MOREnet

Be better connected.

EARLIER WARNINGS W/ TRIPWIRES

John Riley

Kevin Lim

Jim Long

WHAT ARE TRIPWIRES: HONEYFILES, HONEYDOCS, HONEYRECORDS, HONEYTOKENS

A honeyfile is a file that is designed to look like a real file on a server but contains bogus data. Honeyfiles are appealing targets for attackers. A honeyfile serves as a trap for attackers, and the data included within it can contain triggers that notify DLP solutions. Access to the files can also be tracked. A honeyrecord in a database is a honeyfile variant. These records serve the same purpose: they are forged and never utilized, but if they are ever copied, it indicates that there has been illicit activity.

The goal is generally to deploy them so no legitimate user would have reason to access them.

TRIPWIRES OR HONEY.....WHY.....WHO

Can be a “heads-up” to bad actors inside our networks and reduce “dwell time” of an initial compromise.

Inside - someone with too much access due to:

- poorly configured permissions.
- outdated job duties

Outside - Enemies - Bad actors

- compromised accounts, - phishing
- compromised machines - malware, viruses
- poor configurations - incorrect permissions, lack of security software,
- vulnerabilities - unpatched systems, zero days

TRIPWIRES: HONEY ACCOUNTS

- Honey Accounts: A good network honey account should mimic a real user account and look like a real person or organization. Use a real name, job title, or make it look like a shared account. Then change the available hours to 0, strong password, and log in once.

HONEY ACCOUNTS: USING GOOD BAIT

- Types of accounts
- admin's - default administration acct, admin's
- administration -supt, principal, director, cio and other high profile accounts
- accounting/HR = payroll manager, accountants, HR managers
- Old accounts - Director/ Supt move on? Use that account
- techs = it staff
- Service Accounts or Shared accounts = Powerschool admins, Printer admins, quickbook admins
-

TRIPWIRES/HONEY

- Honey Docs/files creation, names, placement

  PowerShell

  Canary Tokens

  software packages – Thinkst canary, rapid7

You may want to consider placing your honey files in alternate directories that users would not be expected to browse in Windows Explorer. You could also use a file extension that does not produce a file preview in Windows Explorer to avoid these false positive alerts.

HONEY DOCS/TOKENS: USING GOOD BAIT

Types of documents

- Passwords
- Payroll -W-2’s
- Human resources - Contracts, Proposals, PII, discipline records,
- Medical records
- SS#’s
- Financial documents - credit cards

WAYS TO SETUP TRIPWIRES

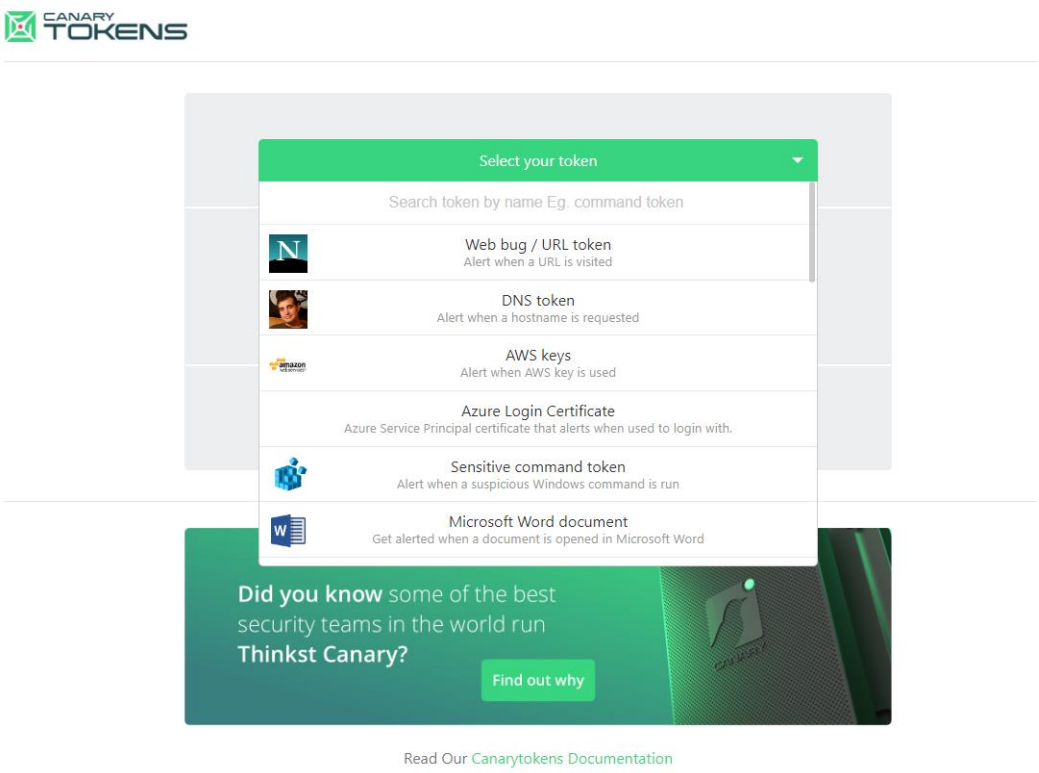
Canary Tokens - Use for files not great for event viewer(spam)

Windows auditing + PowerShell

other options:

