Deloitte.

nuix

# It’s What’s Inside That Counts

Transforming Investigations to Detect and Prevent Insider Threat

175 MAKING AN IMPACT THAT MATTERS since 1845

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Intro

### Speakers

Armando Nardo

*Forensic Technology | Director – Digital Forensics*

Contact Information

☎ +44 20 7303 5791

✉ anardo@deloitte.co.uk

Tom Coppock

*Forensic Technology | Manager – Digital Forensics*

Contact Information

☎ +44 20 7007 6153

✉ tcoppock@deloitte.co.uk

Hoke Smith

*Nuix | VP, Cybersecurity*

Contact Information

☎ +1 571 446 2165

✉ hoke.smith@nuix.com

### Agenda

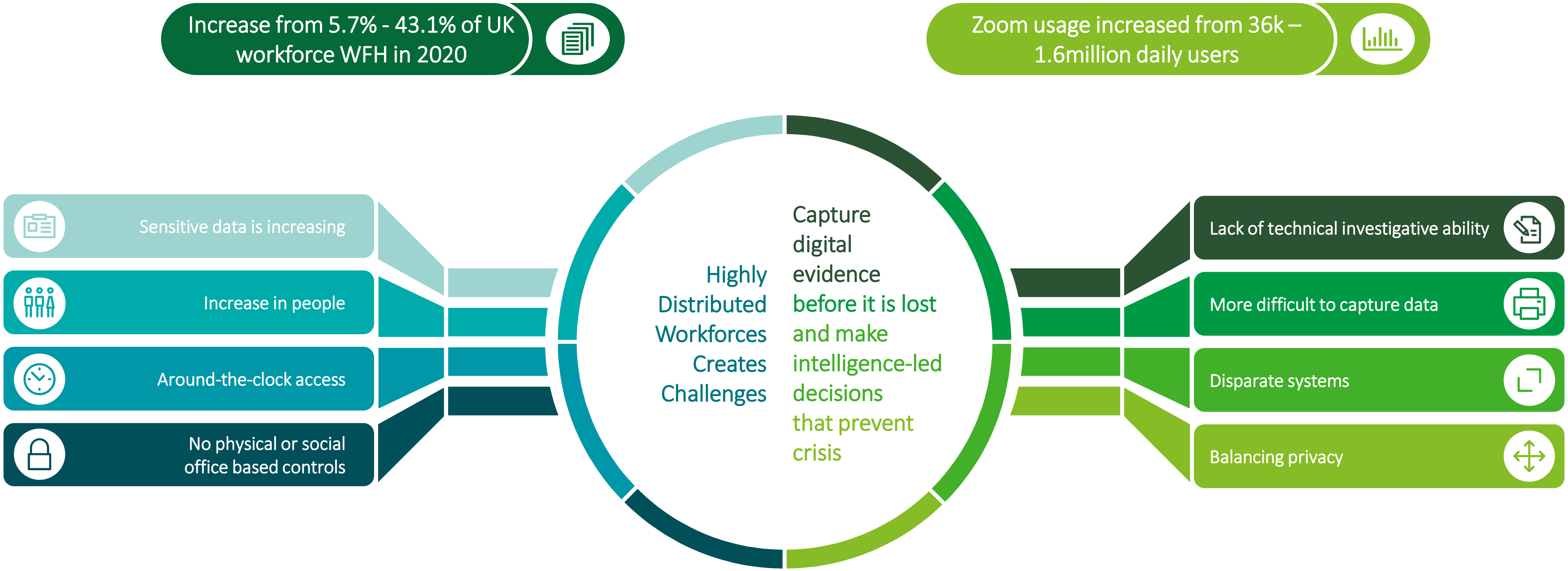
- Challenges
- Overview of Nuix Adaptive Security
- Walkthrough of scenarios
- Summary and questions

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidata non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

# Challenges

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Challenges



Increase from 5.7% - 43.1% of UK workforce WFH in 2020

Zoom usage increased from 36k – 1.6million daily users

Sensitive data is increasing

Increase in people

Around-the-clock access

No physical or social office based controls

Highly Distributed Workforces Creates Challenges

Capture digital evidence before it is lost and make intelligence-led decisions that prevent crisis

Lack of technical investigative ability

More difficult to capture data

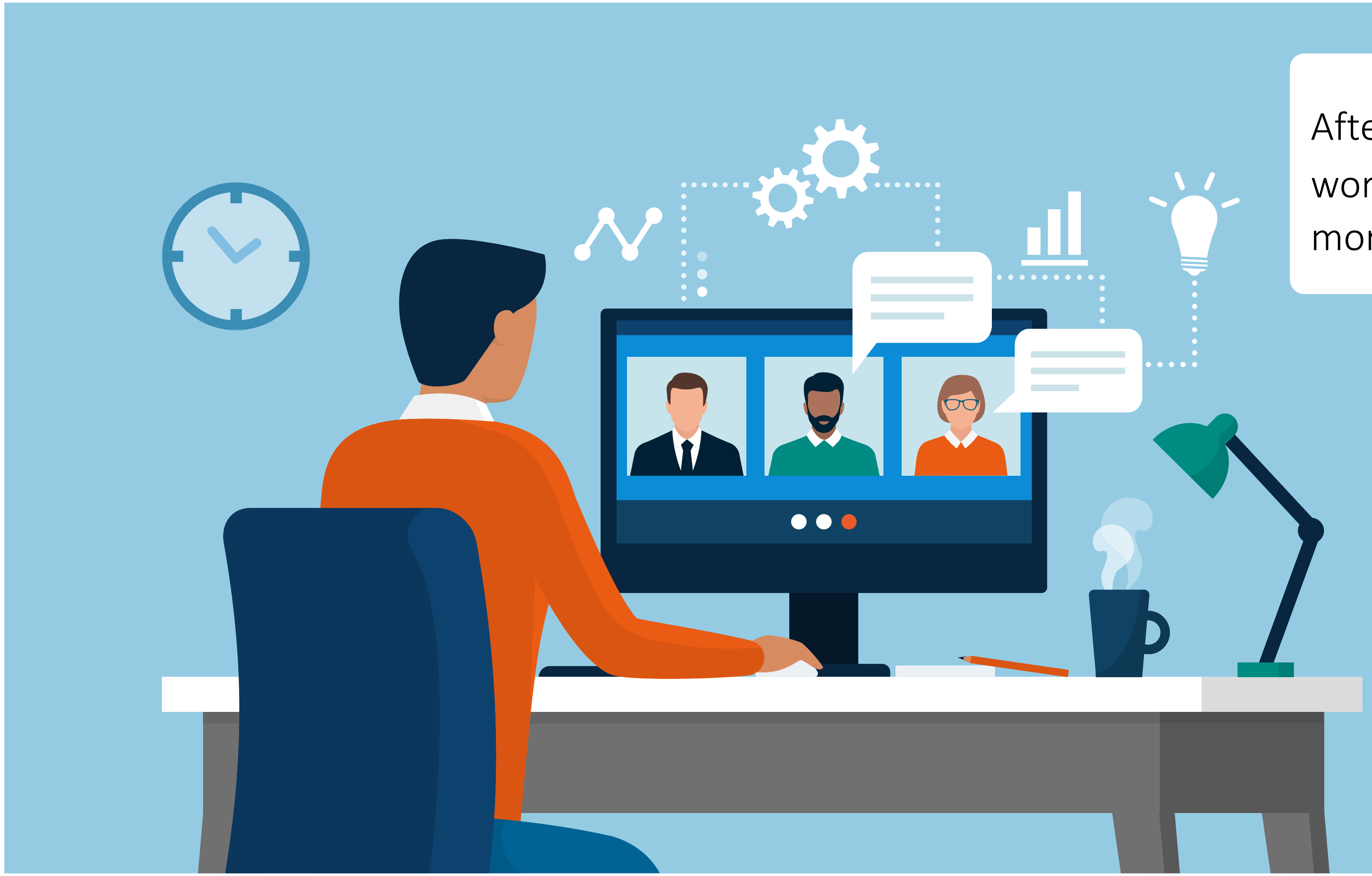
Disparate systems

Balancing privacy

https://wiserd.ac.uk/sites/default/files/documents/Homeworking%20in%20the%20UK_Report_Final_3.pdf
https://www.statista.com/statistics/1118860/zoom-daily-active-users-uk

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Is remote working here to stay?

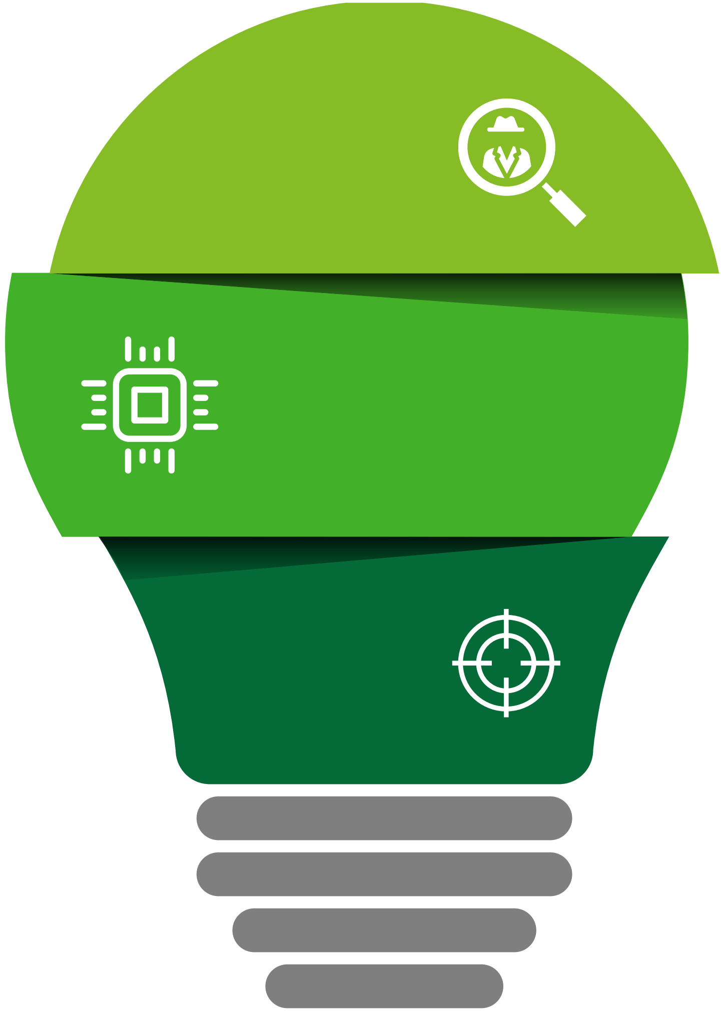


After lockdown **61%** of desk-based workers would prefer to work from home more often

Research was carried out by Ipsos MORI on behalf of Deloitte LLP. It screened a nationally representative quota sample of 2,213 UK adults, filtered to a sample of 1,321 workers aged 16-75, using its Online Omnibus.
https://www2.deloitte.com/uk/en/pages/consulting/articles/working-during-lockdown-impact-of-covid-19-on-productivity-and-wellbeing.html

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

Using technology to address some of our challenges



Enhance your **investigative agility** by combining monitoring with advanced triage in one unified platform. **Drive confidence and reduce effort.**

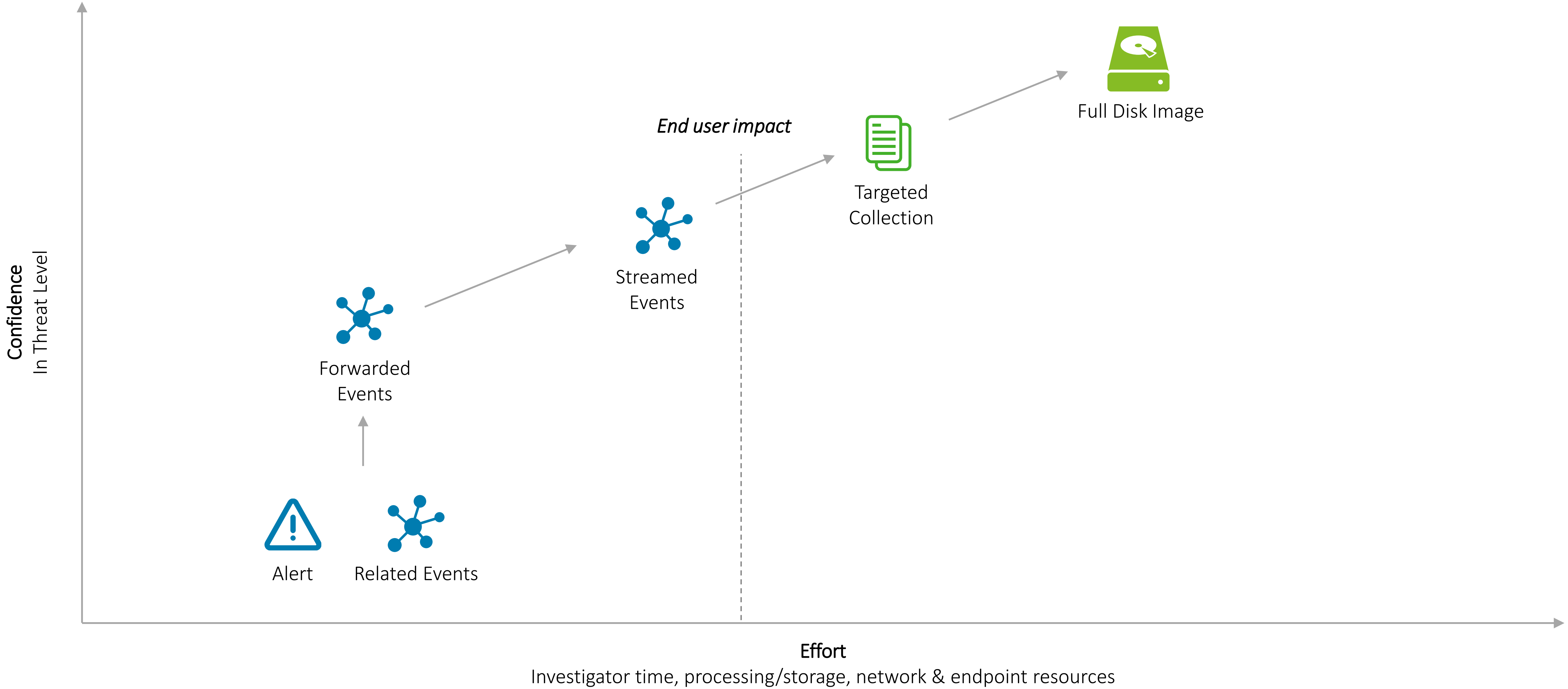
Use endpoint based technology **that monitor both user and system behaviour**, regardless of location, in real-time.

