



Leveraging RemoteOps & DataSet for At-Scale DFIR

KPMG LLP

RSA Conference 2023
April 26, 2023



Dennis Labossiere

Manager

Cyber Security Services



About Us

We help clients effectively and efficiently prepare for and respond to cyber incidents.

Our experienced team of digital forensic and incident response professionals assists in forensic analysis, digital investigations as well as breach preparation.

Our proactive consulting services include:

- Incident Response Plan and playbook development
- Incident response maturity assessments
- Cloud incident response orchestration & automation
- Cloud digital forensic lab development
- Threat hunting and monitoring



The Power of Partnership

- KPMG cyber response services and the Singularity platform help organizations gain visibility, protection, and response against advanced threats.
- KPMG Digital Responder (KDR) integrates with Singularity XDR to rapidly collect and analyze data.
 - IR teams can go back in time and perform true enterprise forensics, understand the root cause of attacks, remediate impacted assets, and return to productivity rapidly and completely.

*“The future of cybersecurity is autonomous, and **SentinelOne**, coupled with the industry experience of **KPMG**, helps prepare enterprises for tomorrow’s threat landscape. SentinelOne Singularity XDR can help our customers respond to incidents as well as collaborate on preventive services.”*

– David Nides, Principal, KPMG

Why KPMG + SentinelOne



Grab forensic artifacts at scale

Automate collection



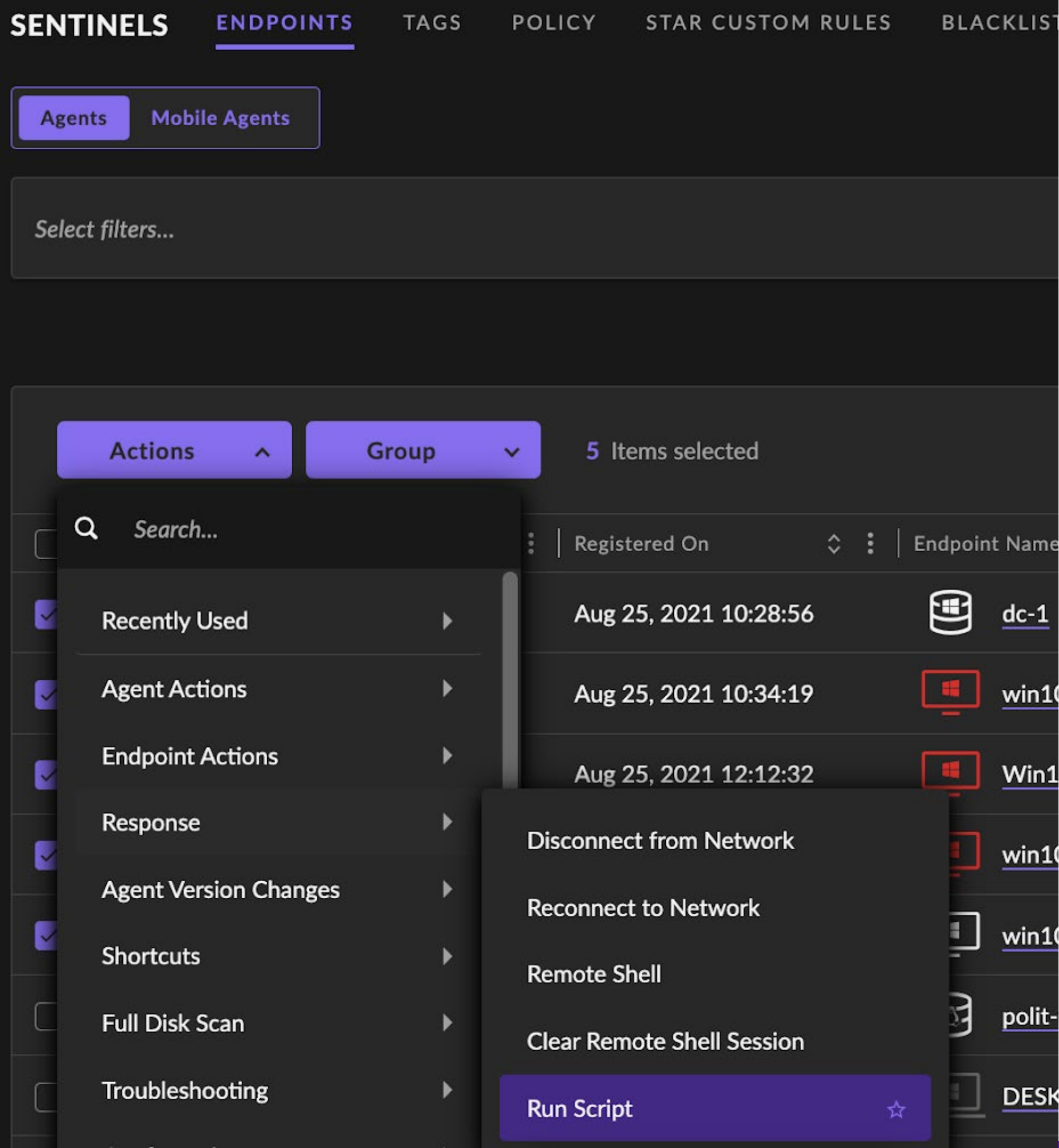
Analyze forensic artifacts at scale

Streamline analysis



Collaborate on forensics at scale

Scale security



Singularity™ RemoteOps

- Enables bulk execution of scripts from a Script Library.
- Scripts can be executed remotely and at scale.
- **How KPMG Uses It:**
 - Run forensic triage packages (e.g. KDR, third-party tools).
 - Collect one-off forensic artifacts (e.g. event logs, Amcache, etc.).
 - Perform compromise assessments (e.g. determine patching level, etc.).
 - Remediate malicious activity.
 - Make system changes or apply patches.
 - Integrate with STAR rules via API for automated response actions.

Singularity RemoteOps

SENTINELS

ENDPOINTS

TAGS

POLICY

STAR CUSTOM RULES

BLACKLIST

EXCLUSIONS

NETWORK CONTROL

DEVICE CONTROL

BENCHMARKS

PACKAGES

UPGRADE POLICY

SITE INFO

GROUP RANKING

Agents

Mobile Agents