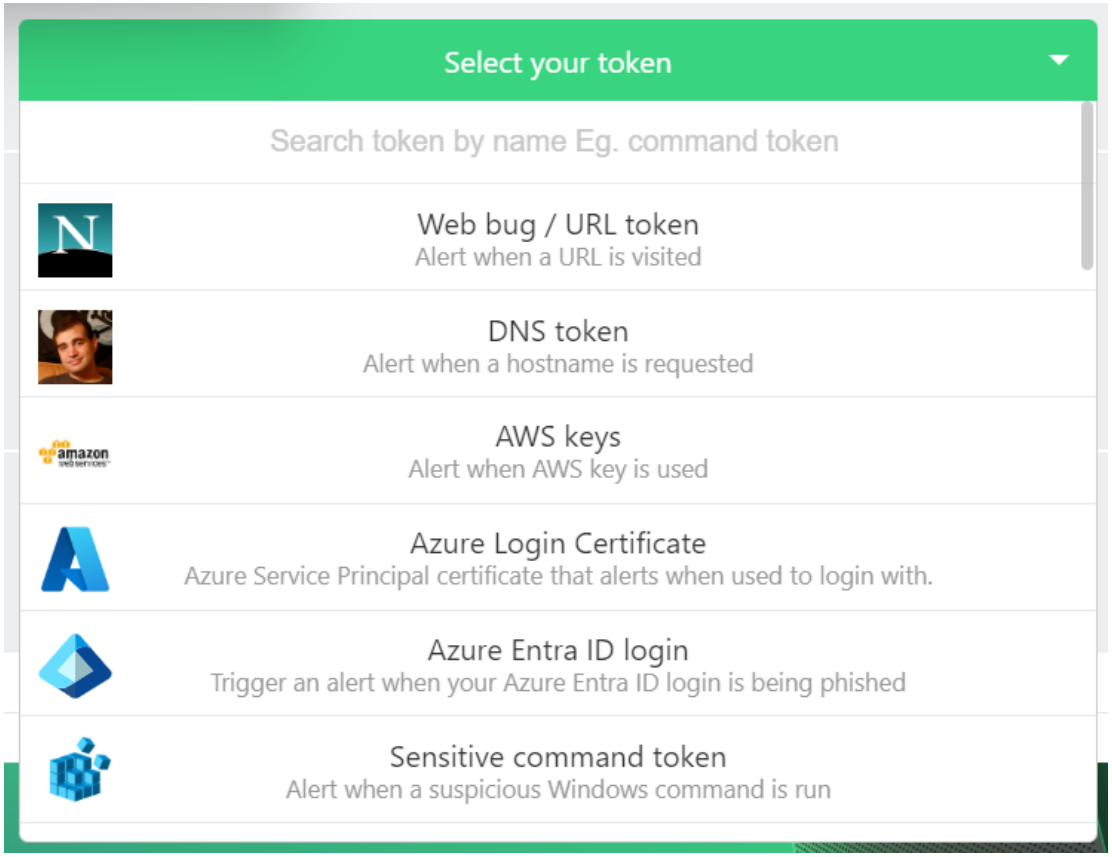
Active Directory management software. Rapid7 Insight Agent, (netrix.....AWS)

CANARY TOKENS - EASIEST TO SET UP



Be better connected.