Being able to have a **targeted and bespoke approach** to specific issues, **reduce false-positives** and **over-collection of data** while speeding up detection.

©2021 Deloitte LLP - Private and Confidential

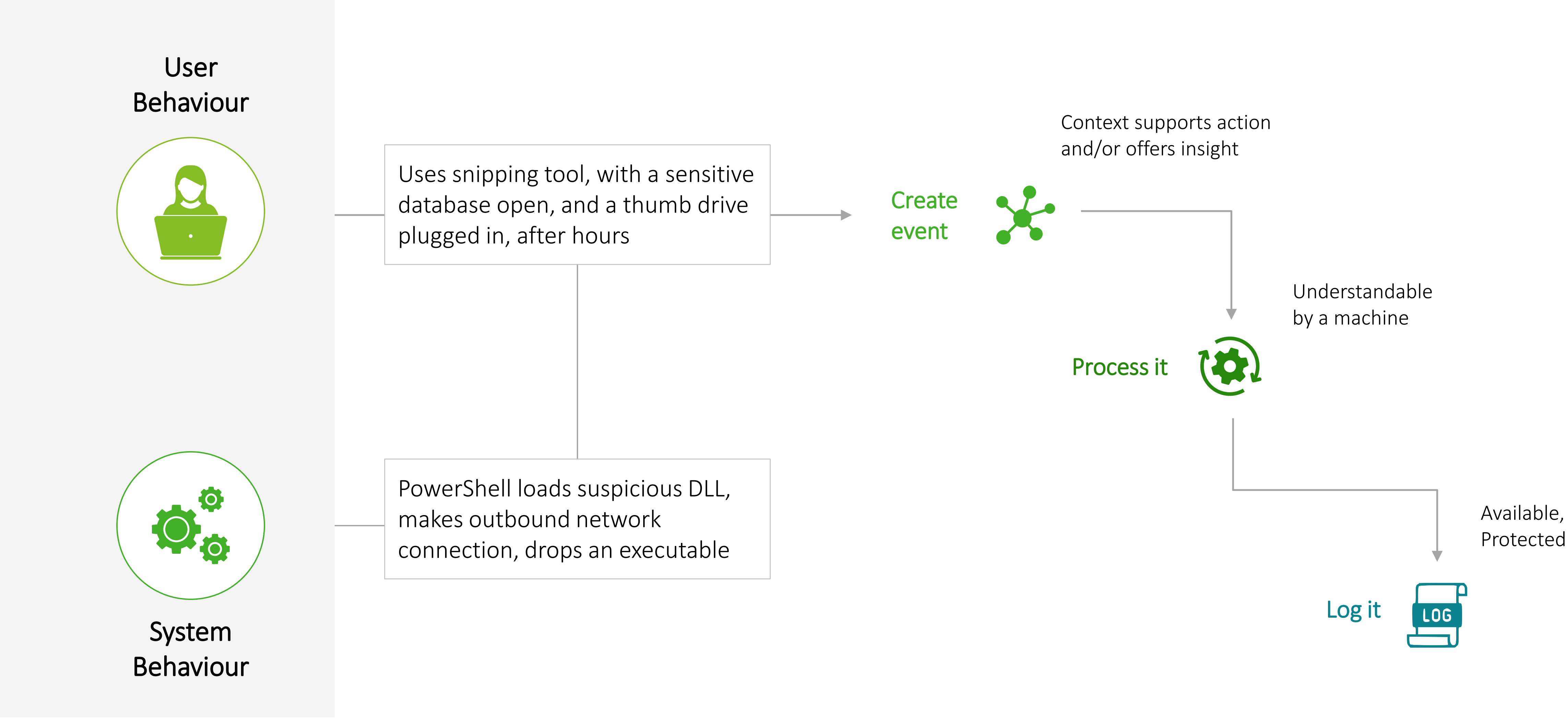
# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Investigative agility



# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Event-based detection and triage



User Behaviour

Uses snipping tool, with a sensitive database open, and a thumb drive plugged in, after hours

System Behaviour

PowerShell loads suspicious DLL, makes outbound network connection, drops an executable

Create event

Context supports action and/or offers insight

Process it

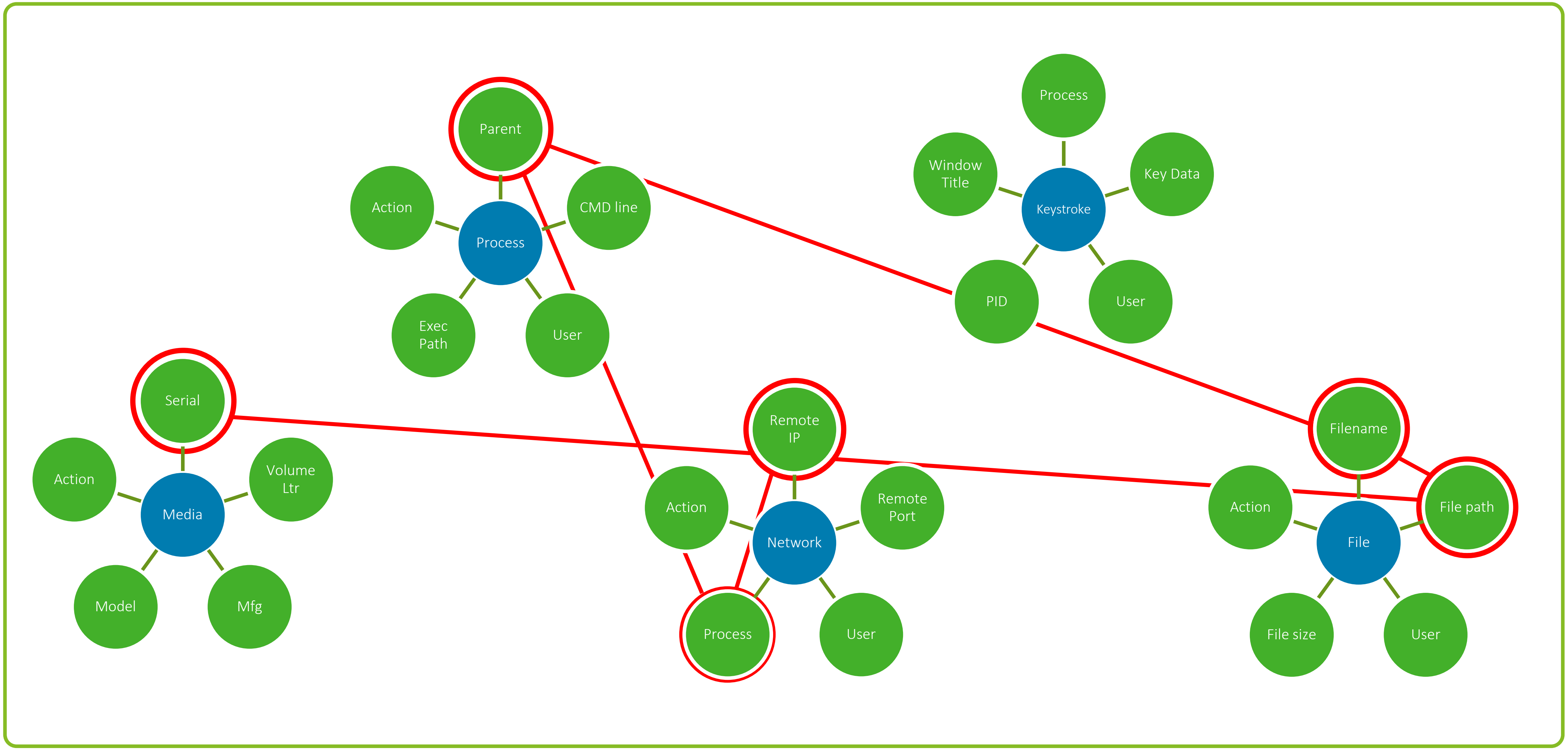
Understandable by a machine

Log it

Available, Protected

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## What is an event?



# Product Overview

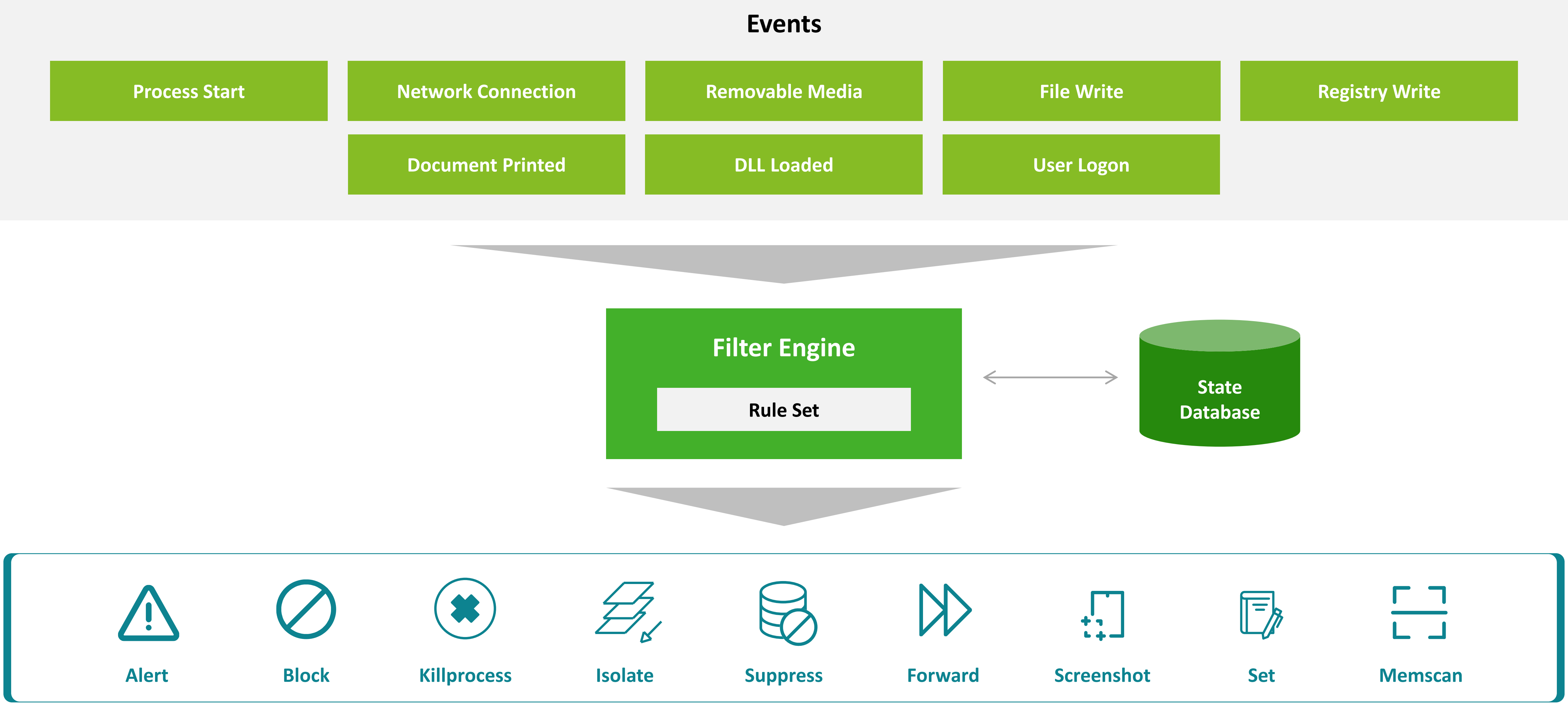
# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Product Overview – Nuix Adaptive Security

- Bespoke rule creating process to mould to your business needs and environments.
- Lightweight agent deployed on the network stores events and sends alerts back to server.
- Offline endpoints log events and alerts locally, reconnecting at next opportunity.
- Keyword searching of endpoints on the fly.
- Record screenshots, keylogs and clipboard information from endpoints and alert when certain conditions are met:
  - Keyword is met
  - Data copied onto a USB.
  - User logs in remotely, then attempts to upload data.
- Isolate endpoints that you believe to have been compromised (insider/external threats).

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

Nuix Adaptive Security



©2021 Deloitte LLP - Private and Confidential

# Scenario 1 - Data Theft and Disclosure

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 1 – Data Theft and Disclosure

### Sell sensitive research to a competitor

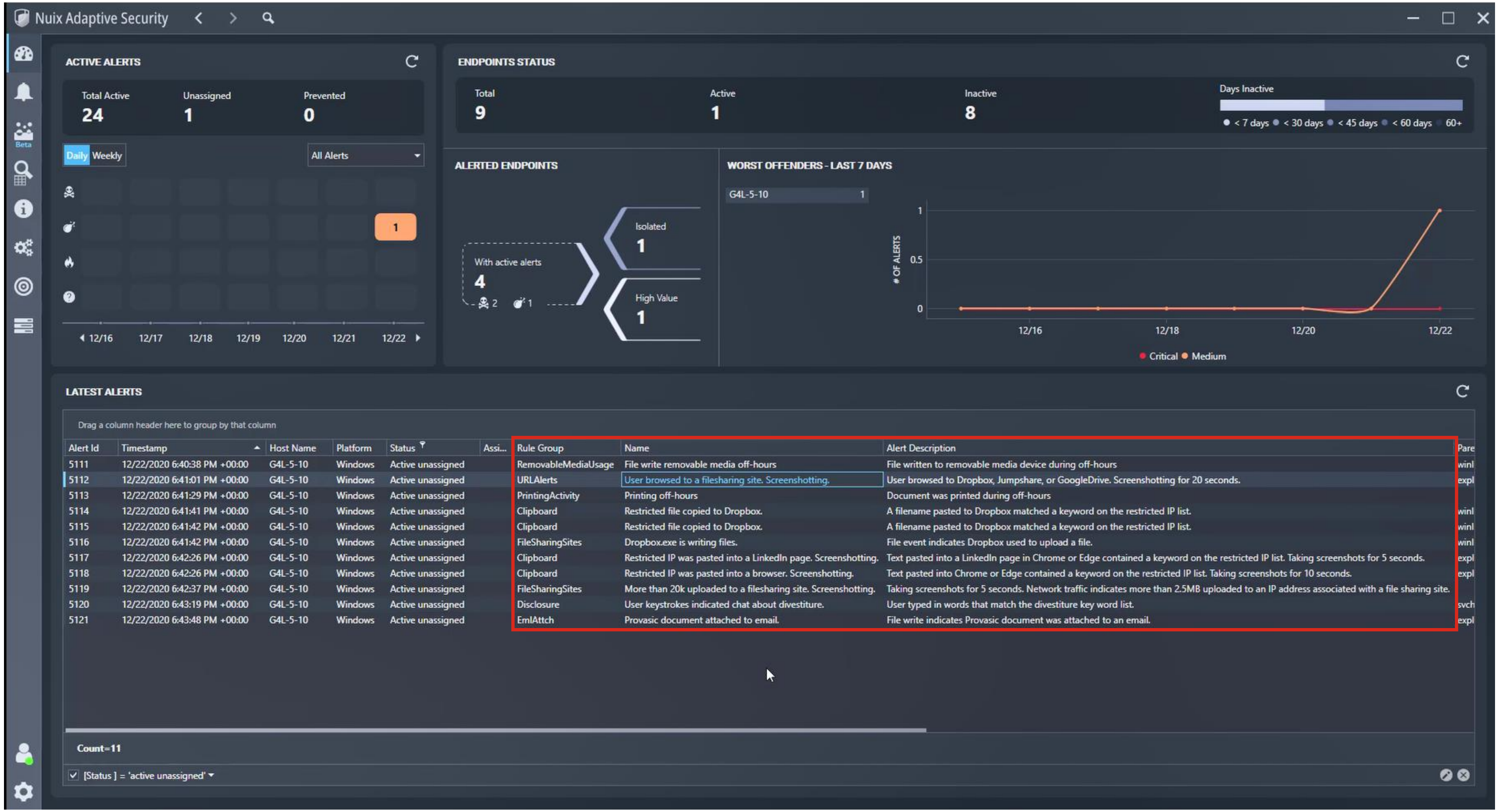
- Acquires report
- Pastes some of the data into a chat window
- Copies to removable media
- Uploads to a file sharing service via browser
- Uploads to a file sharing service via local client
- Prints it

