

Detection Philosophy, Evolution & ATT&CK

A BRIEF DISCUSSION AROUND HOW WE ARE MANAGING OUR
'DETECTION CATALOG' AND HOW IT MAPS TO AND IS ENHANCED BY
THE ATT&CK FRAMEWORK

Fred Stankowski & Travis McWaters

Who are you?

Cyber Threat Intelligence (CTI)



Threat Detection Operations (TDO)



Incident Response (IR)



Attack Surface Management (ASM)

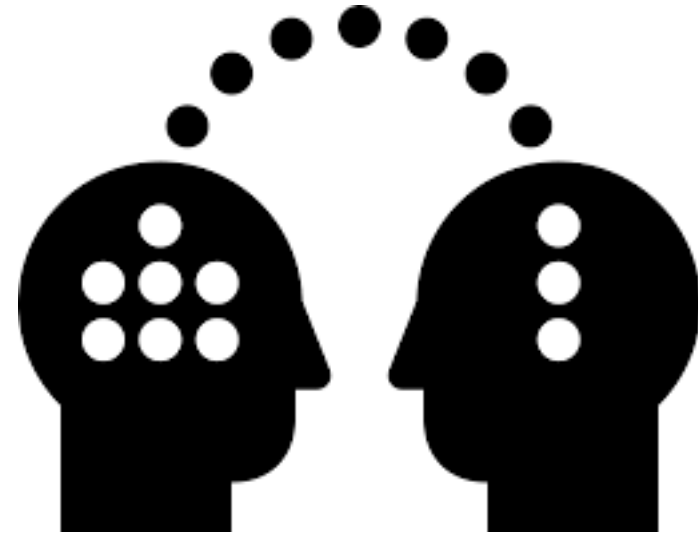


Enterprise Incident Mgmt (EIM)