TYPES OF CANARY TOKENS

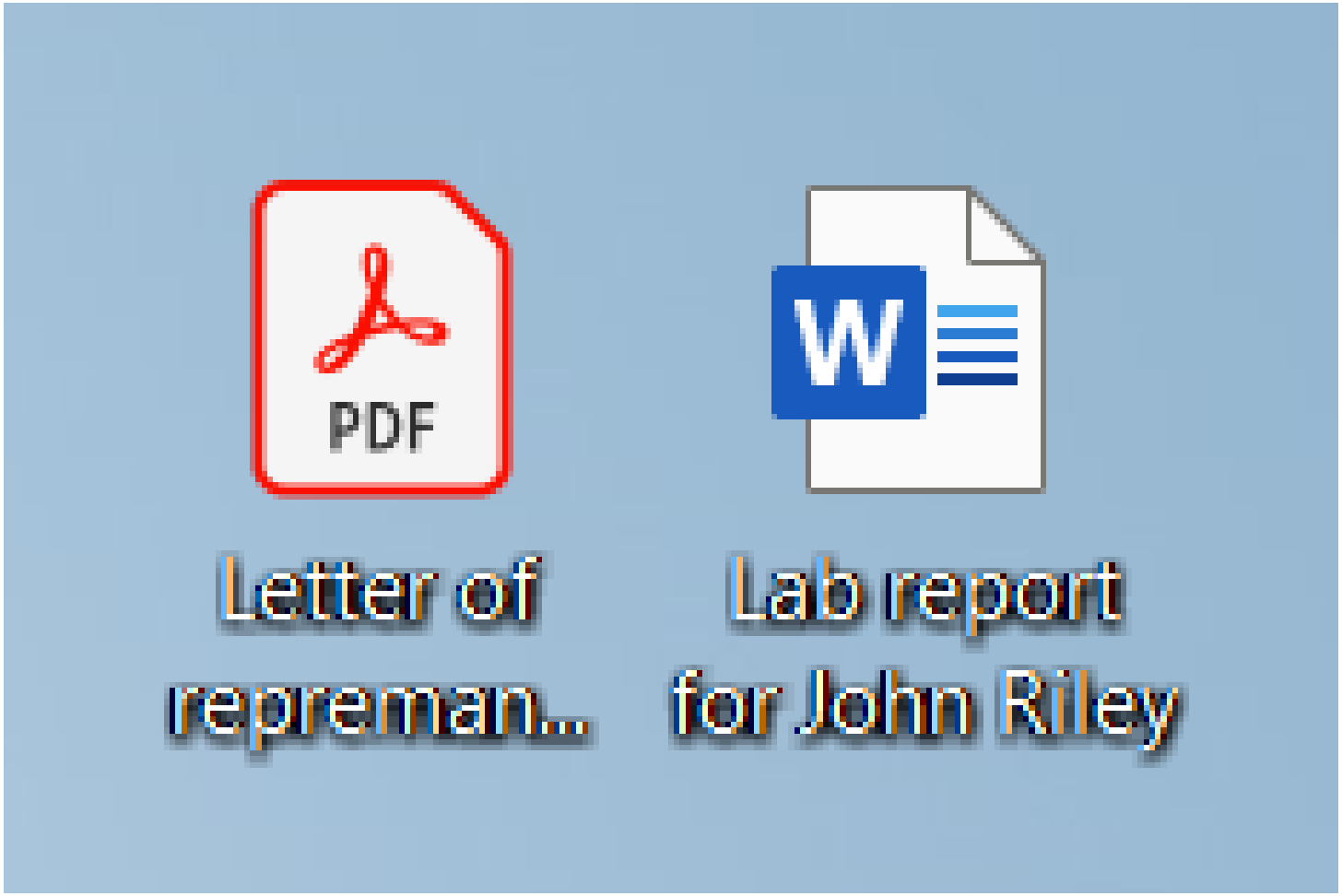


Be better connected.

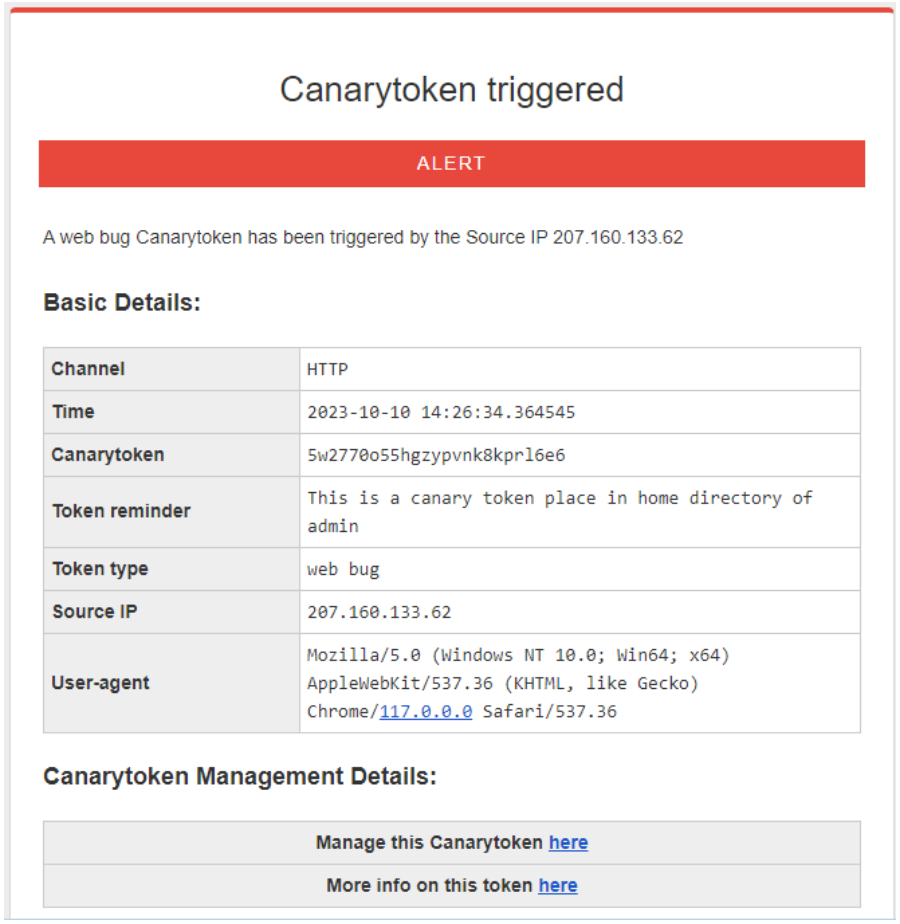
WEB BUGS

- Web Bug - native
- http://canarytokens.com/articles/feedback/terms/mlqvvipn3jrbeqxh7mkv3pdhd/payments.js

WORD DOCS AND PDF'S



CANARYTOKEN TRIGGERED



Canarytoken triggered

ALERT

A web bug Canarytoken has been triggered by the Source IP 207.160.133.62

Basic Details:

Channel	HTTP
Time	2023-10-10 14:26:34.364545
Canarytoken	5w2770o55hgzypvnk8kprl6e6
Token reminder	This is a canary token place in home directory of admin
Token type	web bug
Source IP	207.160.133.62
User-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

Be better connected.

TYPES OF CANARY TOKENS

Web bug/URL token Put in an email with a juicy subject line. Or Embedded in documents Or link to image file

DNS token

AWS Keys

Azure Login Certificate

Sensitive Command Token executables often used by attackers but seldom used by regular users (e.g., whoami.exe, net.exe, wmic.exe, etc.). or attacker tools that are not present on your system (e.g., mimikatz.exe), Ne ed to use in a network management tool to deploy across your organization

Microsoft Word Document Leave the file on a web server in an inaccessible directory, to detect webserver breaches. Attach to an email with a tempting Subject line.

Be better connected.

CANARY TOKENS

Pro’s

- easy to setup and deploy

Con’s

The doc file has to open with word

It triggers a dns query

web bugs should be shortened to disguise the url

May need path to run w/ admin credentials

MOREnet

Be better connected.