### Discuss a sensitive transaction before it closes

- Mentions transaction in chat
- Attaches document to email

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 1 – Data Theft and Disclosure



ACTIVE ALERTS

Total Active 24
Unassigned 1
Prevented 0

ENDPOINTS STATUS

Total 9
Active 1
Inactive 8

ALERTED ENDPOINTS

WORST OFFENDERS - LAST 7 DAYS

LATEST ALERTS

Drag a column header here to group by that column

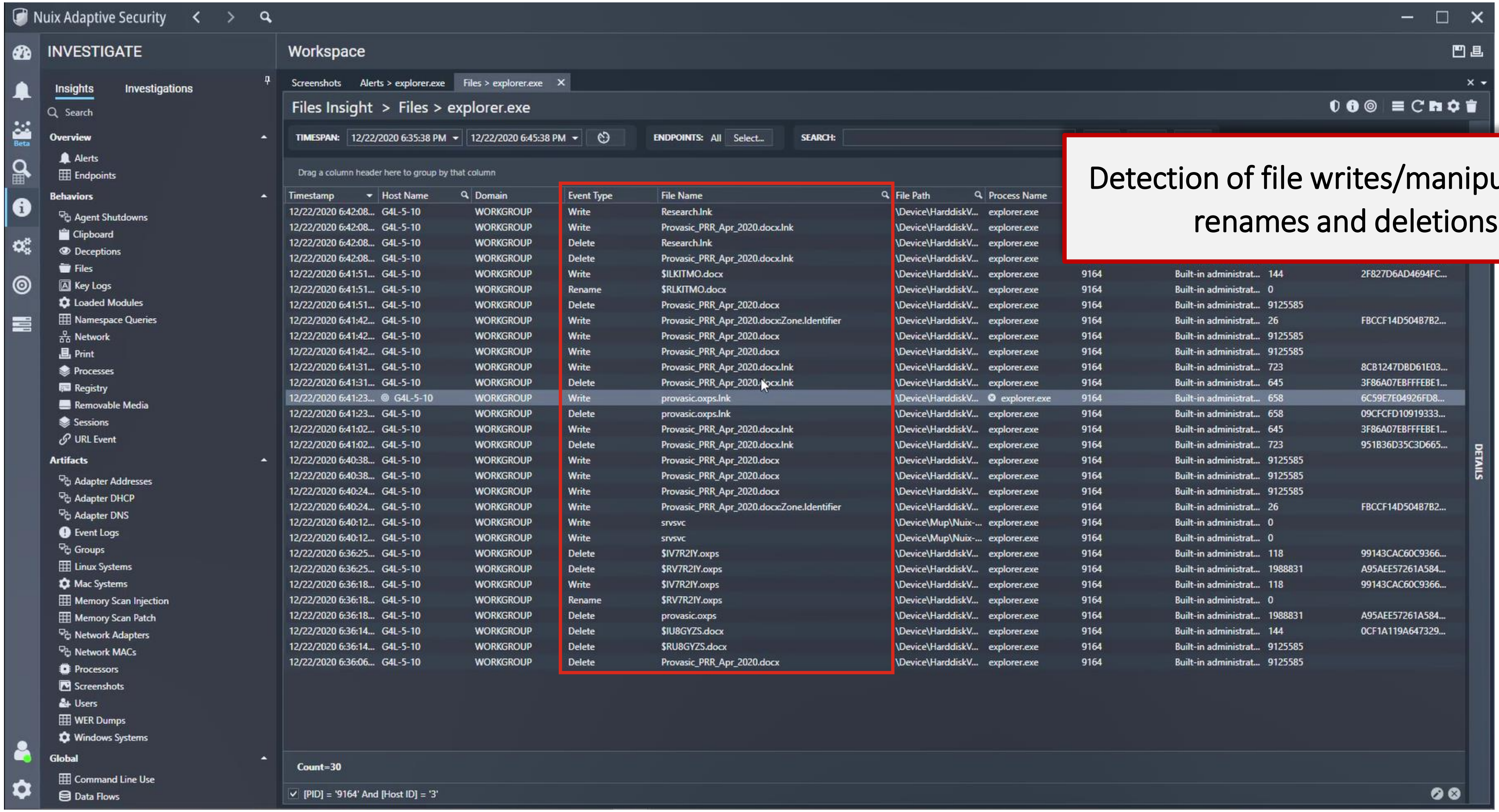
| Alert Id | Timestamp | Host Name | Platform | Status | Assi... | Rule Group | Name | Alert Description | Pare |
|---|---|---|---|---|---|---|---|---|---|
| 5111 | 12/22/2020 6:40:38 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | RemovableMediaUsage | File write removable media off-hours | File written to removable media device during off-hours | winl |
| 5112 | 12/22/2020 6:41:01 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | URLAlerts | User browsed to a filesharing site. Screenshotting. | User browsed to Dropbox, Jumpshare, or GoogleDrive. Screenshotting for 20 seconds. | expl |
| 5113 | 12/22/2020 6:41:29 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | PrintingActivity | Printing off-hours | Document was printed during off-hours |  |
| 5114 | 12/22/2020 6:41:41 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | Clipboard | Restricted file copied to Dropbox. | A filename pasted to Dropbox matched a keyword on the restricted IP list. | winl |
| 5115 | 12/22/2020 6:41:42 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | Clipboard | Restricted file copied to Dropbox. | A filename pasted to Dropbox matched a keyword on the restricted IP list. | winl |
| 5116 | 12/22/2020 6:41:42 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | FileSharingSites | Dropbox.exe is writing files. | File event indicates Dropbox used to upload a file. | winl |
| 5117 | 12/22/2020 6:42:26 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | Clipboard | Restricted IP was pasted into a LinkedIn page. Screenshotting. | Text pasted into a LinkedIn page in Chrome or Edge contained a keyword on the restricted IP list. Taking screenshots for 5 seconds. | expl |
| 5118 | 12/22/2020 6:42:26 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | Clipboard | Restricted IP was pasted into a browser. Screenshotting. | Text pasted into Chrome or Edge contained a keyword on the restricted IP list. Taking screenshots for 10 seconds. | expl |
| 5119 | 12/22/2020 6:42:37 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | FileSharingSites | More than 20k uploaded to a filesharing site. Screenshotting. | Taking screenshots for 5 seconds. Network traffic indicates more than 2.5MB uploaded to an IP address associated with a file sharing site. |  |
| 5120 | 12/22/2020 6:43:19 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | Disclosure | User keystrokes indicated chat about divestiture. | User typed in words that match the divestiture key word list. | svch |
| 5121 | 12/22/2020 6:43:48 PM +00:00 | G4L-5-10 | Windows | Active unassigned |  | EmlAttch | Provasic document attached to email. | File write indicates Provasic document was attached to an email. | expl |

Count=11

☑ [Status ] = 'active unassigned'

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 1 – Data Theft and Disclosure



Files Insight > Files > explorer.exe

TIMESPAN: 12/22/2020 6:35:38 PM – 12/22/2020 6:45:38 PM  ENDPOINTS: All Select...  SEARCH:

Drag a column header here to group by that column

| Timestamp | Host Name | Domain | Event Type | File Name | File Path | Process Name | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 12/22/2020 6:42:08... | G4L-5-10 | WORKGROUP | Write | Research.lnk | \Device\HarddiskV... | explorer.exe | | | | |
| 12/22/2020 6:42:08... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx.lnk | \Device\HarddiskV... | explorer.exe | | | | |
| 12/22/2020 6:42:08... | G4L-5-10 | WORKGROUP | Delete | Research.lnk | \Device\HarddiskV... | explorer.exe | | | | |
| 12/22/2020 6:42:08... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx.lnk | \Device\HarddiskV... | explorer.exe | | | | |
| 12/22/2020 6:41:51... | G4L-5-10 | WORKGROUP | Write | $ILKITMO.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 144 | 2F827D6AD4694FC... |
| 12/22/2020 6:41:51... | G4L-5-10 | WORKGROUP | Rename | $RLKITMO.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 0 | |
| 12/22/2020 6:41:51... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 9125585 | |
| 12/22/2020 6:41:42... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx:Zone.Identifier | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 26 | FBCCF14D504B7B2... |
| 12/22/2020 6:41:42... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 9125585 | |
| 12/22/2020 6:41:42... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 9125585 | |
| 12/22/2020 6:41:31... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx.lnk | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 723 | 8CB1247DBD61E03... |
| 12/22/2020 6:41:31... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx.lnk | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 645 | 3F86A07EBFFFEBE1... |
| 12/22/2020 6:41:23... | G4L-5-10 | WORKGROUP | Write | provasic.oxps.lnk | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 658 | 6C59E7E04926FD8... |
| 12/22/2020 6:41:23... | G4L-5-10 | WORKGROUP | Delete | provasic.oxps.lnk | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 658 | 09CFCFD10919333... |
| 12/22/2020 6:41:02... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx.lnk | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 645 | 3F86A07EBFFFEBE1... |
| 12/22/2020 6:41:02... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx.lnk | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 723 | 951B36D35C3D665... |
| 12/22/2020 6:40:38... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 9125585 | |
| 12/22/2020 6:40:38... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 9125585 | |
| 12/22/2020 6:40:24... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 9125585 | |
| 12/22/2020 6:40:24... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx:Zone.Identifier | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 26 | FBCCF14D504B7B2... |
| 12/22/2020 6:40:12... | G4L-5-10 | WORKGROUP | Write | srvsvc | \Device\Mup\Nuix-... | explorer.exe | 9164 | Built-in administrat... | 0 | |
| 12/22/2020 6:40:12... | G4L-5-10 | WORKGROUP | Write | srvsvc | \Device\Mup\Nuix-... | explorer.exe | 9164 | Built-in administrat... | 0 | |
| 12/22/2020 6:36:25... | G4L-5-10 | WORKGROUP | Delete | $IV7R2IY.oxps | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 118 | 99143CAC60C9366... |
| 12/22/2020 6:36:25... | G4L-5-10 | WORKGROUP | Delete | $RV7R2IY.oxps | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 1988831 | A95AEE57261A584... |
| 12/22/2020 6:36:18... | G4L-5-10 | WORKGROUP | Write | $IV7R2IY.oxps | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 118 | 99143CAC60C9366... |
| 12/22/2020 6:36:18... | G4L-5-10 | WORKGROUP | Rename | $RV7R2IY.oxps | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 0 | |
| 12/22/2020 6:36:18... | G4L-5-10 | WORKGROUP | Delete | provasic.oxps | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 1988831 | A95AEE57261A584... |
| 12/22/2020 6:36:14... | G4L-5-10 | WORKGROUP | Delete | $IU8GYZS.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 144 | 0CF1A119A647329... |
| 12/22/2020 6:36:14... | G4L-5-10 | WORKGROUP | Delete | $RU8GYZS.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 9125585 | |
| 12/22/2020 6:36:06... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | explorer.exe | 9164 | Built-in administrat... | 9125585 | |