Select filters...

Load Filter

Save Filter

Actions

Group

5 Items selected

5,008 Endpoints

50 Results

Columns

Export

Search...

Registered On

Endpoint Name

IP Addresses

Endpoint Tags

Account

Last Logged In User

Recently Used

Agent Actions

Endpoint Actions

Response

Agent Version Changes

Shortcuts

Full Disk Scan

Troubleshooting

Disconnect from Network

Reconnect to Network

Remote Shell

Clear Remote Shell Session

Run Script

Aug 25, 2021 10:28:56	dc-1	10.0.50.2	Live_Response : Pen...	United Synthetic Security and...	administrator
Aug 25, 2021 10:34:19	win10-1	10.0.50.10, 169.254.39.46	MD_Containment_AI...	United Synthetic Security and...	user1
Aug 25, 2021 12:12:32	Win10-2	10.0.50.20	Demo : ADA_demo	United Synthetic Security and...	user2
	win10-3	10.0.50.30	Demo : ADA_demo	United Synthetic Security and...	user3
	win10-4	10.0.50.40	N/A	United Synthetic Security and...	user
	polit-test	10.0.50.52	N/A	United Synthetic Security and...	N/A
	DESKTOP-IQLA2IH	10.0.2.6	N/A	United Synthetic Security and...	user

Singularity™ RemoteOps

AUTOMATIONTASKSREMOTE OPS

Today ▾





Select filters...

Bulk ViewSingle View

Actions ▾

No Items Selected

1 Items50 Results ▾Columns ▾

<input type="checkbox"/>	Task Name	Description	Initiated By	Initiated Time	Total In Current Scope	Completed	Failed	Pending
<input type="checkbox"/>	 Remote Script	PersistenceSniperSkylight2.0	Brad Roughan	Mar 16, 2023 08:55:47	5	 4	 0	 0

Singularity™ RemoteOps

Incident Response and/or Compromise Assessment



Script Library with variety of forensic scripts (e.g. autoruns, Amcache, PowerShell history, event logs, etc.)



Outputs sent to DataSet for parsing and querying



Pre-built dashboards for identifying quick wins

Script Configuration

SCRIPT SELECTION

INPUT / OUTPUT

TASK PARAMETERS

SUMMARY

PersistenceSniperSkylight2.0Data Collection1.0.1bradley.roughan+martumley@sentinelone.com

INPUT

Script Input

-token

'-IncludeHighFalsePositivesChecks

OUTPUT

Output Destination

None - No output handling needed

TASK PARAMETERS

Task Description

PersistenceSniperSkylight2.0

Script Execution Timeout

3600

Cancel

Submit & Add Another

Submit

Singularity RemoteOps Script Library

- Allows teams to store various scripts.
- Various pre-built scripts included.
- **How KPMG Uses It:**
 - Collect forensic artifacts.
 - Perform compromise assessments (e.g. determine patching level, etc.).
 - Remediate malicious activity.