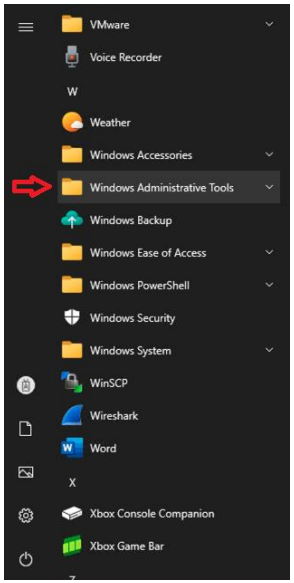
POWERSHELL MONITORING EXAMPLE CONFIGURATION

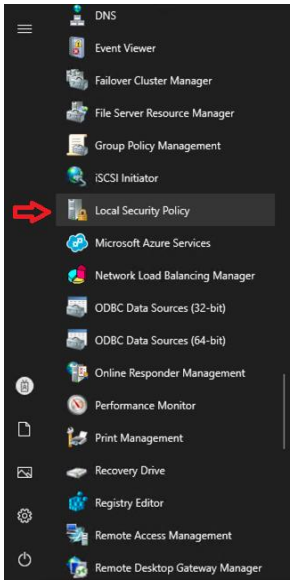
MONITORING REQUIREMENTS

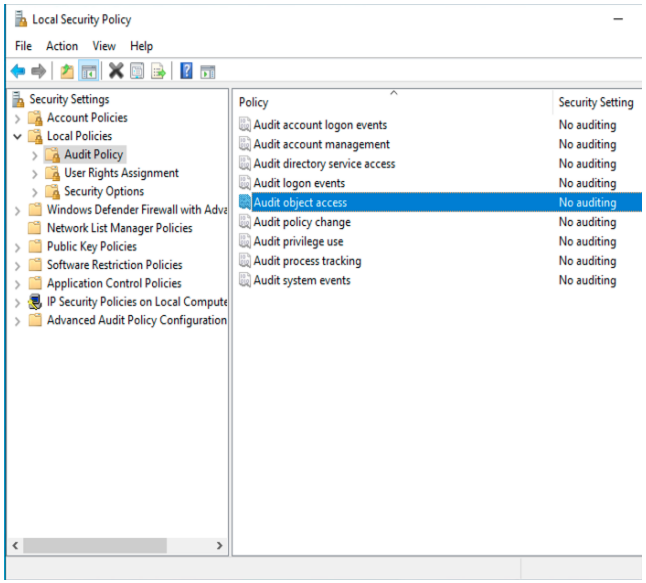
- PowerShell scripts are available through the link on slide 24
- Create directory "c:\batchfiles" and place the below files to it
  - acct-access.ps1
  - file-access.ps1
  - psbypass.bat.txt - change filename to psbypass.bat
- SMTP Relay
  - The script requires an SMTP Relay to send alert emails
  - Google Workspace includes access to a SMTP Relay