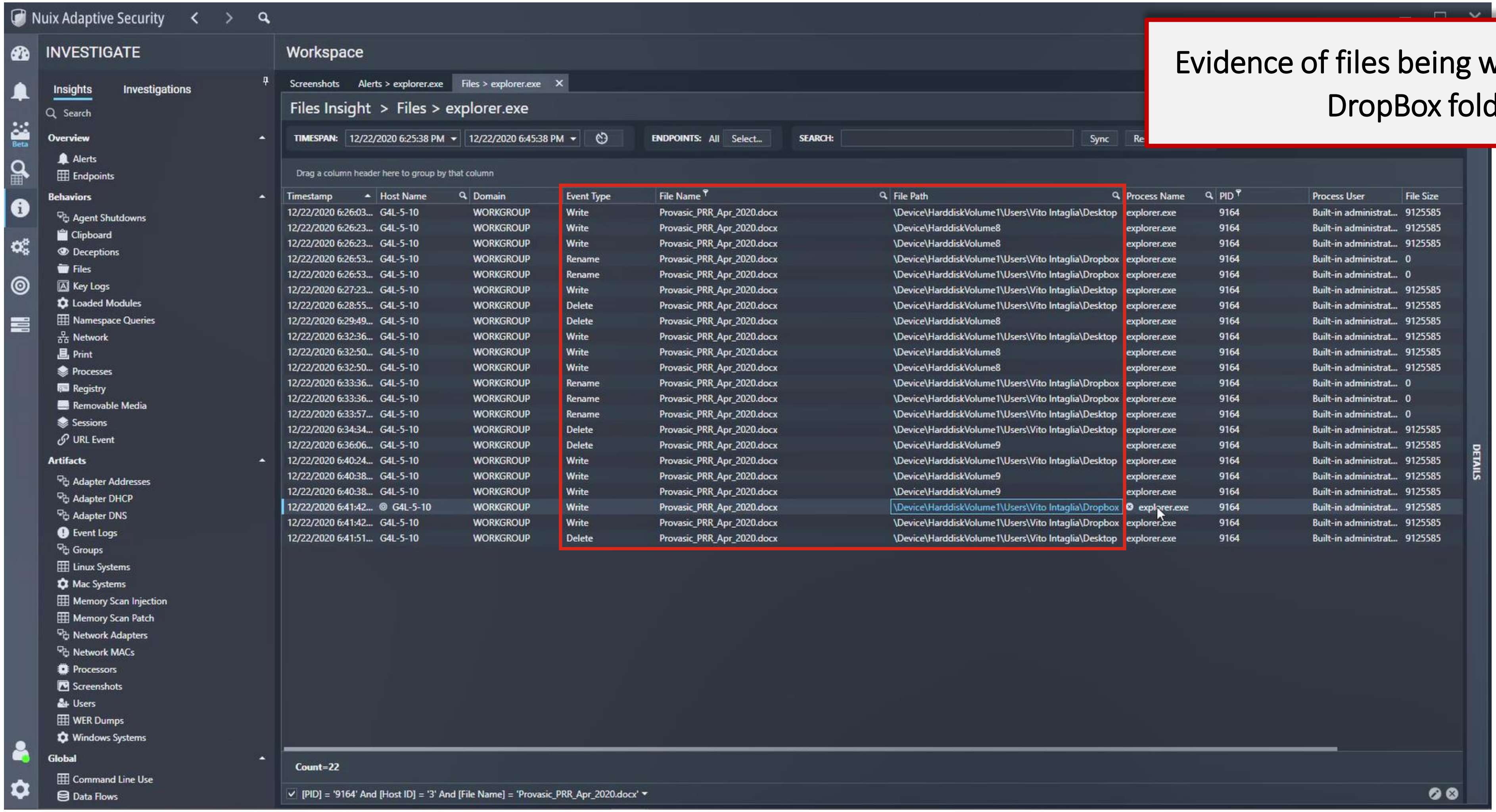
Count=30

☑ [PID] = '9164' And [Host ID] = '3'

Detection of file writes/manipulations, renames and deletions

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 1 – Data Theft and Disclosure



Files Insight > Files > explorer.exe

TIMESPAN: 12/22/2020 6:25:38 PM – 12/22/2020 6:45:38 PM  ENDPOINTS: All Select...  SEARCH:

Drag a column header here to group by that column

| Timestamp | Host Name | Domain | Event Type | File Name | File Path | Process Name | PID | Process User | File Size |
|---|---|---|---|---|---|---|---|---|---|
| 12/22/2020 6:26:03... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Desktop | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:26:23... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume8 | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:26:23... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume8 | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:26:53... | G4L-5-10 | WORKGROUP | Rename | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Dropbox | explorer.exe | 9164 | Built-in administrat... | 0 |
| 12/22/2020 6:26:53... | G4L-5-10 | WORKGROUP | Rename | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Dropbox | explorer.exe | 9164 | Built-in administrat... | 0 |
| 12/22/2020 6:27:23... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Desktop | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:28:55... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Desktop | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:29:49... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume8 | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:32:36... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Desktop | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:32:50... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume8 | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:32:50... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume8 | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:33:36... | G4L-5-10 | WORKGROUP | Rename | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Dropbox | explorer.exe | 9164 | Built-in administrat... | 0 |
| 12/22/2020 6:33:36... | G4L-5-10 | WORKGROUP | Rename | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Dropbox | explorer.exe | 9164 | Built-in administrat... | 0 |
| 12/22/2020 6:33:57... | G4L-5-10 | WORKGROUP | Rename | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Desktop | explorer.exe | 9164 | Built-in administrat... | 0 |
| 12/22/2020 6:34:34... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Desktop | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:36:06... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume9 | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:40:24... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Desktop | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:40:38... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume9 | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:40:38... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume9 | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:41:42... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Dropbox | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:41:42... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Dropbox | explorer.exe | 9164 | Built-in administrat... | 9125585 |
| 12/22/2020 6:41:51... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx | \Device\HarddiskVolume1\Users\Vito Intaglia\Desktop | explorer.exe | 9164 | Built-in administrat... | 9125585 |

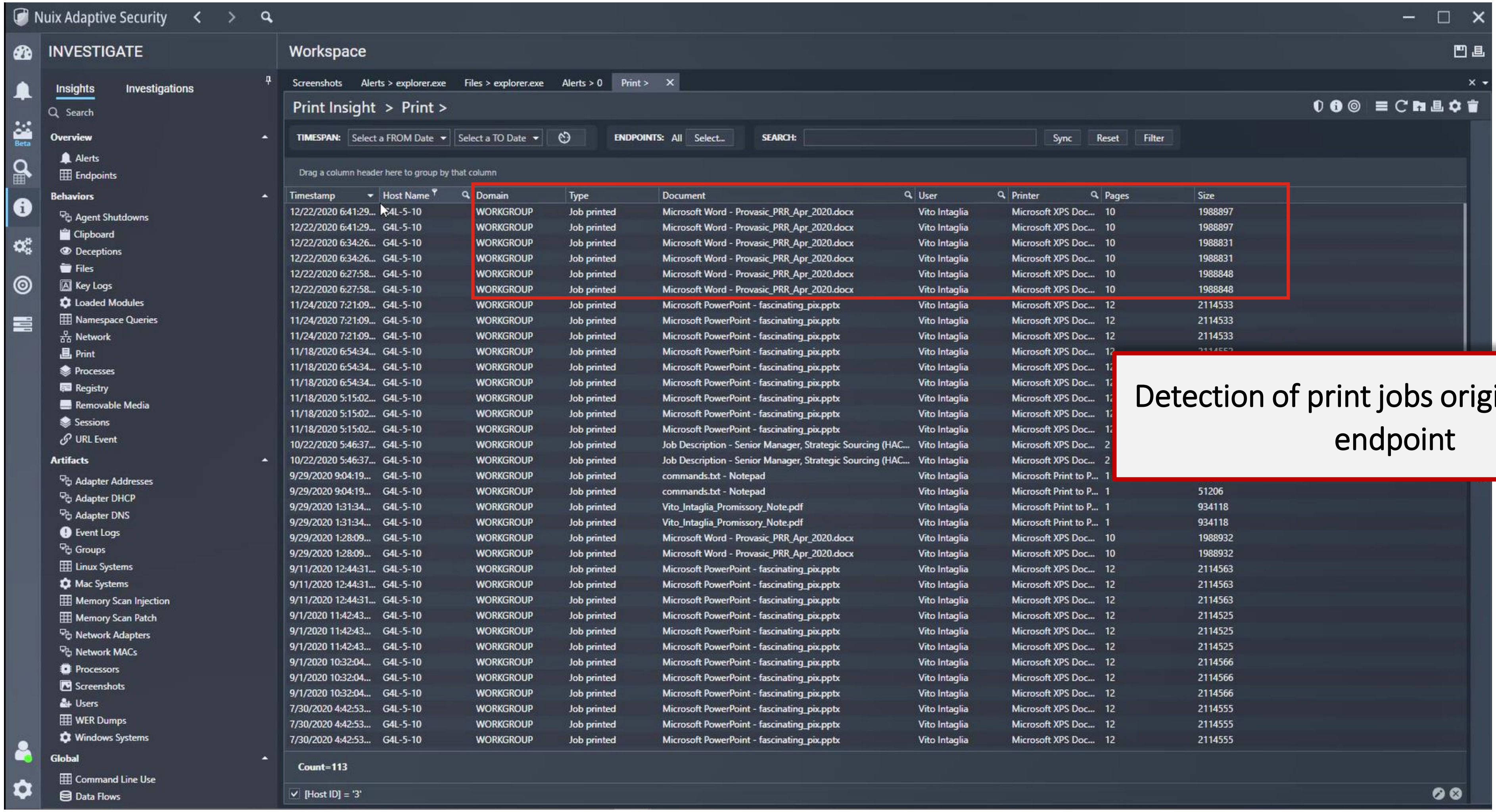
Count=22

☑ [PID] = '9164' And [Host ID] = '3' And [File Name] = 'Provasic_PRR_Apr_2020.docx'

Evidence of files being written to local DropBox folder

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 1 – Data Theft and Disclosure



| Timestamp | Host Name | Domain | Type | Document | User | Printer | Pages | Size |
|---|---|---|---|---|---|---|---|---|
| 12/22/2020 6:41:29... | G4L-5-10 | WORKGROUP | Job printed | Microsoft Word - Provasic_PRR_Apr_2020.docx | Vito Intaglia | Microsoft XPS Doc... | 10 | 1988897 |
| 12/22/2020 6:41:29... | G4L-5-10 | WORKGROUP | Job printed | Microsoft Word - Provasic_PRR_Apr_2020.docx | Vito Intaglia | Microsoft XPS Doc... | 10 | 1988897 |
| 12/22/2020 6:34:26... | G4L-5-10 | WORKGROUP | Job printed | Microsoft Word - Provasic_PRR_Apr_2020.docx | Vito Intaglia | Microsoft XPS Doc... | 10 | 1988831 |
| 12/22/2020 6:34:26... | G4L-5-10 | WORKGROUP | Job printed | Microsoft Word - Provasic_PRR_Apr_2020.docx | Vito Intaglia | Microsoft XPS Doc... | 10 | 1988831 |
| 12/22/2020 6:27:58... | G4L-5-10 | WORKGROUP | Job printed | Microsoft Word - Provasic_PRR_Apr_2020.docx | Vito Intaglia | Microsoft XPS Doc... | 10 | 1988848 |
| 12/22/2020 6:27:58... | G4L-5-10 | WORKGROUP | Job printed | Microsoft Word - Provasic_PRR_Apr_2020.docx | Vito Intaglia | Microsoft XPS Doc... | 10 | 1988848 |
| 11/24/2020 7:21:09... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114533 |
| 11/24/2020 7:21:09... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114533 |
| 11/24/2020 7:21:09... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114533 |
| 11/18/2020 6:54:34... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114553 |
| 11/18/2020 6:54:34... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 1 | |
| 11/18/2020 6:54:34... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 1 | |
| 11/18/2020 5:15:02... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 1 | |
| 11/18/2020 5:15:02... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 1 | |
| 11/18/2020 5:15:02... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 1 | |
| 10/22/2020 5:46:37... | G4L-5-10 | WORKGROUP | Job printed | Job Description - Senior Manager, Strategic Sourcing (HAC... | Vito Intaglia | Microsoft XPS Doc... | 2 | |
| 10/22/2020 5:46:37... | G4L-5-10 | WORKGROUP | Job printed | Job Description - Senior Manager, Strategic Sourcing (HAC... | Vito Intaglia | Microsoft XPS Doc... | 2 | |
| 9/29/2020 9:04:19... | G4L-5-10 | WORKGROUP | Job printed | commands.txt - Notepad | Vito Intaglia | Microsoft Print to P... | 1 | |
| 9/29/2020 9:04:19... | G4L-5-10 | WORKGROUP | Job printed | commands.txt - Notepad | Vito Intaglia | Microsoft Print to P... | 1 | 51206 |
| 9/29/2020 1:31:34... | G4L-5-10 | WORKGROUP | Job printed | Vito_Intaglia_Promissory_Note.pdf | Vito Intaglia | Microsoft Print to P... | 1 | 934118 |
| 9/29/2020 1:31:34... | G4L-5-10 | WORKGROUP | Job printed | Vito_Intaglia_Promissory_Note.pdf | Vito Intaglia | Microsoft Print to P... | 1 | 934118 |
| 9/29/2020 1:28:09... | G4L-5-10 | WORKGROUP | Job printed | Microsoft Word - Provasic_PRR_Apr_2020.docx | Vito Intaglia | Microsoft XPS Doc... | 10 | 1988932 |
| 9/29/2020 1:28:09... | G4L-5-10 | WORKGROUP | Job printed | Microsoft Word - Provasic_PRR_Apr_2020.docx | Vito Intaglia | Microsoft XPS Doc... | 10 | 1988932 |
| 9/11/2020 12:44:31... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114563 |
| 9/11/2020 12:44:31... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114563 |
| 9/11/2020 12:44:31... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114563 |
| 9/1/2020 11:42:43... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114525 |
| 9/1/2020 11:42:43... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114525 |
| 9/1/2020 11:42:43... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114525 |
| 9/1/2020 10:32:04... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114566 |
| 9/1/2020 10:32:04... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114566 |
| 9/1/2020 10:32:04... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114566 |
| 7/30/2020 4:42:53... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114555 |
| 7/30/2020 4:42:53... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114555 |
| 7/30/2020 4:42:53... | G4L-5-10 | WORKGROUP | Job printed | Microsoft PowerPoint - fascinating_pix.pptx | Vito Intaglia | Microsoft XPS Doc... | 12 | 2114555 |