Why you need a catalog

- Historical Record
- Knowledge Transfer
- Work Management



Evolution – V0

OneNote File Edit View Insert Format Notebooks Tools Window Help

Archive » Alert Catalog

Home Insert Draw View Table

<

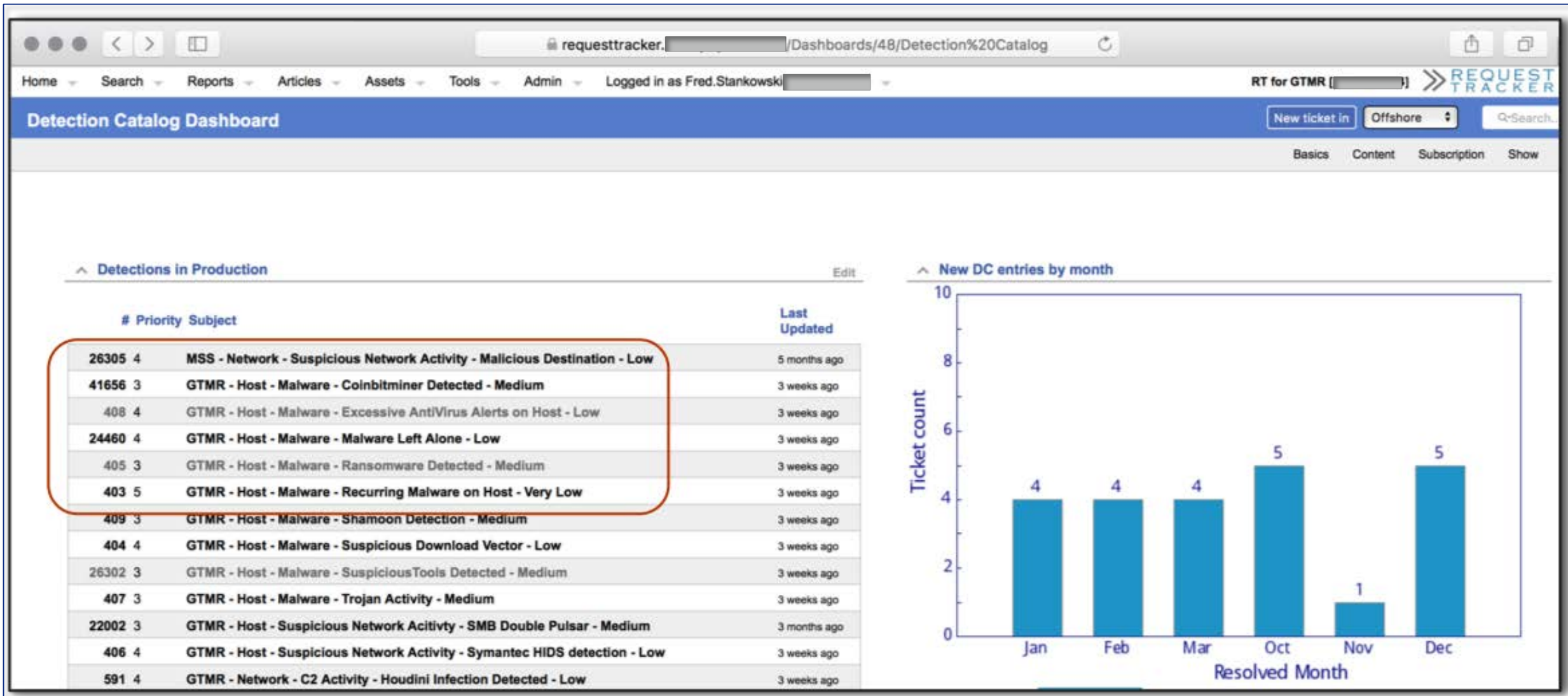
Alert Catalog Summary

Wednesday, January 27, 2016 3:11 PM

SATD Automated Alerts

Friendly Title	Status	Who	Description
[Host-Malware-0001] Recurring Malware on Host	Prod	DM	Systems that repetitively have Malware alerts, may
[Host-Malware-0002] Malware on VIP Host	Prod	DM	Malware detected on Banded employee equipmen
[Host-Malware-0003] Suspicious Download Vector	Prod	DM	File downloaded by unusual executable. Good for f
[Network-C2 Activity-0004] Suspicious Browsing to Intel listed Domains BlueCoat	Building	TH	Using Blue Coat Malicious Outbound category to fi
[Network-C2 Activity-0005] Suspicious Browsing to Intel listed Domains MWG	Building	TH	Search MWG logs using the Domain <u>BlackList</u> built
[Network-C2 Activity-0006] Houdini Infection Detected	Prod	DM	Detect Houdini malware by its unusual user agent :
[Host-Malware-0007] Ransomware Detected	Prod	DM	Detect Ransomware/crypto malware in the Syman
[Host-Malware-0008] Malware detected by Symantec IDS	Prod	TH	Monitor Symantec Host Intrusion Prevention Syste
[Host-Malware-0009] Trojan activity detected	Prod	DM	Detect Trojan activity by monitoring Symantec Risk
[Host-Malware-0010] Excessive Malware alerts on Host	Prod	TH	Detect <u>sep</u> risk events that occur repeating in hour
[Host-Malware-0011] <u>Shamoon</u> Detected	Prod	TH	Detection of W32.Disttrack
[Network-Suspicious Network Activity-0012] <u>Shamoon</u> Detection	Prod	TH	Detection of <u>Shamoon</u> by domain
[Host-Malware-0013] <u>Shamoon</u> Checksum Detected	Prod	AB	Detection of <u>Shamoon</u> by checksum

Evolution V1



#26302: GTMR - Host - Malware - SuspiciousTools Detected - Medium New ticket in Offshore Q-Search

Display History Basics People Dates Links Jumbo Reminders Actions ☆ 🕒

^ Ticket metadata Hide unset fields

^ The Basics

Id: 26302

Status: production

Priority: 3/

Queue: Detection Catalog

^ Incident Metadata

Current_Status: (no value)

^ Alert

Alert_Name: (no value)

