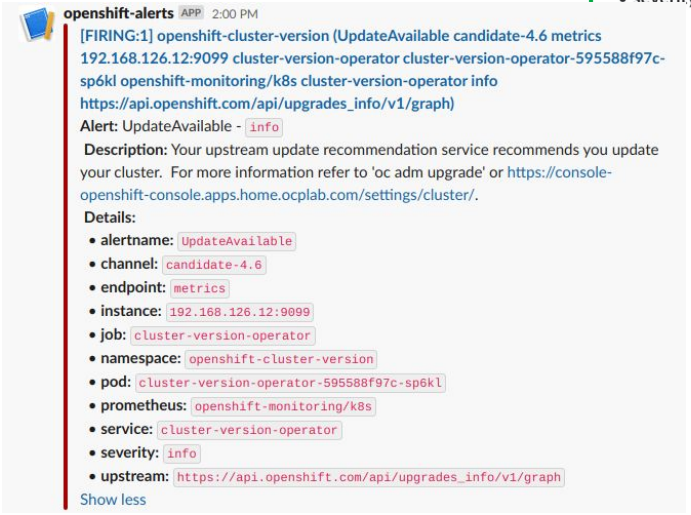
GitHub - SigmaHQ/sigma: Main Sigma Rule Repository
https://posts.specterops.io/detection-spectrum-198a0bfb9302
https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

ambaga

Viðvörun og Bráðaflokkun (Alerting and Triaging)

- Sjónaukinn (Single pane of glass)
- Samhengi til að bregðast við
  - Aðgerðarhæft (Actionable), nákvæmar, hjálplegar
    - Hver
    - Hvað
    - Hvenær
    - Hvar
    - Hvers vegna
  - Fækka smellum
- Suðhlutfall (Signal to noise ratio)
- Vel skjalað Detection
- Endurgjöf og umbætur



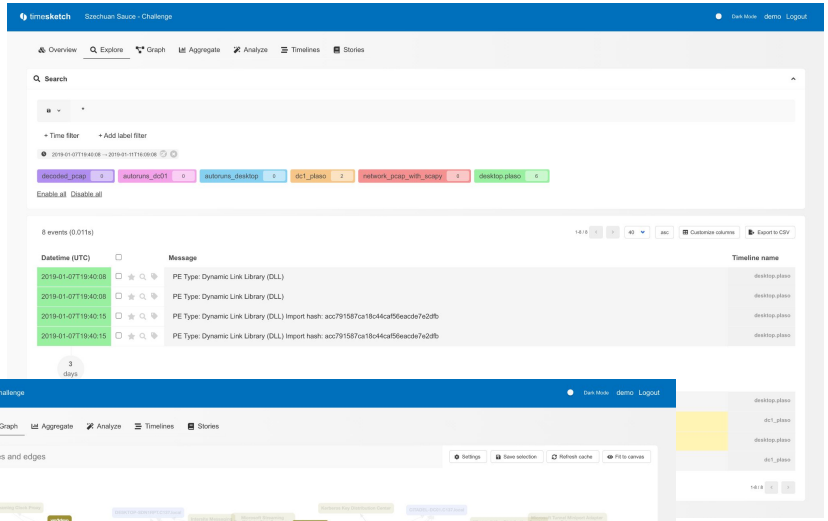


https://harthoover.com/pretty-alertmanager-alerts-in-slack/
https://gexperts.com/wp/sending-alerts-to-slack-in-openshift/

ambaga

Viðbragð (Response)