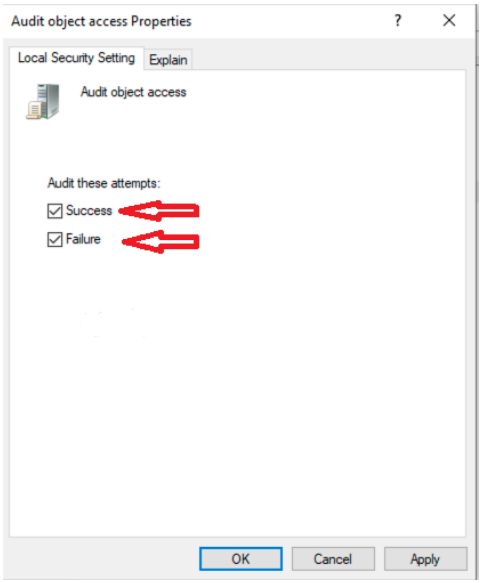
FILE MONITORING CONFIGURATION

- Enable Audit Policy





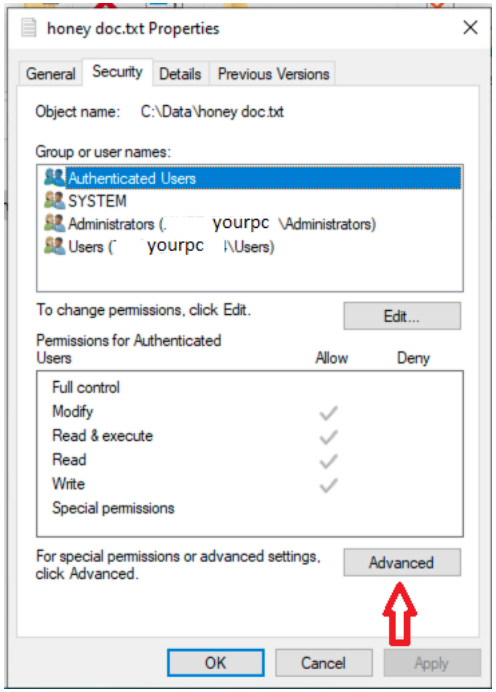


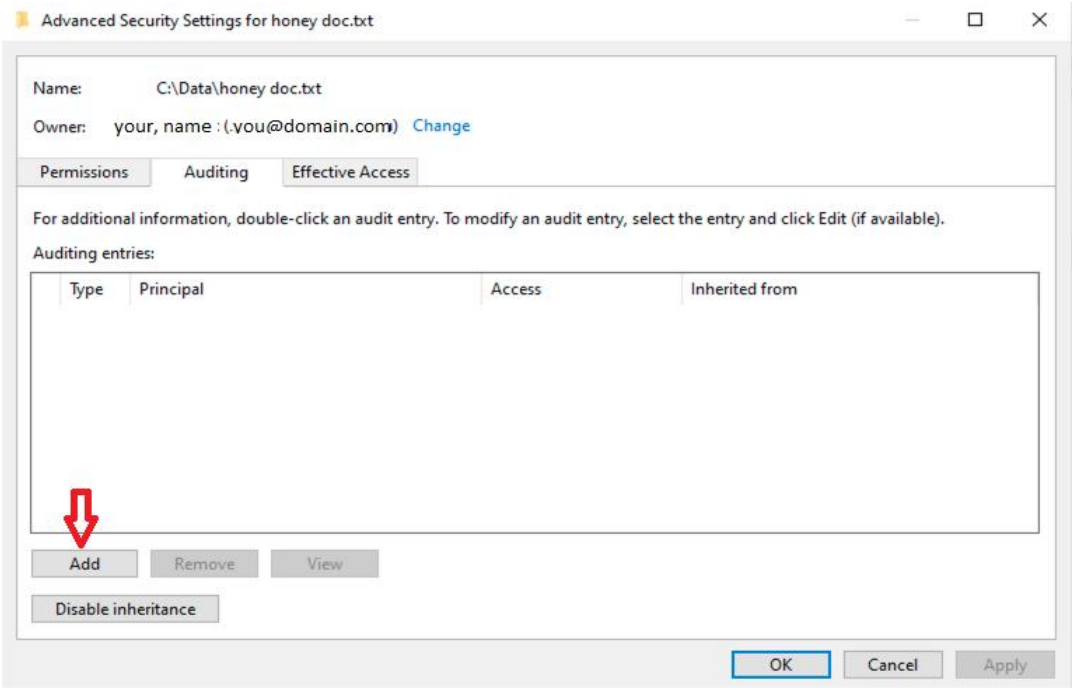


Be better connected.

FILE MONITORING CONFIGURATION

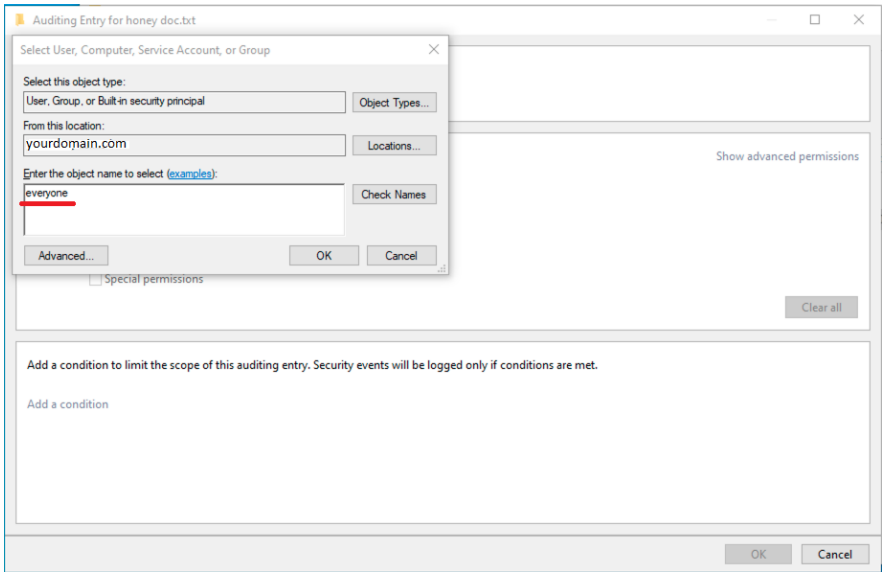
- Configure Auditing for honey file

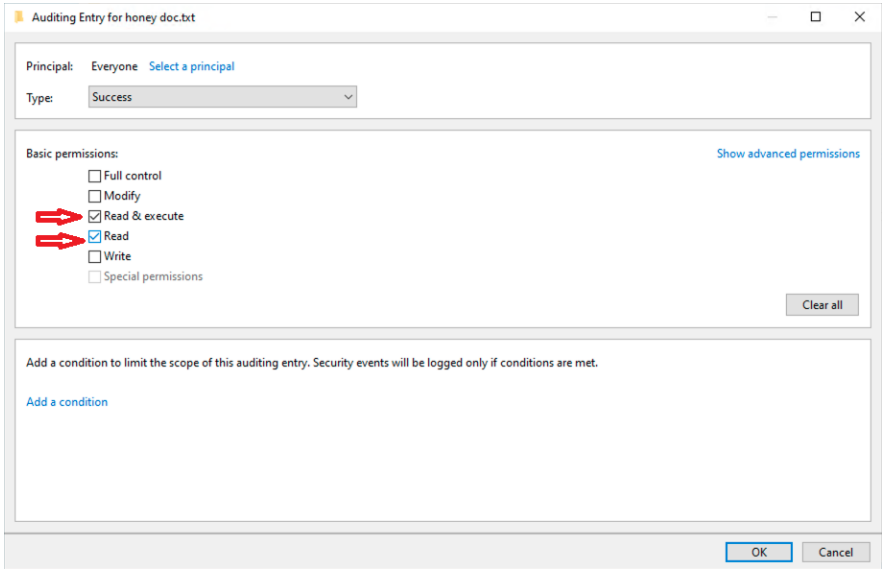




Be better connected.

FILE MONITORING CONFIGURATION





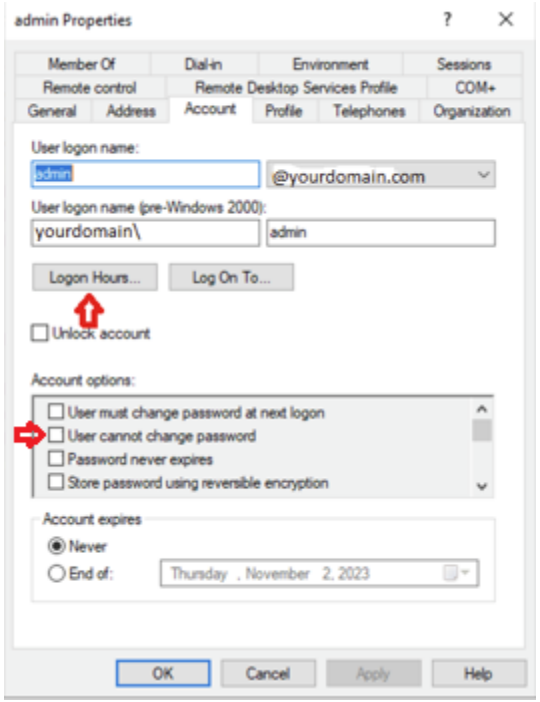
Be better connected.