^ Custom Fields

Detection_Platform: Splunk - ISG

Detection_Name_on_Platform: GTMR - Alert - Endpoint - Malware - 0023 Suspicious Tools Detected

index="endpoint_monitor" sourcetype="symantec:ep:risk:file" (PwDump OR Hacktool.PTHToolkit OR SecurityRisk.WinCredEd OR SecurityRisk.BL) OR (file_name="*.ps1") OR ("Security Assessment Tool" AND (signature != AngryIPScanner AND signature != PasswordRevealer)) OR (Category_Type="Hack Tool" AND (signature!=Hacktool.Kms AND signature!=Hacktool.ProduKey))

^ Reminders

New reminder:

Subject:

Owner: Fred.Stankowski@pepsico.com (Stankowski, Fred (BIS)) ⌵

Due:

Save

^ Dates

Created: Wed Aug 02 16:32:30 2017

Starts: Not set

Started: Wed Aug 02 16:40:38 2017

Last Contact: Wed Aug 16 11:43:10 2017

Due: Not set

Closed: Thu Aug 17 08:56:08 2017

Updated: Fri Mar 09 15:31:51 2018 by Travis.Mcwaters@pepsico.com (Mcwaters, Travis (BIS))



^ Links Graph

Depends on: (Create)

Depended on by: (Create)


Parents: (Create)

Evolution V2



Spaces ▾ People Questions Polls Calendars Create ...

- GTMR - Host - Malware - Coinbitminer Detected
- GTMR - Host - Malware - Excessive AntiVirus Alerts on Host [Draft]
- GTMR - Host - Malware - Malware Left Alone
- GTMR - Host - Malware - Ransomware Detected
- GTMR - Host - Malware - Recurring Malware on Host
- GTMR - Host - Malware - Shamoon Detection [Draft]
- GTMR - Host - Malware - Suspicious Download Vector
- GTMR - Host - Malware - SuspiciousTools Detected [Draft]
- GTMR - Host - Malware - Trojan Activity
- GTMR - Host - Suspicious Host Activity - cmd.exe called Powershell [Draft]
- GTMR - Host - Suspicious Host Activity - Explorer called Powershell [Draft]
- GTMR - Host - Suspicious Host Activity - Malformed File Process Launch [test]
- GTMR - Host - Suspicious Host Activity - SEP Risk Events on Critical Server
- GTMR - Host - Suspicious Network Activity - SMB Double Pulsar
- GTMR - Host - Suspicious Network Activity - Symantec HIDS detection
- GTMR - Host - Windows - SWIFT - Security Log Cleared
- GTMR - Host - Windows - SWIFT - Service failed or Unexpected Shutdown
- GTMR - Host - Windows - SWIFT - Service Installed

 Space tools ▾ <<

```
{
  "Status": "production",
  "Queue": "Event Correlation",
  "Detection_Name_on_Platform": "GTMR - Host - Malware - Coinbitminer Detected",
  "Priority": 3,
  "Subject": "GTMR - Host - Malware - Coinbitminer Detected",
  "Detection_Platform": "Splunk - ISG"
},
{
  "Status": "test",
  "Queue": "Test Detections",
  "Detection_Name_on_Platform": "GTMR - Host - Suspicious Host Activity - Malformed File Process Launch",
  "Priority": 5,
  "Subject": "GTMR - Host - Suspicious Host Activity - Malformed File Process Launch",
  "Detection_Platform": "Splunk - ISG"
},
```

Network - Suspicious Network Activity - SMB Worm Behavior

Goal

Detect SMB Worms by the firewall deny messages they generate

Categorization

These attempts are categorized as [Scanning / Network Service Scanning \(T1046\)](#)

Strategy Abstract

The strategy will function as follows:

- Look for traffic blocked by the firewalls bound for destination port 445
- Count the number of destination hosts a source tried to reach
- Validate the source is a Company asset, not external
- Alert if the number of targets exceeds NNN in under MMM minutes

- Blind Spots and Assumptions
- False Positives
- Validation
- Priority
- Response

Technical Context

<...>

**Nomenclature
Matters**

**Use a code repo
sooner**



**Good docs
mitigate attrition
pains**