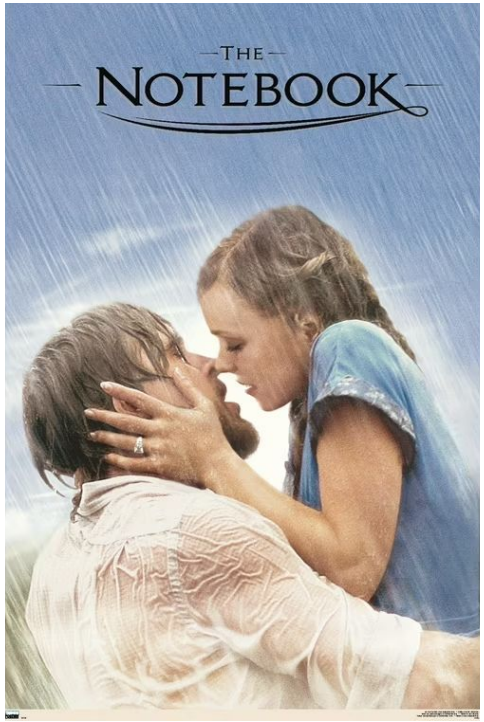
- Verkferlar og skjölun
  - Hlutverk
  - SANS 6 steps
- Nótnabækur (Notebooks)
- Ógnarveiði (Threat Hunting)
  - Yfirheyra vélar (Live response)
  - EDR, Velociraptor
- Tímalína
  - Línuvörður!
- Sjálfvirknivæða!



https://github.com/0x4D31/awesome-threat-detection
https://github.com/google/timesketch

ambaga

Notebook



ambaga

Notebooks

- Jupyter No
- Open Sou
- Vefviðmót
  - Keyra k
  - Vinna g
  - Tölfræð

threat-hunting-notebook.ipynb ● | maltiverse_web_ip_lookup.py | __init__.py

threat-hunting-notebook.ipynb > My Title > Malicious IP Address Checker 2 > import interacting_with_apis.maltiverse_web_ip_lookup as ip_checker

+ Code | + Markdown | Run All | Clear All Outputs | Restart | Variables | Outline | ··· | Python 3.11.3

My Title

This Notebook will contain my Python threat hunting tools.

Malicious IP Address Checker

This tool checks if an IP address it malicious. To add an IP address to check, change the IP variable and run the cell.

```
from maltiverse import Maltiverse

IP = "171.61.223.122"

api = Maltiverse()
result = api.ip_get(IP)
try:
    # print the 'classficiation' of the IP address
    print(f"\n=> The IP address {IP} has been identified as {result['classification']} by Malitverse\n")
except KeyError:
    # no classficiation avaliable from Maltiverse
    print(f"\n - The IP address {IP} cannot be classified by Malitverse\n")
```

[1] ✓ 0.6s Python

```
=> The IP address 171.61.223.122 has been identified as malicious by Malitverse
```

Malicious IP Address Checker 2

This tool checks if an IP address it malicious. To add an IP address to check, change the IP variable and run the cell.

```
import interacting_with_apis.maltiverse_web_ip_lookup as ip_checker

IP = "171.61.223.122"
ip_checker.run(IP)
```

[2] ✓ 0.4s Python

```
=> The IP address 171.61.223.122 has been identified as malicious by Malitverse
```

ELK_Threat_Hunting.ipynb

Notebooks

- Rauntíma vinnsla - þarf raunstöðu
- Sjálfskjalandi
- Endurkeyrt og endurnotað
- Sjónræn birting - gröf og tölfræði
- Risastórt samfélag og tengimöguleikar
- Einfalt að staðfesta niðurstöður
- Aðgengileg sniðmát
  - Azure-Sentinel-Notebooks
- Frumgerðarskrímsli!
  - Afurðin oft nothæf detection
- Fjölbreyttur stuðningur
  - Local, cloud, managed (Sagemaker, Colab)