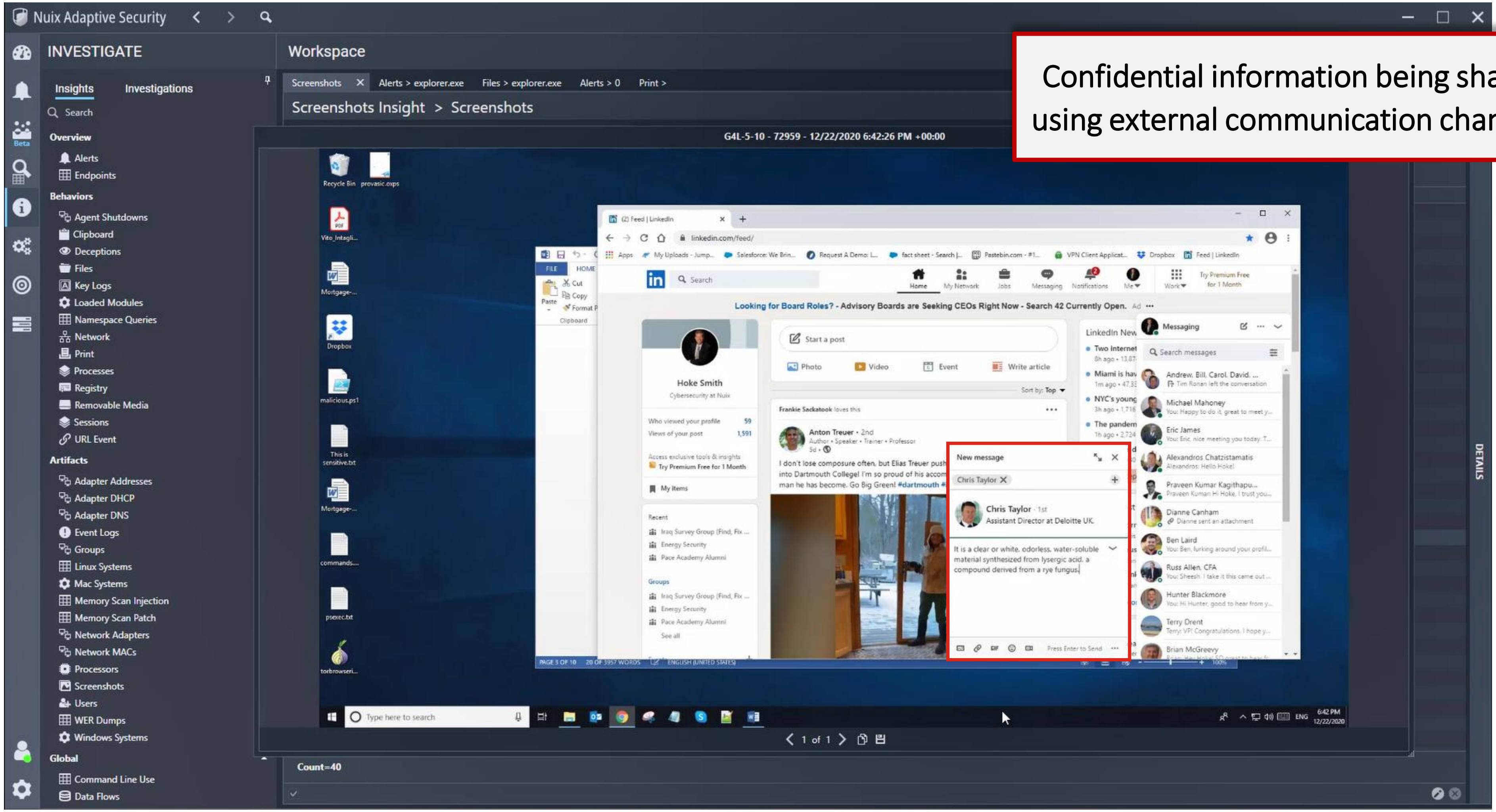
Count=113

☑ [Host ID] = '3'

Detection of print jobs originating from endpoint

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 1 – Data Theft and Disclosure



New message

Chris Taylor

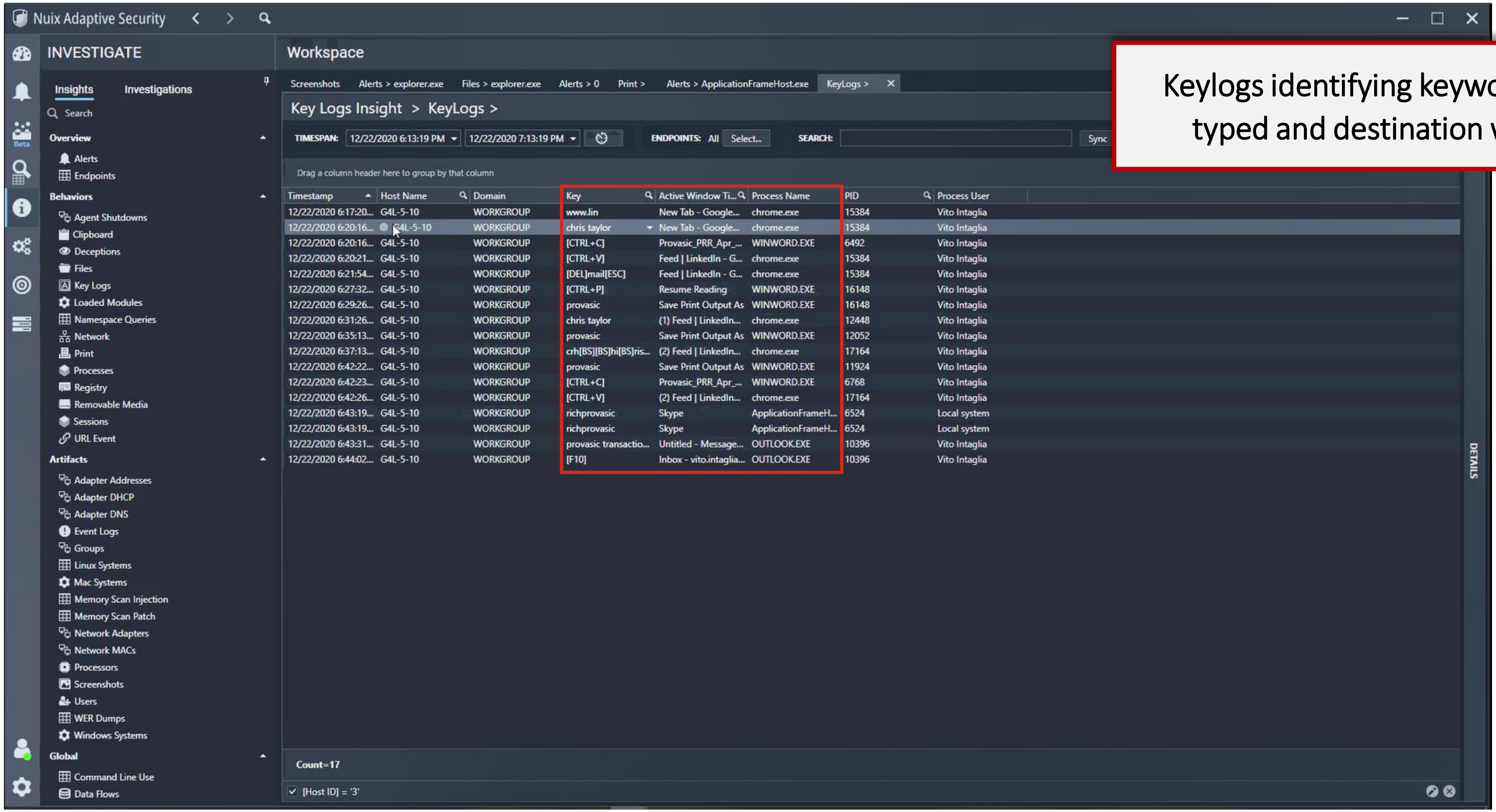
Chris Taylor · 1st
Assistant Director at Deloitte UK

It is a clear or white, odorless, water-soluble material synthesized from lysergic acid, a compound derived from a rye fungus.

Confidential information being shared using external communication channels

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 1 – Data Theft and Disclosure



Key Logs Insight > KeyLogs >

TIMESPAN: 12/22/2020 6:13:19 PM – 12/22/2020 7:13:19 PM   ENDPOINTS: All Select...   SEARCH:

Drag a column header here to group by that column

| Timestamp | Host Name | Domain | Key | Active Window Ti... | Process Name | PID | Process User |
|---|---|---|---|---|---|---|---|
| 12/22/2020 6:17:20... | G4L-5-10 | WORKGROUP | www.lin | New Tab - Google... | chrome.exe | 15384 | Vito Intaglia |
| 12/22/2020 6:20:16... | G4L-5-10 | WORKGROUP | chris taylor | New Tab - Google... | chrome.exe | 15384 | Vito Intaglia |
| 12/22/2020 6:20:16... | G4L-5-10 | WORKGROUP | [CTRL+C] | Provasic_PRR_Apr_... | WINWORD.EXE | 6492 | Vito Intaglia |
| 12/22/2020 6:20:21... | G4L-5-10 | WORKGROUP | [CTRL+V] | Feed \| LinkedIn - G... | chrome.exe | 15384 | Vito Intaglia |
| 12/22/2020 6:21:54... | G4L-5-10 | WORKGROUP | [DEL]mail[ESC] | Feed \| LinkedIn - G... | chrome.exe | 15384 | Vito Intaglia |
| 12/22/2020 6:27:32... | G4L-5-10 | WORKGROUP | [CTRL+P] | Resume Reading | WINWORD.EXE | 16148 | Vito Intaglia |
| 12/22/2020 6:29:26... | G4L-5-10 | WORKGROUP | provasic | Save Print Output As | WINWORD.EXE | 16148 | Vito Intaglia |
| 12/22/2020 6:31:26... | G4L-5-10 | WORKGROUP | chris taylor | (1) Feed \| LinkedIn... | chrome.exe | 12448 | Vito Intaglia |
| 12/22/2020 6:35:13... | G4L-5-10 | WORKGROUP | provasic | Save Print Output As | WINWORD.EXE | 12052 | Vito Intaglia |
| 12/22/2020 6:37:13... | G4L-5-10 | WORKGROUP | crh[BS][BS]hi[BS]ris... | (2) Feed \| LinkedIn... | chrome.exe | 17164 | Vito Intaglia |
| 12/22/2020 6:42:22... | G4L-5-10 | WORKGROUP | provasic | Save Print Output As | WINWORD.EXE | 11924 | Vito Intaglia |
| 12/22/2020 6:42:23... | G4L-5-10 | WORKGROUP | [CTRL+C] | Provasic_PRR_Apr_... | WINWORD.EXE | 6768 | Vito Intaglia |
| 12/22/2020 6:42:26... | G4L-5-10 | WORKGROUP | [CTRL+V] | (2) Feed \| LinkedIn... | chrome.exe | 17164 | Vito Intaglia |
| 12/22/2020 6:43:19... | G4L-5-10 | WORKGROUP | richprovasic | Skype | ApplicationFrameH... | 6524 | Local system |
| 12/22/2020 6:43:19... | G4L-5-10 | WORKGROUP | richprovasic | Skype | ApplicationFrameH... | 6524 | Local system |
| 12/22/2020 6:43:31... | G4L-5-10 | WORKGROUP | provasic transactio... | Untitled - Message... | OUTLOOK.EXE | 10396 | Vito Intaglia |
| 12/22/2020 6:44:02... | G4L-5-10 | WORKGROUP | [F10] | Inbox - vito.intaglia... | OUTLOOK.EXE | 10396 | Vito Intaglia |

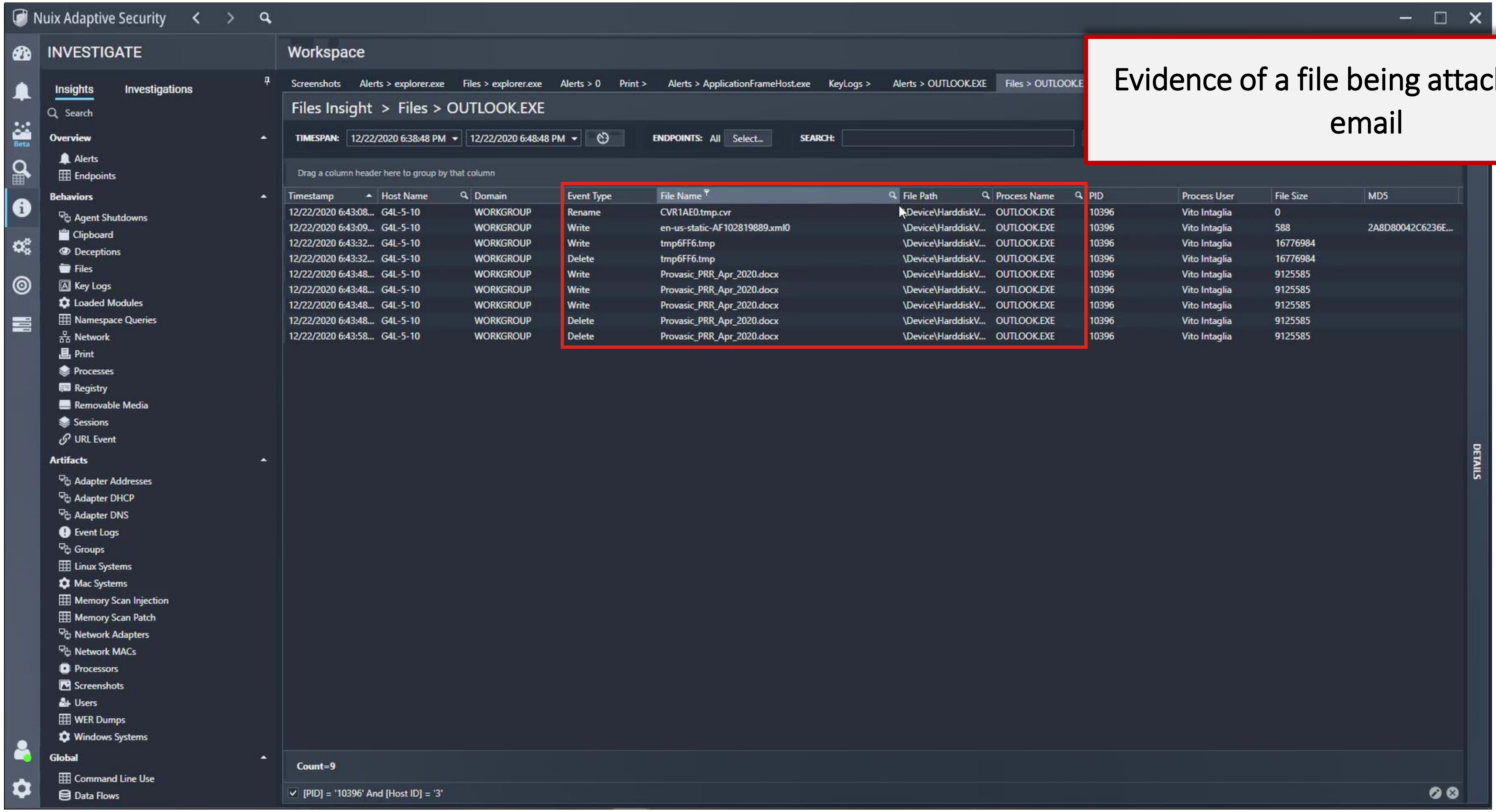
Count=17

☑ [Host ID] = '3'

Keylogs identifying keywords being typed and destination window

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 1 – Data Theft and Disclosure



Files Insight > Files > OUTLOOK.EXE

TIMESPAN: 12/22/2020 6:38:48 PM – 12/22/2020 6:48:48 PM  ENDPOINTS: All Select...  SEARCH:

Drag a column header here to group by that column

| Timestamp | Host Name | Domain | Event Type | File Name | File Path | Process Name | PID | Process User | File Size | MD5 |
|---|---|---|---|---|---|---|---|---|---|---|
| 12/22/2020 6:43:08... | G4L-5-10 | WORKGROUP | Rename | CVR1AE0.tmp.cvr | \Device\HarddiskV... | OUTLOOK.EXE | 10396 | Vito Intaglia | 0 | |
| 12/22/2020 6:43:09... | G4L-5-10 | WORKGROUP | Write | en-us-static-AF102819889.xml0 | \Device\HarddiskV... | OUTLOOK.EXE | 10396 | Vito Intaglia | 588 | 2A8D80042C6236E... |
| 12/22/2020 6:43:32... | G4L-5-10 | WORKGROUP | Write | tmp6FF6.tmp | \Device\HarddiskV... | OUTLOOK.EXE | 10396 | Vito Intaglia | 16776984 | |
| 12/22/2020 6:43:32... | G4L-5-10 | WORKGROUP | Delete | tmp6FF6.tmp | \Device\HarddiskV... | OUTLOOK.EXE | 10396 | Vito Intaglia | 16776984 | |
| 12/22/2020 6:43:48... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | OUTLOOK.EXE | 10396 | Vito Intaglia | 9125585 | |
| 12/22/2020 6:43:48... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | OUTLOOK.EXE | 10396 | Vito Intaglia | 9125585 | |
| 12/22/2020 6:43:48... | G4L-5-10 | WORKGROUP | Write | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | OUTLOOK.EXE | 10396 | Vito Intaglia | 9125585 | |
| 12/22/2020 6:43:48... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | OUTLOOK.EXE | 10396 | Vito Intaglia | 9125585 | |
| 12/22/2020 6:43:58... | G4L-5-10 | WORKGROUP | Delete | Provasic_PRR_Apr_2020.docx | \Device\HarddiskV... | OUTLOOK.EXE | 10396 | Vito Intaglia | 9125585 | |

Count=9

☑ [PID] = '10396' And [Host ID] = '3'

Evidence of a file being attached to an email

# Scenario 2 - Fraudulent Transaction

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 2 – Fraudulent Transaction

### Falsify a purchase order

### Prepare

- Research target company
- Get tools to clean up evidence
- Set up secure communications

### Execute

- Copy template to local system
- Modify template
- Falsify signature
- Print document

### Cleanup

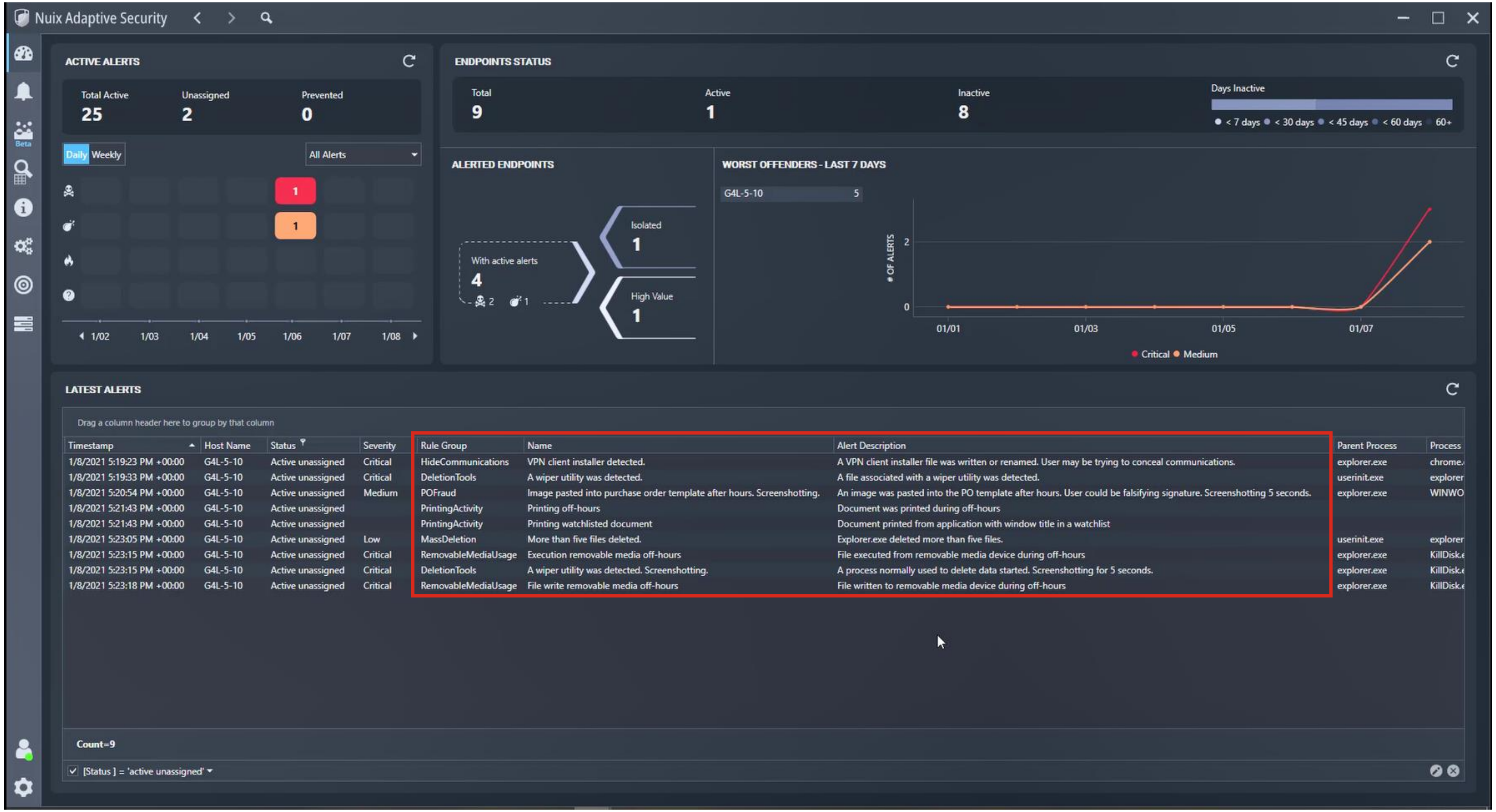
- Delete files
- Run a deletion utility

### Communicate

- Interact with other involved parties over chat, email, etc.

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 2 – Fraudulent Transaction



ACTIVE ALERTS

Total Active 25
Unassigned 2
Prevented 0

ENDPOINTS STATUS

Total 9
Active 1
Inactive 8

ALERTED ENDPOINTS

With active alerts 4
2 1
Isolated 1
High Value 1

LATEST ALERTS

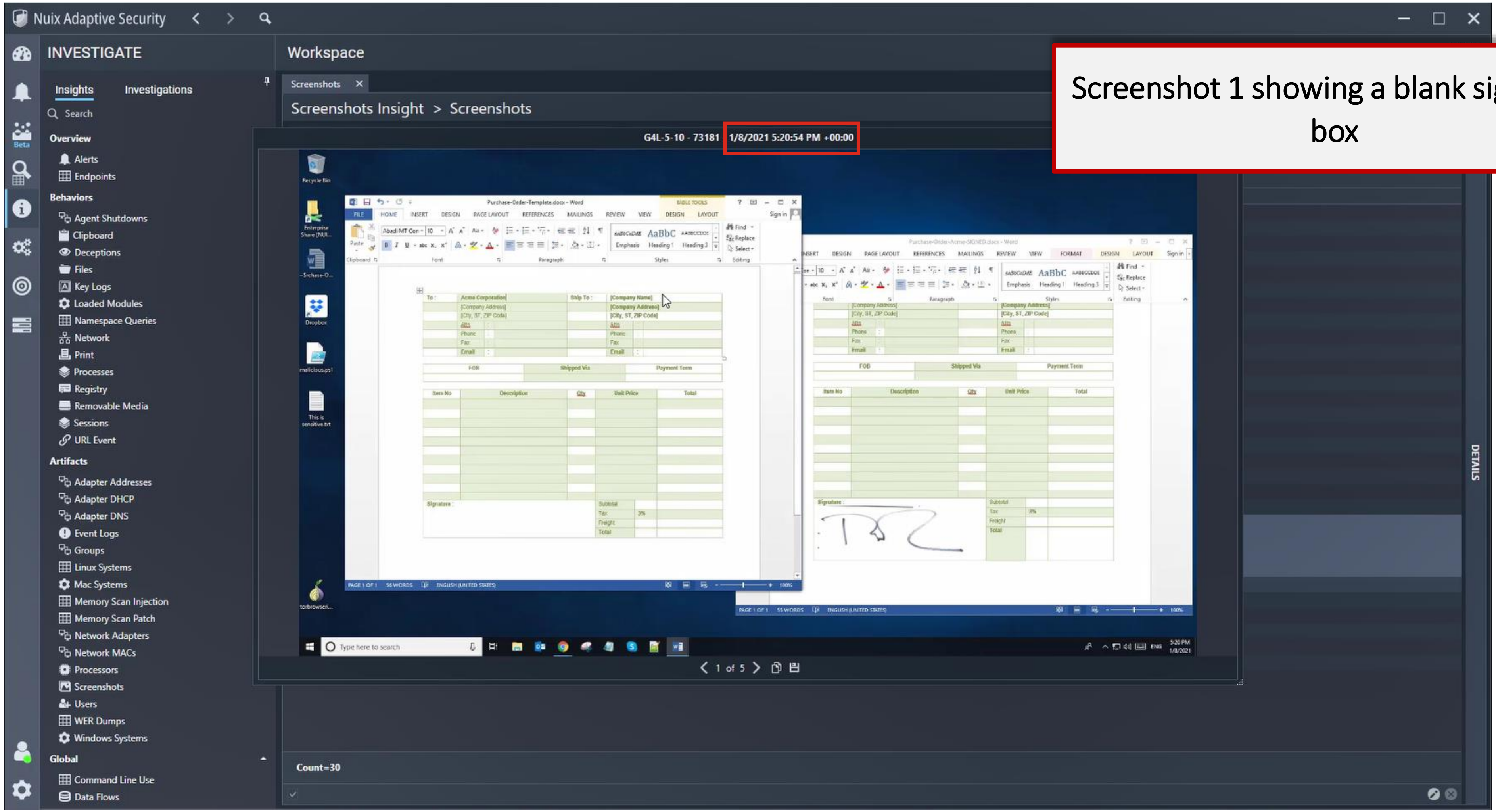
| Timestamp | Host Name | Status | Severity | Rule Group | Name | Alert Description | Parent Process | Process |
|---|---|---|---|---|---|---|---|---|
| 1/8/2021 5:19:23 PM +00:00 | G4L-5-10 | Active unassigned | Critical | HideCommunications | VPN client installer detected. | A VPN client installer file was written or renamed. User may be trying to conceal communications. | explorer.exe | chrome. |
| 1/8/2021 5:19:33 PM +00:00 | G4L-5-10 | Active unassigned | Critical | DeletionTools | A wiper utility was detected. | A file associated with a wiper utility was detected. | userinit.exe | explorer |
| 1/8/2021 5:20:54 PM +00:00 | G4L-5-10 | Active unassigned | Medium | POFraud | Image pasted into purchase order template after hours. Screenshotting. | An image was pasted into the PO template after hours. User could be falsifying signature. Screenshotting 5 seconds. | explorer.exe | WINWO |
| 1/8/2021 5:21:43 PM +00:00 | G4L-5-10 | Active unassigned | | PrintingActivity | Printing off-hours | Document was printed during off-hours | | |
| 1/8/2021 5:21:43 PM +00:00 | G4L-5-10 | Active unassigned | | PrintingActivity | Printing watchlisted document | Document printed from application with window title in a watchlist | | |
| 1/8/2021 5:23:05 PM +00:00 | G4L-5-10 | Active unassigned | Low | MassDeletion | More than five files deleted. | Explorer.exe deleted more than five files. | userinit.exe | explorer |
| 1/8/2021 5:23:15 PM +00:00 | G4L-5-10 | Active unassigned | Critical | RemovableMediaUsage | Execution removable media off-hours | File executed from removable media device during off-hours | explorer.exe | KillDisk. |
| 1/8/2021 5:23:15 PM +00:00 | G4L-5-10 | Active unassigned | Critical | DeletionTools | A wiper utility was detected. Screenshotting. | A process normally used to delete data started. Screenshotting for 5 seconds. | explorer.exe | KillDisk. |
| 1/8/2021 5:23:18 PM +00:00 | G4L-5-10 | Active unassigned | Critical | RemovableMediaUsage | File write removable media off-hours | File written to removable media device during off-hours | explorer.exe | KillDisk. |

Count=9

☑ [Status ] = 'active unassigned'