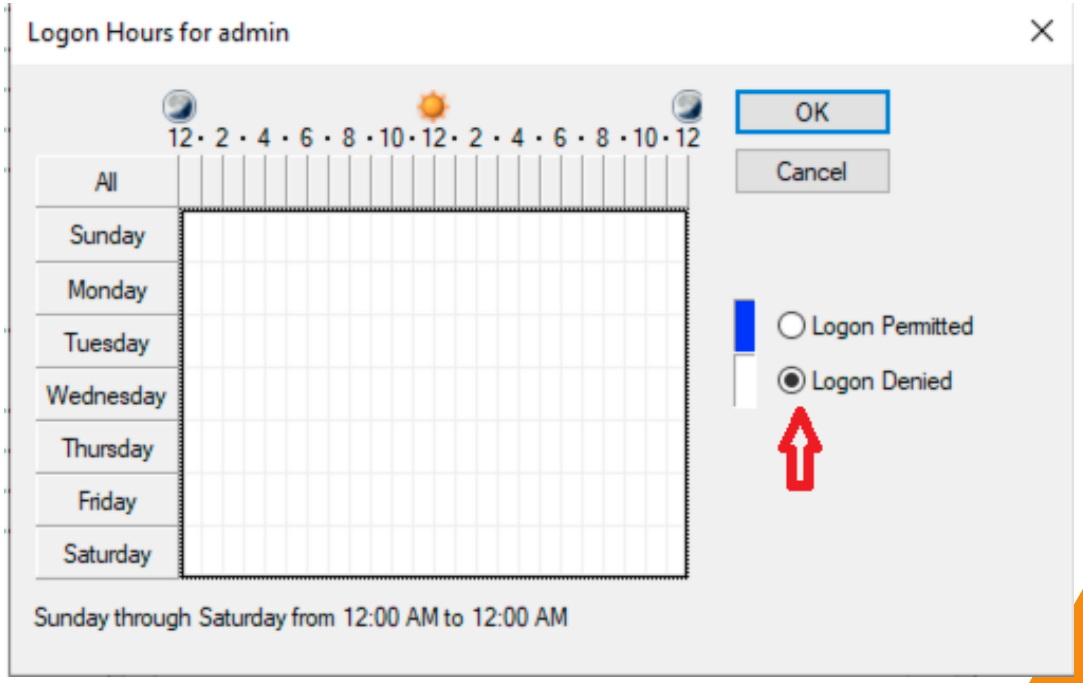
FILE MONITOR CONFIGURATION

- Configure Script Variables – file-access.ps1
  - $Log = "Security" - Windows log that the script runs against
  - $eventid = 4663 - Event ID that is filtered for
  - $msg = "ReadData" - Filtered event subject - in this case "file read"
  - $FileName = "c:\temp\file-access.txt" - Event file summary
  - $PSEmailServer = "smtprelay.domain.net" - SMTP relay server
  - $mailto = "youremail.domain.net" - Alert email recipient
  - $hfile = "super-cool-info.txt" - Name of honeyfile