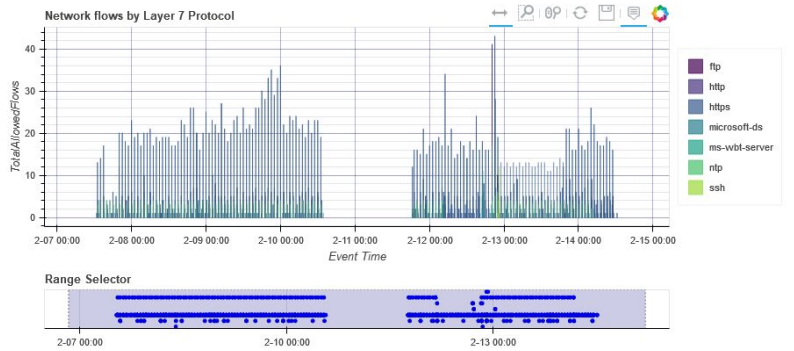
Azure-Sentinel-Notebooks

```
In [105]:
netflow_df = qry_prov.Network.list_azure_network_flows_by_host(search_q_times, host_name="MSTICAlertsWin1")

nbdisplay.display_timeline_values(
    data=az_net_comms_df,
    group_by="L7Protocol",
    source_columns=["SrcIP", "DestIP", "TotalAllowedFlows"],
    time_column="FlowStartTime",
    title="Network flows by Layer 7 Protocol",
    y="TotalAllowedFlows",
    legend="right",
    height=300,
    kind=["vbar"]
)
```

executed in 2.12s, finished 14:17:49 2019-11-02

BokehJS 1.3.4 successfully loaded.

