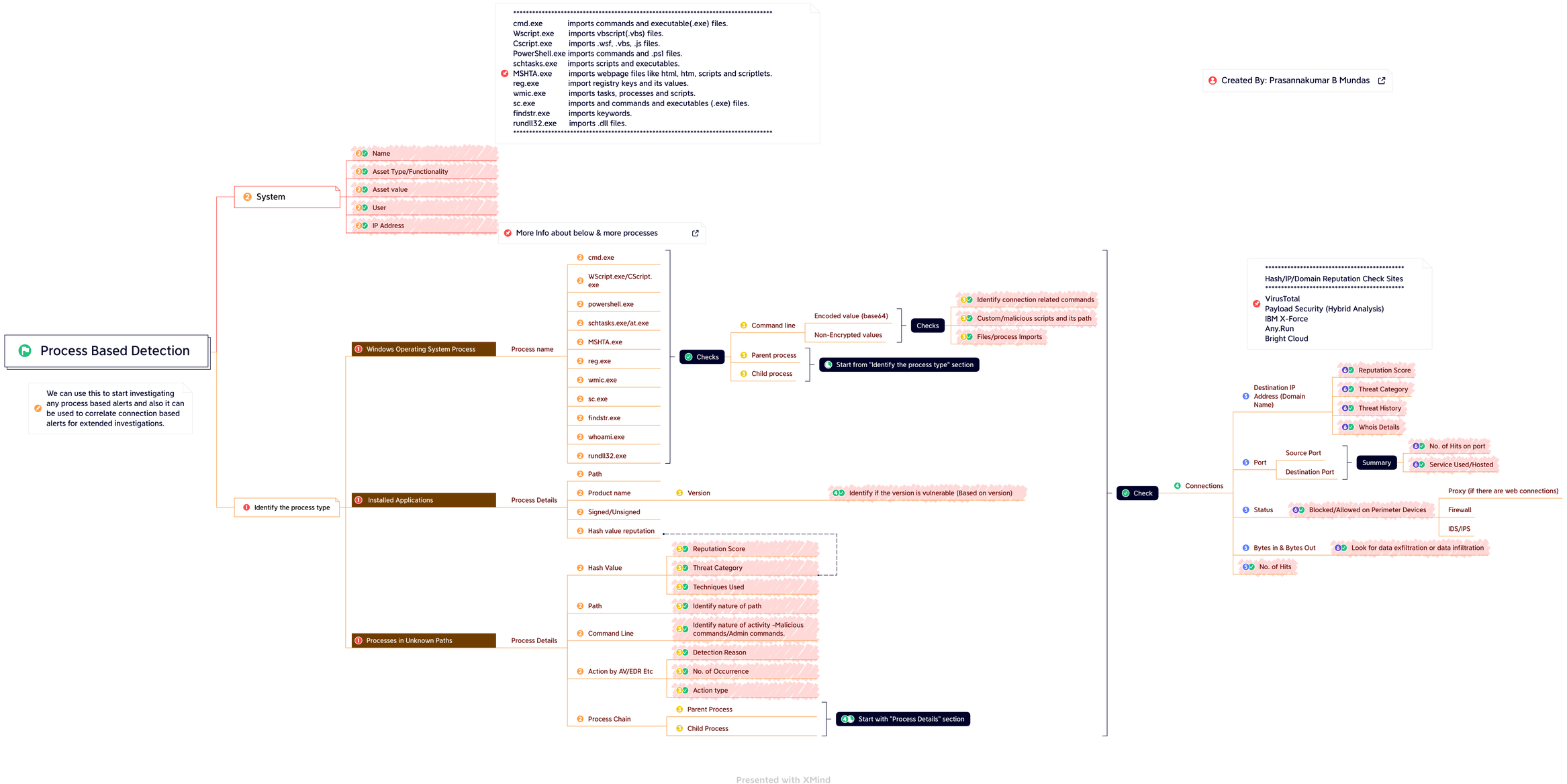
cmd.exe imports commands and executable(.exe) files.
Wscript.exe imports vbscript(.vbs) files.
Cscript.exe imports .wsf, .vbs, .js files.
PowerShell.exe imports commands and .ps1 files.
schtasks.exe imports scripts and executables.
MSHTA.exe imports webpage files like html, htm, scripts and scriptlets.
reg.exe import registry keys and its values.
wmic.exe imports tasks, processes and scripts.
sc.exe imports and commands and executables (.exe) files.
findstr.exe imports keywords.
rundll32.exe imports .dll files.
Created By: Prasannakumar B Mundas
Process Based Detection
We can use this to start investigating any process based alerts and also it can be used to correlate connection based alerts for extended investigations.
Identify the process type
System
Name
Asset Type/Functionality
Asset value
User
IP Address
More Info about below & more processes
Windows Operating System Process
Process name
cmd.exe
WScript.exe/CScript.exe
powershell.exe
schtasks.exe/at.exe
MSHTA.exe
reg.exe
wmic.exe
sc.exe
findstr.exe
whoami.exe
rundll32.exe
Checks
Command line
Encoded value (base64)
Non-Encrypted values
Checks
Identify connection related commands
Custom/malicious scripts and its path
Files/process Imports
Parent process
Child process
Start from "Identify the process type" section
Installed Applications
Process Details
Path
Product name
Version
Identify if the version is vulnerable (Based on version)
Signed/Unsigned
Hash value reputation
Reputation Score
Threat Category
Techniques Used
Processes in Unknown Paths
Process Details
Hash Value
Path
Identify nature of path
Command Line
Identify nature of activity -Malicious commands/Admin commands.
Detection Reason
Action by AV/EDR Etc
No. of Occurrence
Action type
Process Chain
Parent Process
Child Process
Start with "Process Details" section
Check
Connections
Hash/IP/Domain Reputation Check Sites
VirusTotal
Payload Security (Hybrid Analysis)
IBM X-Force
Any.Run
Bright Cloud
Destination IP Address (Domain Name)
Reputation Score
Threat Category
Threat History
Whois Details
Port
Source Port
Destination Port
Summary
No. of Hits on port
Service Used/Hosted
Status
Blocked/Allowed on Perimeter Devices
Proxy (if there are web connections)
Firewall
IDS/IPS
Bytes in & Bytes Out
Look for data exfiltration or data infiltration
No. of Hits
Presented with XMind