ACCOUNT MONITORING CONFIGURATION

- Set logon hours to created honey-account in ADUC



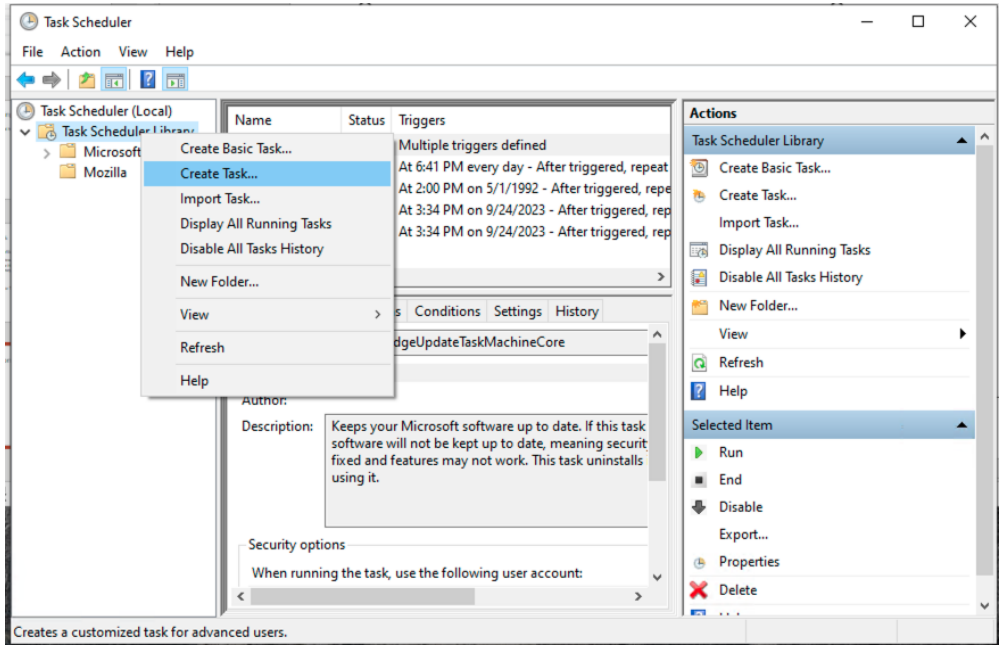


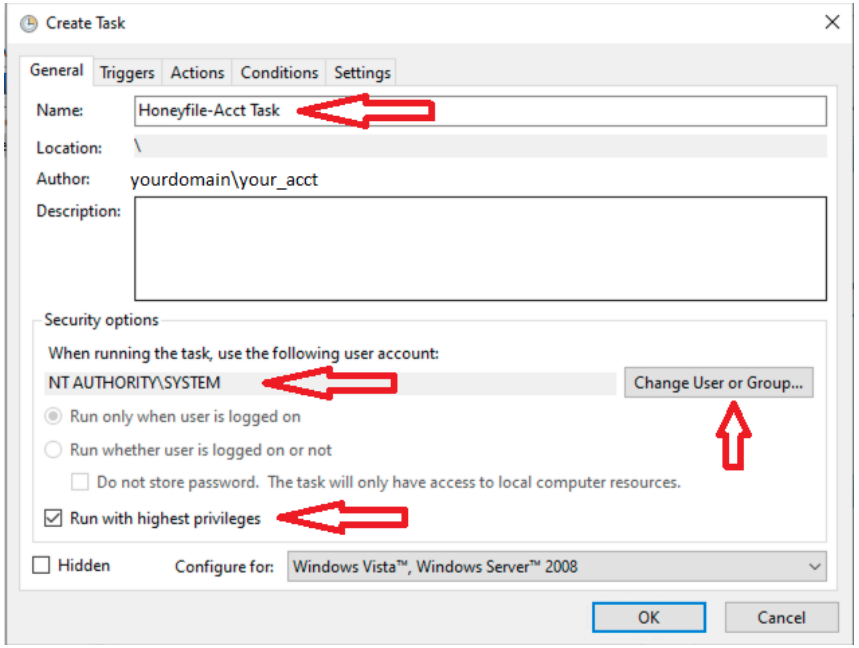
Be better connected.

ACCOUNT MONITOR CONFIGURATION

- Configure Script Variables – acct-access.ps1
  - $Log = "Security" - Windows log that the script runs against
  - $eventid = 4625 - Event ID that is filtered for
  - $msg = "admin" - Filtered event subject - in this case we are monitoring the "admin" account
  - $FileName = "c:\temp\acct-access.txt" - Event file summary
  - $PSEmailServer = "smtprelay.domain.net" - SMTP relay server
  - $mailto = "youremail.domain.net" - Alert email recipient