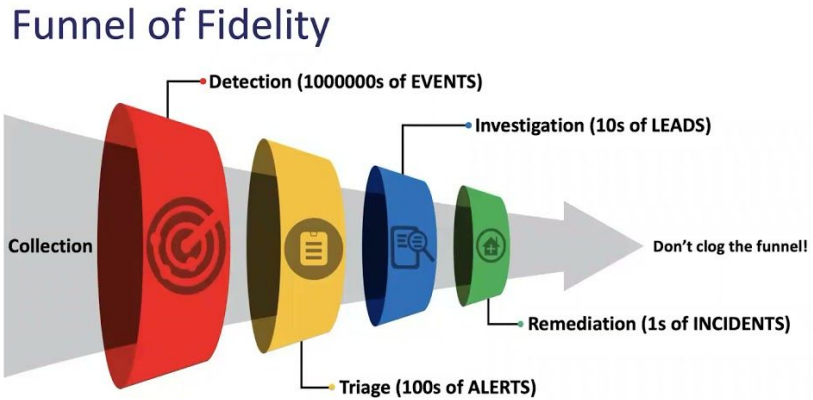


https://github.com/Azure/Azure-Sentinel-Notebooks

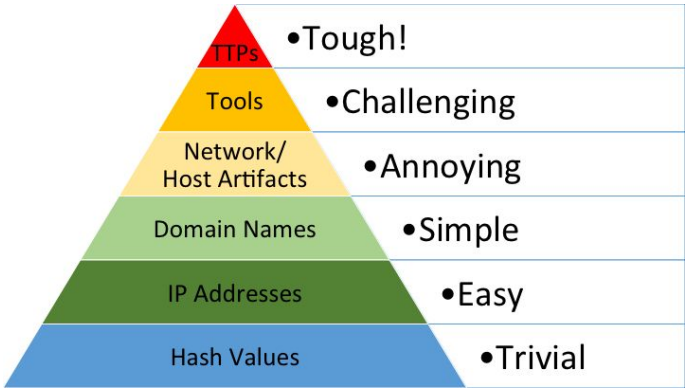
ambaga

Að lokum

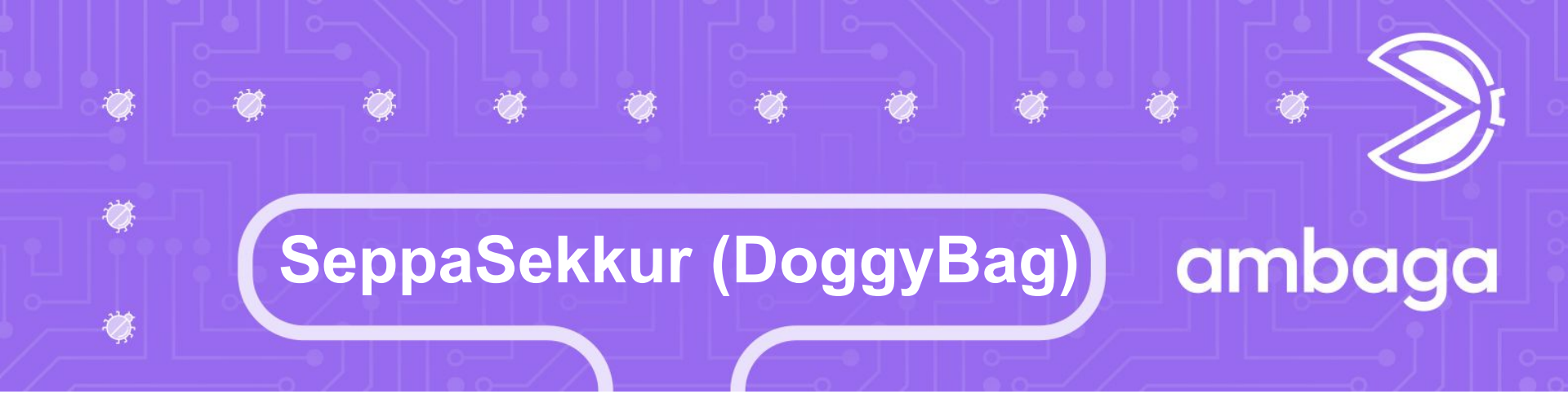
Ekki stífla trektina!



No Pain No Gain!



ambaga



Detection

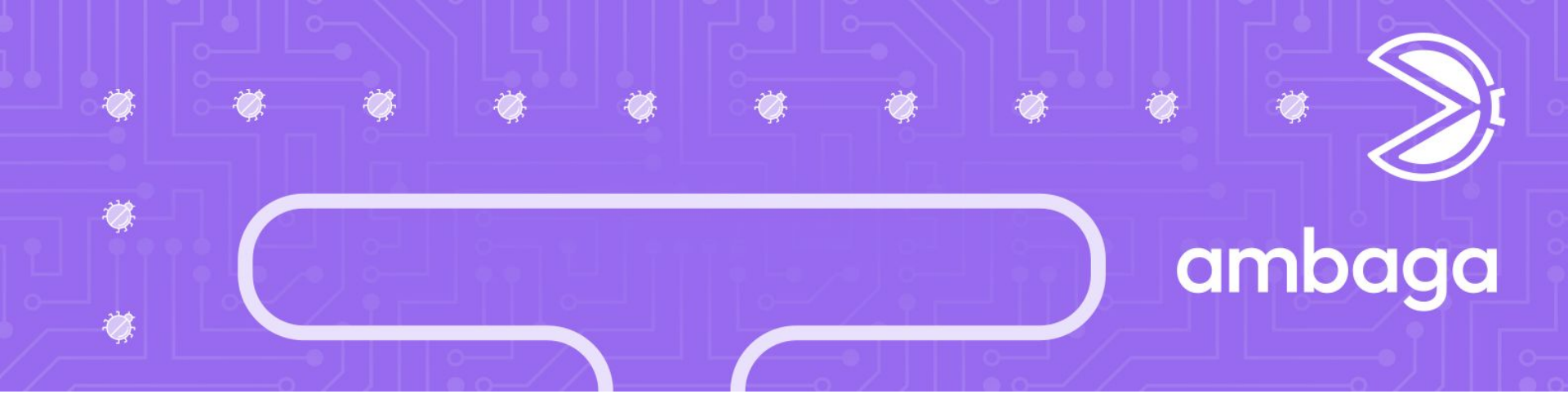
- A framework for developing alerting and detection strategies for incident response.
- Enterprise Detection & Response: The Pyramid of Pain
- https://github.com/nianticlabs/venator
- Introducing the Funnel of Fidelity | by Jared Atkinson | Posts By SpecterOps Team Members
- Detection Spectrum. Have you ever heard someone call… | by Jared Atkinson | Posts By SpecterOps Team Members
- A curated list of awesome threat detection and hunting resources 🕵
- Detection.FYI