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

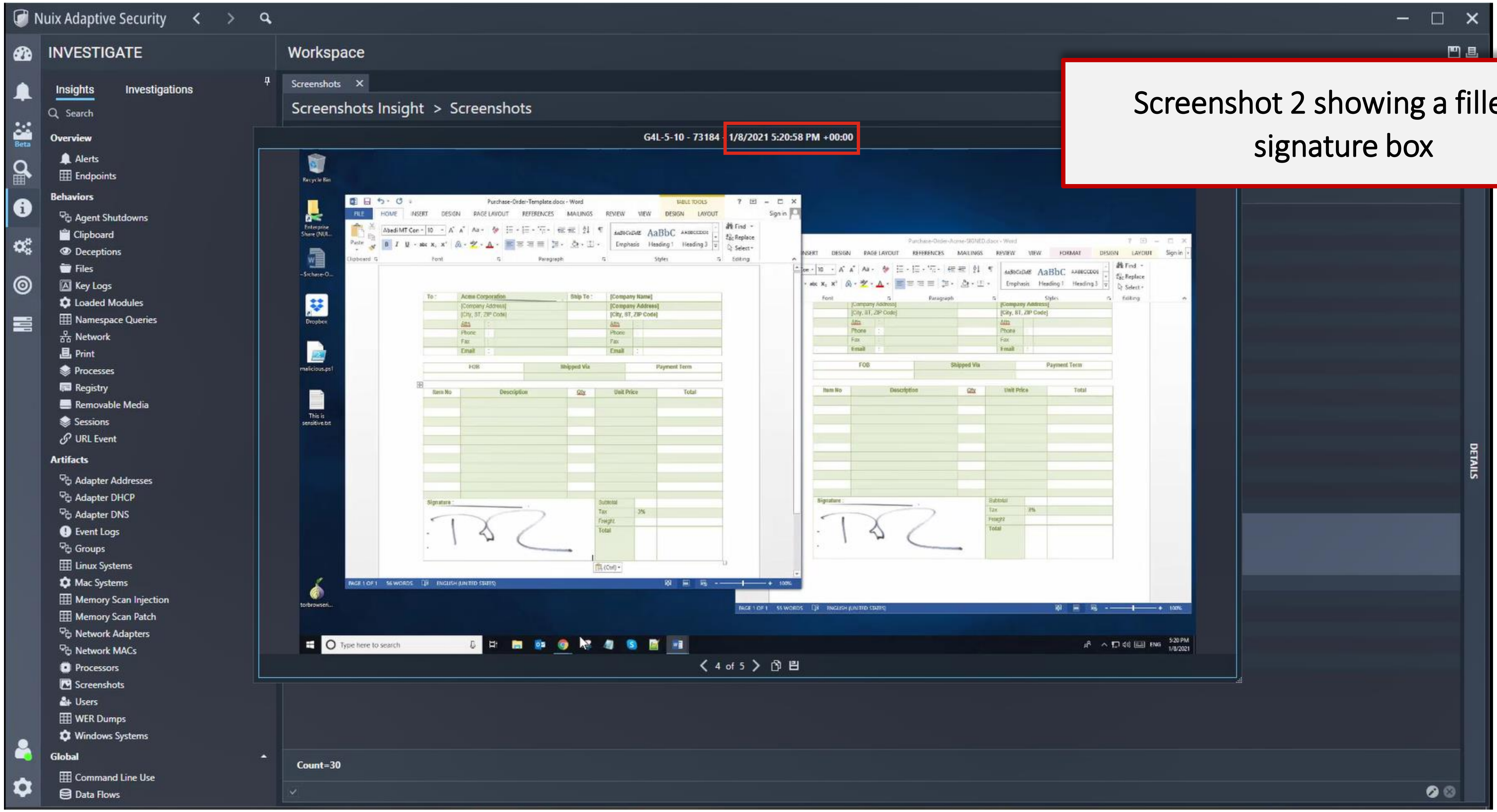
## Scenario 2 – Fraudulent Transaction



Screenshot 1 showing a blank signature box

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

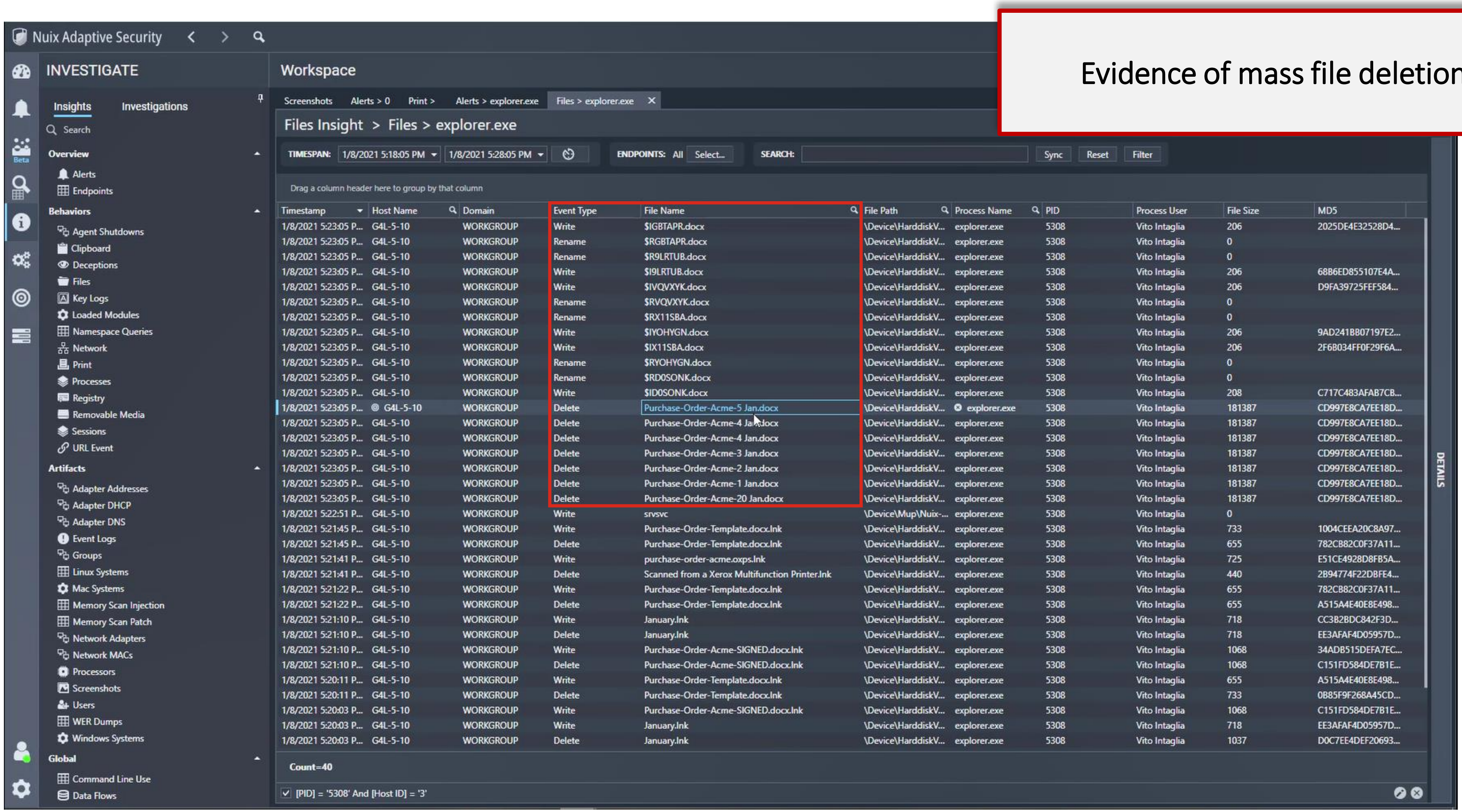
## Scenario 2 – Fraudulent Transaction



Screenshot 2 showing a filled in signature box

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 2 – Fraudulent Transaction



TIMESPAN: 1/8/2021 5:18:05 PM – 1/8/2021 5:28:05 PM ENDPOINTS: All Select... SEARCH:

Drag a column header here to group by that column

| Timestamp | Host Name | Domain | Event Type | File Name | File Path | Process Name | PID | Process User | File Size | MD5 |
|---|---|---|---|---|---|---|---|---|---|---|
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Write | $IGBTAPR.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 206 | 2025DE4E32528D4... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Rename | $RGBTAPR.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 0 | |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Rename | $R9LRTUB.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 0 | |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Write | $I9LRTUB.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 206 | 68B6ED855107E4A... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Write | $IVQVXYK.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 206 | D9FA39725FEF584... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Rename | $RVQVXYK.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 0 | |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Rename | $RX11SBA.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 0 | |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Write | $IYOHYGN.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 206 | 9AD241BB07197E2... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Write | $IX11SBA.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 206 | 2F6B034FF0F29F6A... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Rename | $RYOHYGN.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 0 | |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Rename | $RD0SONK.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 0 | |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Write | $ID0SONK.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 208 | C717C483AFAB7CB... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Acme-5 Jan.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 181387 | CD997E8CA7EE18D... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Acme-4 Jan.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 181387 | CD997E8CA7EE18D... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Acme-4 Jan.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 181387 | CD997E8CA7EE18D... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Acme-3 Jan.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 181387 | CD997E8CA7EE18D... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Acme-2 Jan.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 181387 | CD997E8CA7EE18D... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Acme-1 Jan.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 181387 | CD997E8CA7EE18D... |
| 1/8/2021 5:23:05 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Acme-20 Jan.docx | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 181387 | CD997E8CA7EE18D... |
| 1/8/2021 5:22:51 P... | G4L-5-10 | WORKGROUP | Write | srvsvc | \Device\Mup\Nuix-... | explorer.exe | 5308 | Vito Intaglia | 0 | |
| 1/8/2021 5:21:45 P... | G4L-5-10 | WORKGROUP | Write | Purchase-Order-Template.docx.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 733 | 1004CEEA20C8A97... |
| 1/8/2021 5:21:45 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Template.docx.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 655 | 782CB82C0F37A11... |
| 1/8/2021 5:21:41 P... | G4L-5-10 | WORKGROUP | Write | purchase-order-acme.oxps.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 725 | E51CE4928D8FB5A... |
| 1/8/2021 5:21:41 P... | G4L-5-10 | WORKGROUP | Delete | Scanned from a Xerox Multifunction Printer.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 440 | 2B94774F22DBFE4... |
| 1/8/2021 5:21:22 P... | G4L-5-10 | WORKGROUP | Write | Purchase-Order-Template.docx.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 655 | 782CB82C0F37A11... |
| 1/8/2021 5:21:22 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Template.docx.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 655 | A515A4E40E8E498... |
| 1/8/2021 5:21:10 P... | G4L-5-10 | WORKGROUP | Write | January.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 718 | CC3B2BDC842F3D... |
| 1/8/2021 5:21:10 P... | G4L-5-10 | WORKGROUP | Delete | January.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 718 | EE3AFAF4D05957D... |
| 1/8/2021 5:21:10 P... | G4L-5-10 | WORKGROUP | Write | Purchase-Order-Acme-SIGNED.docx.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 1068 | 34ADB515DEFA7EC... |
| 1/8/2021 5:21:10 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Acme-SIGNED.docx.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 1068 | C151FD584DE7B1E... |
| 1/8/2021 5:20:11 P... | G4L-5-10 | WORKGROUP | Write | Purchase-Order-Template.docx.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 655 | A515A4E40E8E498... |
| 1/8/2021 5:20:11 P... | G4L-5-10 | WORKGROUP | Delete | Purchase-Order-Template.docx.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 733 | 0B85F9F268A45CD... |
| 1/8/2021 5:20:03 P... | G4L-5-10 | WORKGROUP | Write | Purchase-Order-Acme-SIGNED.docx.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 1068 | C151FD584DE7B1E... |
| 1/8/2021 5:20:03 P... | G4L-5-10 | WORKGROUP | Write | January.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 718 | EE3AFAF4D05957D... |
| 1/8/2021 5:20:03 P... | G4L-5-10 | WORKGROUP | Delete | January.lnk | \Device\HarddiskV... | explorer.exe | 5308 | Vito Intaglia | 1037 | D0C7EE4DEF20693... |

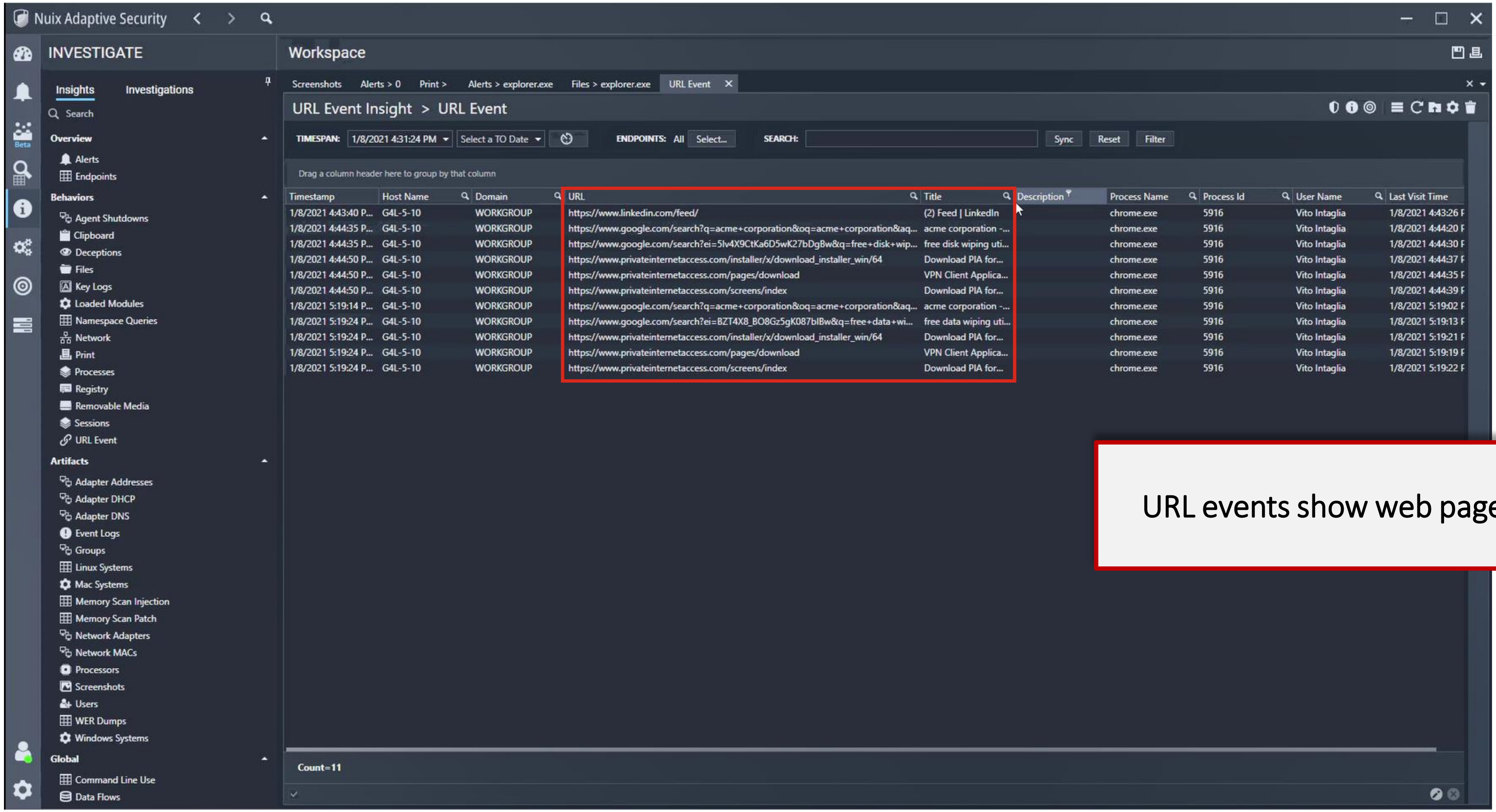
Count=40

☑ [PID] = '5308' And [Host ID] = '3'

Evidence of mass file deletion

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 2 – Fraudulent Transaction



URL Event Insight > URL Event

TIMESPAN: 1/8/2021 4:31:24 PM | Select a TO Date | ENDPOINTS: All | SEARCH:

Drag a column header here to group by that column

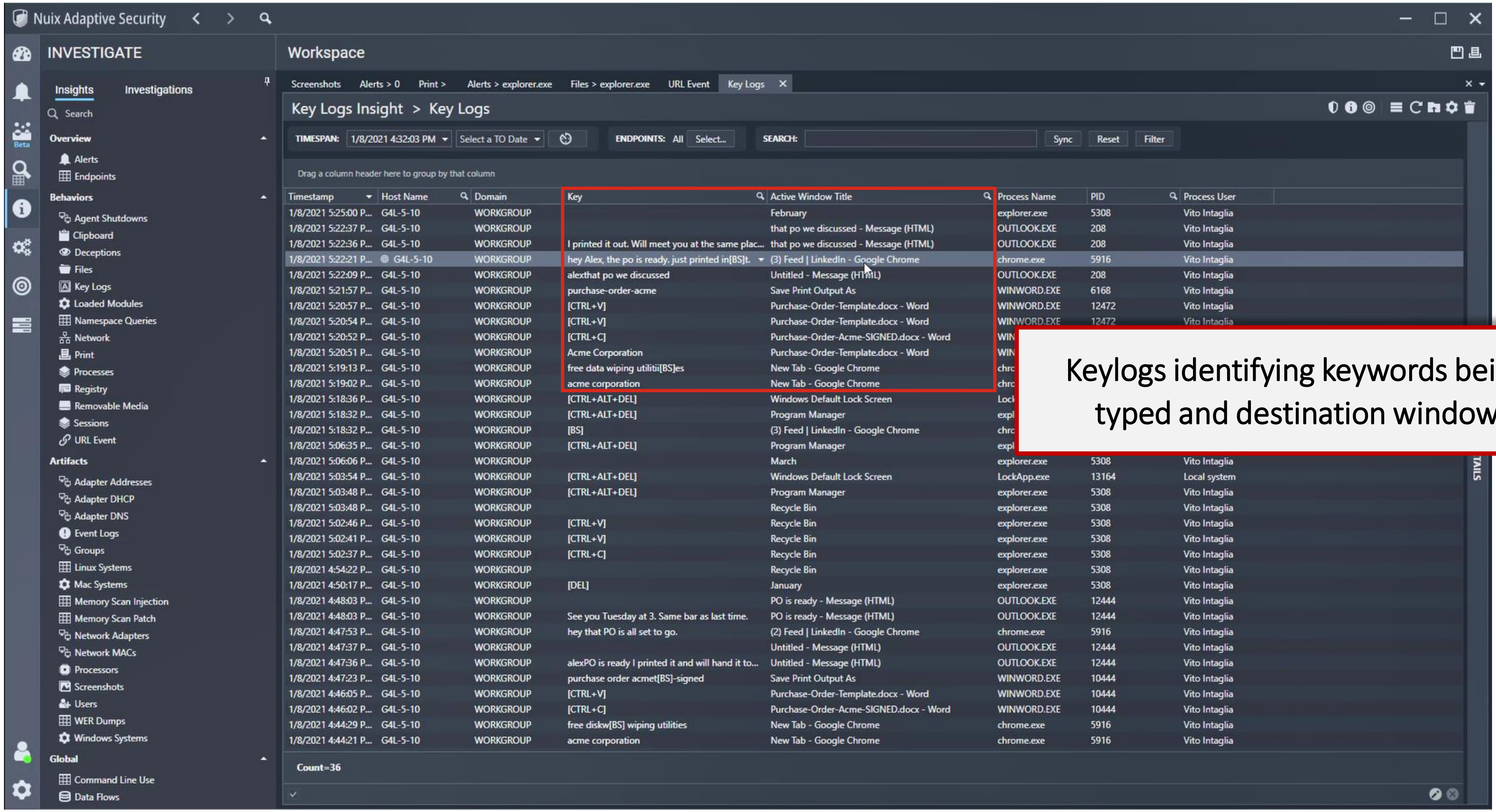
| Timestamp | Host Name | Domain | URL | Title | Description | Process Name | Process Id | User Name | Last Visit Time |
|---|---|---|---|---|---|---|---|---|---|
| 1/8/2021 4:43:40 P... | G4L-5-10 | WORKGROUP | https://www.linkedin.com/feed/ | (2) Feed \| LinkedIn |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 4:43:26 |
| 1/8/2021 4:44:35 P... | G4L-5-10 | WORKGROUP | https://www.google.com/search?q=acme+corporation&oq=acme+corporation&aq... | acme corporation -... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 4:44:20 |
| 1/8/2021 4:44:35 P... | G4L-5-10 | WORKGROUP | https://www.google.com/search?ei=5lv4X9CtKa6D5wK27bDgBw&q=free+disk+wip... | free disk wiping uti... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 4:44:30 |
| 1/8/2021 4:44:50 P... | G4L-5-10 | WORKGROUP | https://www.privateinternetaccess.com/installer/x/download_installer_win/64 | Download PIA for... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 4:44:37 |
| 1/8/2021 4:44:50 P... | G4L-5-10 | WORKGROUP | https://www.privateinternetaccess.com/pages/download | VPN Client Applica... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 4:44:35 |
| 1/8/2021 4:44:50 P... | G4L-5-10 | WORKGROUP | https://www.privateinternetaccess.com/screens/index | Download PIA for... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 4:44:39 |
| 1/8/2021 5:19:14 P... | G4L-5-10 | WORKGROUP | https://www.google.com/search?q=acme+corporation&oq=acme+corporation&aq... | acme corporation -... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 5:19:02 |
| 1/8/2021 5:19:24 P... | G4L-5-10 | WORKGROUP | https://www.google.com/search?ei=BZT4X8_BO8Gz5gK087bIBw&q=free+data+wi... | free data wiping uti... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 5:19:13 |
| 1/8/2021 5:19:24 P... | G4L-5-10 | WORKGROUP | https://www.privateinternetaccess.com/installer/x/download_installer_win/64 | Download PIA for... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 5:19:21 |
| 1/8/2021 5:19:24 P... | G4L-5-10 | WORKGROUP | https://www.privateinternetaccess.com/pages/download | VPN Client Applica... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 5:19:19 |
| 1/8/2021 5:19:24 P... | G4L-5-10 | WORKGROUP | https://www.privateinternetaccess.com/screens/index | Download PIA for... |  | chrome.exe | 5916 | Vito Intaglia | 1/8/2021 5:19:22 |

Count=11

URL events show web pages visited

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Scenario 2 – Fraudulent Transaction



TIMESPAN: 1/8/2021 4:32:03 PM   Select a TO Date   ENDPOINTS: All   Select...   SEARCH:

| Timestamp | Host Name | Domain | Key | Active Window Title | Process Name | PID | Process User |
|---|---|---|---|---|---|---|---|
| 1/8/2021 5:25:00 P... | G4L-5-10 | WORKGROUP |  | February | explorer.exe | 5308 | Vito Intaglia |
| 1/8/2021 5:22:37 P... | G4L-5-10 | WORKGROUP |  | that po we discussed - Message (HTML) | OUTLOOK.EXE | 208 | Vito Intaglia |
| 1/8/2021 5:22:36 P... | G4L-5-10 | WORKGROUP | I printed it out. Will meet you at the same plac... | that po we discussed - Message (HTML) | OUTLOOK.EXE | 208 | Vito Intaglia |
| 1/8/2021 5:22:21 P... | G4L-5-10 | WORKGROUP | hey Alex, the po is ready. just printed in[BS]t. | (3) Feed \| LinkedIn - Google Chrome | chrome.exe | 5916 | Vito Intaglia |
| 1/8/2021 5:22:09 P... | G4L-5-10 | WORKGROUP | alexthat po we discussed | Untitled - Message (HTML) | OUTLOOK.EXE | 208 | Vito Intaglia |
| 1/8/2021 5:21:57 P... | G4L-5-10 | WORKGROUP | purchase-order-acme | Save Print Output As | WINWORD.EXE | 6168 | Vito Intaglia |
| 1/8/2021 5:20:57 P... | G4L-5-10 | WORKGROUP | [CTRL+V] | Purchase-Order-Template.docx - Word | WINWORD.EXE | 12472 | Vito Intaglia |
| 1/8/2021 5:20:54 P... | G4L-5-10 | WORKGROUP | [CTRL+V] | Purchase-Order-Template.docx - Word | WINWORD.EXE | 12472 | Vito Intaglia |
| 1/8/2021 5:20:52 P... | G4L-5-10 | WORKGROUP | [CTRL+C] | Purchase-Order-Acme-SIGNED.docx - Word | WIN |  |  |
| 1/8/2021 5:20:51 P... | G4L-5-10 | WORKGROUP | Acme Corporation | Purchase-Order-Template.docx - Word | WIN |  |  |
| 1/8/2021 5:19:13 P... | G4L-5-10 | WORKGROUP | free data wiping utilitii[BS]es | New Tab - Google Chrome | chrc |  |  |
| 1/8/2021 5:19:02 P... | G4L-5-10 | WORKGROUP | acme corporation | New Tab - Google Chrome | chrc |  |  |
| 1/8/2021 5:18:36 P... | G4L-5-10 | WORKGROUP | [CTRL+ALT+DEL] | Windows Default Lock Screen | Lock |  |  |
| 1/8/2021 5:18:32 P... | G4L-5-10 | WORKGROUP | [CTRL+ALT+DEL] | Program Manager | expl |  |  |
| 1/8/2021 5:18:32 P... | G4L-5-10 | WORKGROUP | [BS] | (3) Feed \| LinkedIn - Google Chrome | chrc |  |  |
| 1/8/2021 5:06:35 P... | G4L-5-10 | WORKGROUP | [CTRL+ALT+DEL] | Program Manager | expl |  |  |
| 1/8/2021 5:06:06 P... | G4L-5-10 | WORKGROUP |  | March | explorer.exe | 5308 | Vito Intaglia |
| 1/8/2021 5:03:54 P... | G4L-5-10 | WORKGROUP | [CTRL+ALT+DEL] | Windows Default Lock Screen | LockApp.exe | 13164 | Local system |
| 1/8/2021 5:03:48 P... | G4L-5-10 | WORKGROUP | [CTRL+ALT+DEL] | Program Manager | explorer.exe | 5308 | Vito Intaglia |
| 1/8/2021 5:03:48 P... | G4L-5-10 | WORKGROUP |  | Recycle Bin | explorer.exe | 5308 | Vito Intaglia |
| 1/8/2021 5:02:46 P... | G4L-5-10 | WORKGROUP | [CTRL+V] | Recycle Bin | explorer.exe | 5308 | Vito Intaglia |
| 1/8/2021 5:02:41 P... | G4L-5-10 | WORKGROUP | [CTRL+V] | Recycle Bin | explorer.exe | 5308 | Vito Intaglia |
| 1/8/2021 5:02:37 P... | G4L-5-10 | WORKGROUP | [CTRL+C] | Recycle Bin | explorer.exe | 5308 | Vito Intaglia |
| 1/8/2021 4:54:22 P... | G4L-5-10 | WORKGROUP |  | Recycle Bin | explorer.exe | 5308 | Vito Intaglia |
| 1/8/2021 4:50:17 P... | G4L-5-10 | WORKGROUP | [DEL] | January | explorer.exe | 5308 | Vito Intaglia |
| 1/8/2021 4:48:03 P... | G4L-5-10 | WORKGROUP |  | PO is ready - Message (HTML) | OUTLOOK.EXE | 12444 | Vito Intaglia |
| 1/8/2021 4:48:03 P... | G4L-5-10 | WORKGROUP | See you Tuesday at 3. Same bar as last time. | PO is ready - Message (HTML) | OUTLOOK.EXE | 12444 | Vito Intaglia |
| 1/8/2021 4:47:53 P... | G4L-5-10 | WORKGROUP | hey that PO is all set to go. | (2) Feed \| LinkedIn - Google Chrome | chrome.exe | 5916 | Vito Intaglia |
| 1/8/2021 4:47:37 P... | G4L-5-10 | WORKGROUP |  | Untitled - Message (HTML) | OUTLOOK.EXE | 12444 | Vito Intaglia |
| 1/8/2021 4:47:36 P... | G4L-5-10 | WORKGROUP | alexPO is ready I printed it and will hand it to... | Untitled - Message (HTML) | OUTLOOK.EXE | 12444 | Vito Intaglia |
| 1/8/2021 4:47:23 P... | G4L-5-10 | WORKGROUP | purchase order acmet[BS]-signed | Save Print Output As | WINWORD.EXE | 10444 | Vito Intaglia |
| 1/8/2021 4:46:05 P... | G4L-5-10 | WORKGROUP | [CTRL+V] | Purchase-Order-Template.docx - Word | WINWORD.EXE | 10444 | Vito Intaglia |
| 1/8/2021 4:46:02 P... | G4L-5-10 | WORKGROUP | [CTRL+C] | Purchase-Order-Acme-SIGNED.docx - Word | WINWORD.EXE | 10444 | Vito Intaglia |
| 1/8/2021 4:44:29 P... | G4L-5-10 | WORKGROUP | free diskw[BS] wiping utilities | New Tab - Google Chrome | chrome.exe | 5916 | Vito Intaglia |
| 1/8/2021 4:44:21 P... | G4L-5-10 | WORKGROUP | acme corporation | New Tab - Google Chrome | chrome.exe | 5916 | Vito Intaglia |

Count=36

Keylogs identifying keywords being typed and destination window

# Summary and questions

# It's what's inside that counts: transforming investigations to detect and prevent insider threats

## Summary and questions

**See what the user sees**
Capture screenshots of key activities

**Live preview a computer remotely**
Collect targeted data in moments without disrupting the end-user

**Capture document activity**
File writes, document manipulations and deletions, plus printed activity.

**Capture advanced data loss indicators**
Identify transmittal of confidential materials into unmonitored channels

**Adapt on the fly**
Craft bespoke rules for new and unfolding situations to gain investigative insights

**Capture what the user is typing**
Targeted captures of text for alerting or lookback purposes

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

## Summary and questions

With this approach and solution, you benefit from:

- **Quickly identify anomalous behaviour** through evidence such as keypresses, files printed and screenshots, that cover user behaviours.

- **Mitigate financial loss, reputational damage and regulatory scrutiny** by being proactively alerted to issues and events as they happen rather than retrospectively.

- **Adapt the solution as your risk profile changes** by tailor alerts for different jurisdictions, business units and functions.

- **Enable digital forensic collections** of key evidence remotely, covertly and before it is inadvertently lost.

- **Reduce time and costs** by having both monitoring and investigation capabilities in one solution – avoiding current potentially cumbersome processes.

- **Corroborate other fraud monitoring controls** through evidence-based actions of the user.

# It’s what’s inside that counts: transforming investigations to detect and prevent insider threats

Questions?

## Speakers

### Armando Nardo

*Forensic Technology | Director – Digital Forensics*

Contact Information

☎ +44 20 7303 5791

✉ anardo@deloitte.co.uk

### Tom Coppock

*Forensic Technology | Manager – Digital Forensics*

Contact Information

☎ +44 20 7007 6153

✉ tcoppock@deloitte.co.uk

### Hoke Smith

*Nuix | VP, Cybersecurity*

Contact Information

☎ +1 571 446 2165

✉ hoke.smith@nuix.com

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.