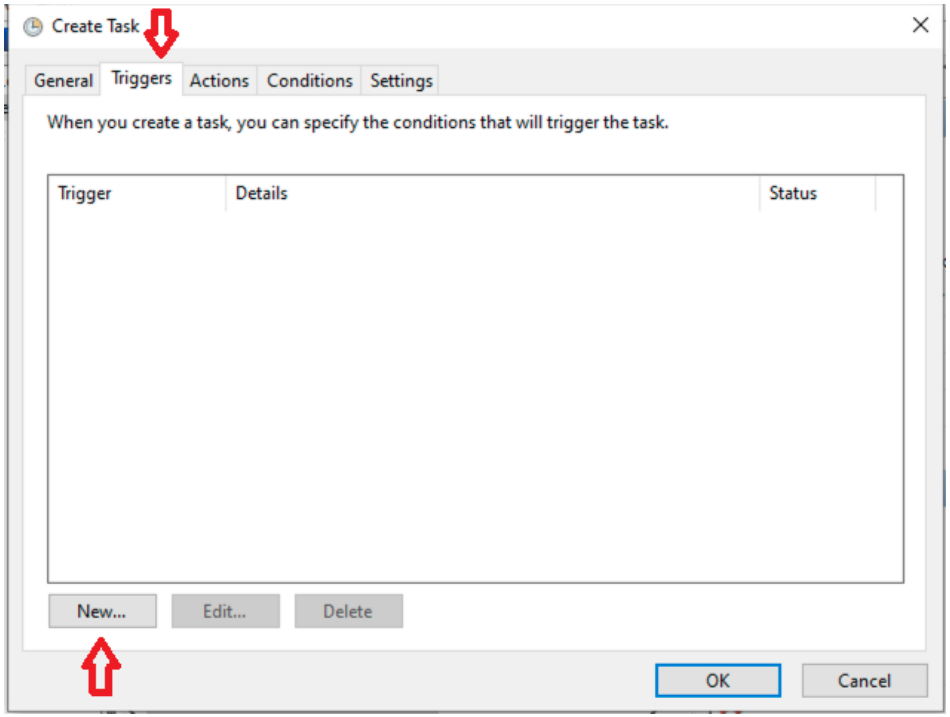
TASK SCHEDULER CONFIGURATION

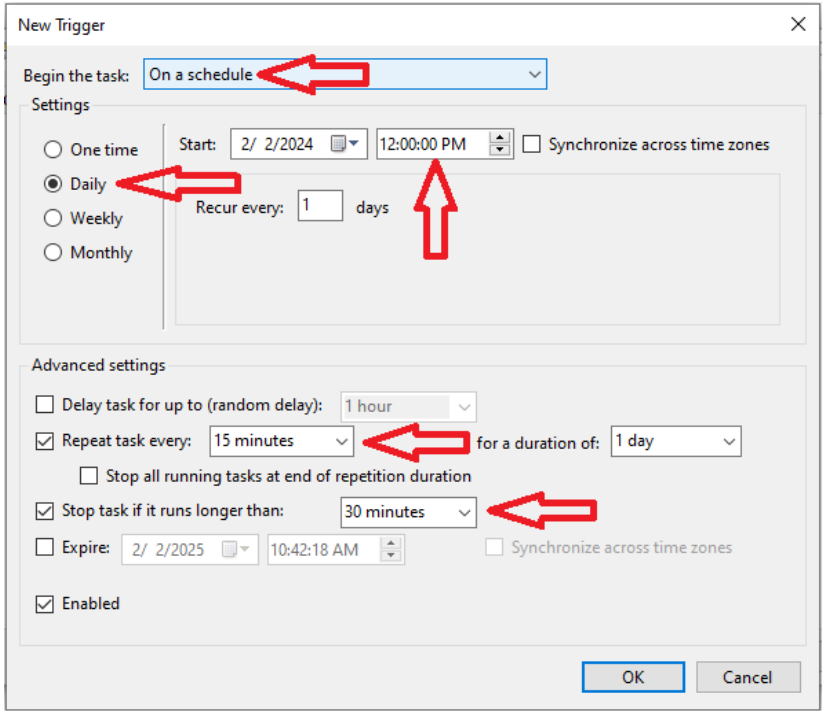




Be better connected.

TASK SCHEDULER CONFIGURATION

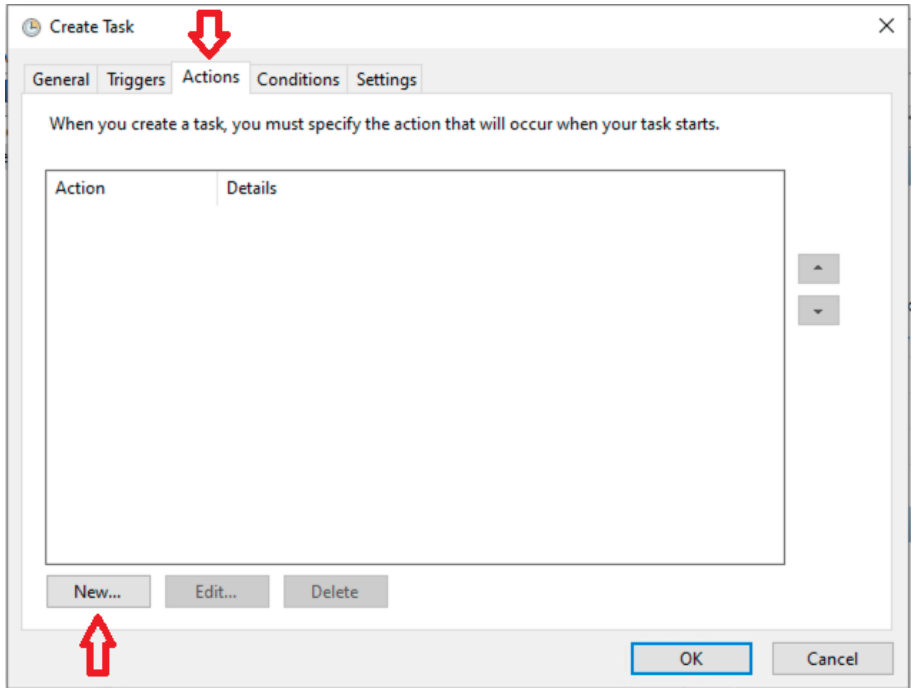


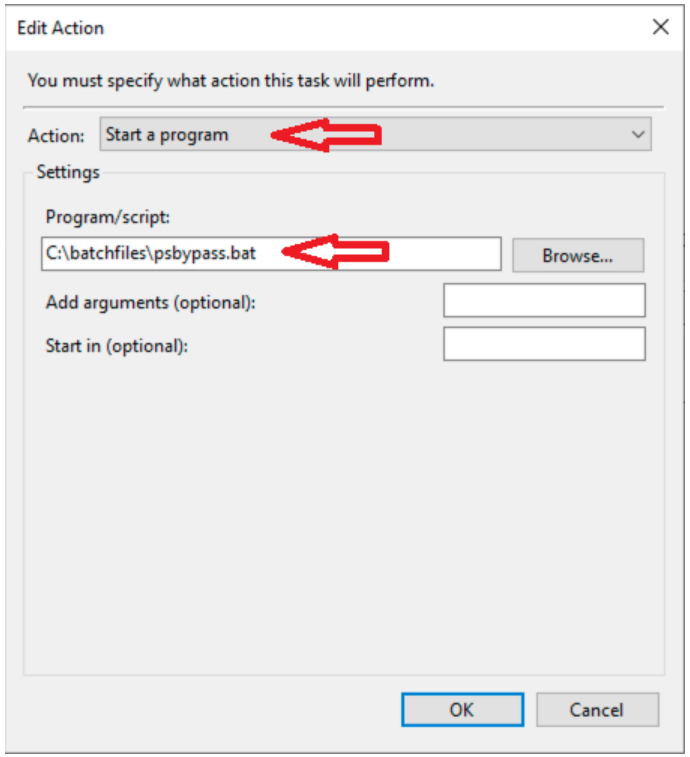


- Adjust task frequency that works for your case
- Start with a 15 min interval and adjust as needed
- Give task enough time to complete before the task runs again
- Some logs are very large and could take longer to for the script to parse

Be better connected.

TASK SCHEDULER CONFIGURATION





- Running the PowerShell scripts within a batch file is simpler than configuring Task Scheduler to run a standalone PowerShell script
- The batch file also sets the PowerShell Execution Policy to allow scripts to run and then resets it back to "Restricted" when the task completes

QUESTIONS?

rileyjr@more.net
kevinl@more.net
long@more.net

Link to the scripts:
http://bit.ly/45svdk0

Be better connected.

THANK YOU FOR COMING!