DFIR

- GitHub - google/osdfir-infrastructure: Helm charts for running open source digital forensic tools in Kubernetes
- OpenRelik
- Johann Berggren kynnir OpenRelik

Notebooks

- AWS
  - How to improve your security incident response processes with Jupyter notebooks
- MSFT
  - Interactive Azure Sentinel Notebooks provides security insights and actions to investigate anomalies and hunt for malicious behaviors.
  - MSTICPy
- GCP
  - Introduction to Colab Enterprise | Google Cloud

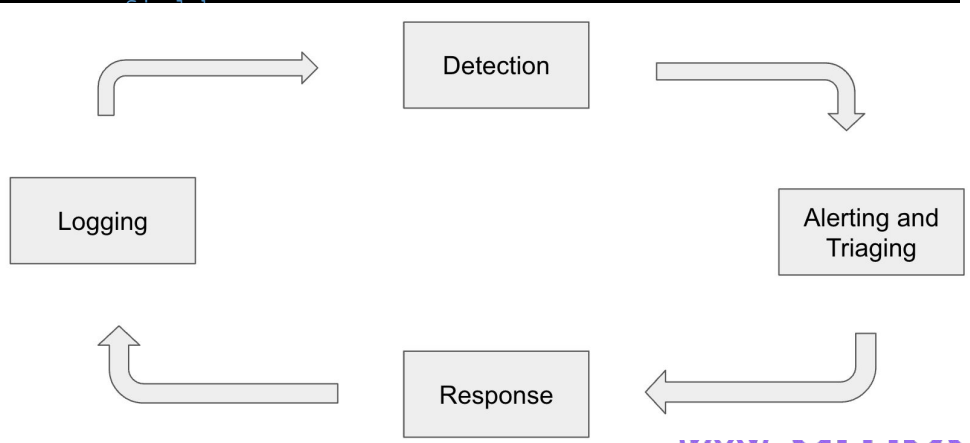


Takk fyrir ykkur, þið eruð nóg!

Sigma dæmi - Brothætt

```yaml
title: Detection of Specific Malicious File by Hash
id: 8c7a1b6e-3d5f-4e2b-9a6f-1b2c3d4e5f6a
description: Detects a known malicious file based
on its MD5 hash value.
status: lame
author: Beggi
date: 2024-11-11
references:
   - https://tiktok.is/things-and-stuff
logsource:
   category: file_event
   product: windows
```

```yaml
detection:
    selection:
        Hashes|contains:
            - 5a89aac6c8259abbba2fa2ad3fcefc6e
    # Example MD5 hash
    condition: selection
```



Sigma dæmi - Ekki eins brothætt

```yaml
title: Suspicious Command Shell Spawned by Office Application
id: a1b2c3d4-5e6f-7081-1337-b4c5d6e7f8g9
description: Detects when Office applications spawn a command
shell, which may indicate macro malware execution.
status: stable
author: Beggi
date: 2024-11-12
references:
   - https://attack.mitre.org/techniques/T1059/
   - https://attack.mitre.org/techniques/T1566/001/
logsource:
   category: process_creation
   product: windows
detection:
   selection:
       ParentImage|endswith:
           - '\WINWORD.EXE'
           - '\EXCEL.EXE'
           - '\POWERPNT.EXE'
           - '\OUTLOOK.EXE'
       Image|endswith:
           - '\cmd.exe'
           - '\powershell.exe'
           - '\wscript.exe'
           - '\cscript.exe'
   condition: selection
fields:
   - Timestamp
   - Image
   - CommandLine
   - ParentImage
   - ParentCommandLine
   - User
falsepositives:
   - Legitimate administrative scripts or macros (should be
verified)
level: high
```

Dagur í lífi D&R

- Safna gögnum (LogLogLog)
- Vinna gögn (Transform/Parse)
- Búa til vaktanir (Detection)
- Bregðast við viðvörun (Alerts)
- Stigmögnun (Escalation)
- Atvik (Incident)
- Drekka kaffi
- Laga Blindblett (Blindspots)
- Sækja á leikskólann

ambaga