Singularity RemoteOps Script Library

Script Configuration

SCRIPT SELECTION

INPUT / OUTPUT

TASK PARAMETERS

SUMMARY

PersistenceSniperSkylight2.0Data Collection1.0.1bradley.roughan+martumley@sentinelone.com

INPUT

OUTPUT

Script Input

-token

' -IncludeHighFalsePositivesChecks

Output Destination

None - No output handling needed

TASK PARAMETERS

Task Description

PersistenceSniperSkylight2.0

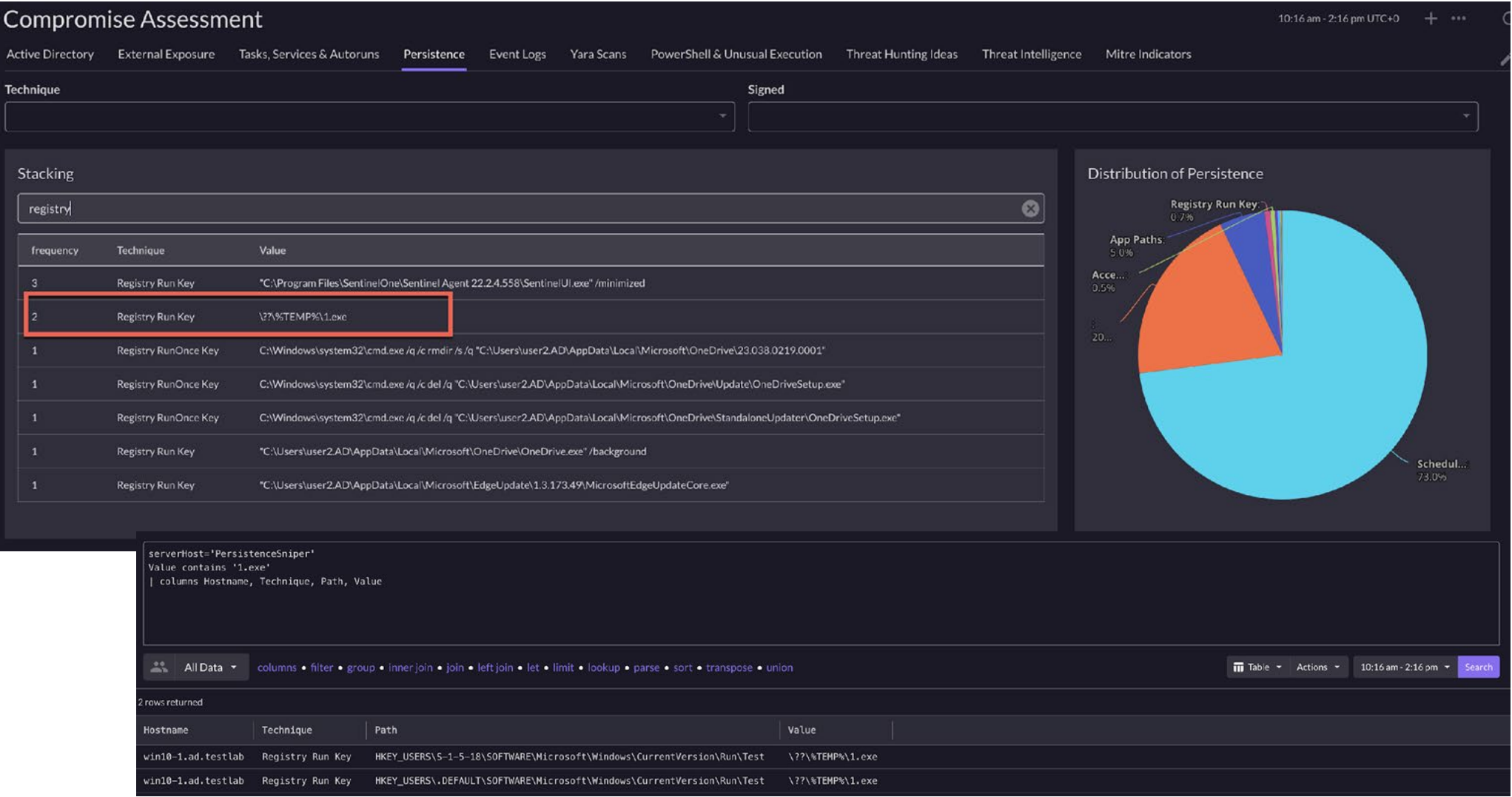
Script Execution Timeout

3600

Cancel

Submit & Add Another

Submit



DataSet

A cloud-native, flexible, analytics platform for structured or unstructured data.

- **How KPMG Uses It:**
 - Quickly ingest data at scale.
 - Collect data and/or forensic artifacts at scale.
 - Can be used to make system changes or apply patches.
 - Integrates with STAR Rules via API for automated response actions.

Compromise Assessment

Active DirectoryExternal ExposureTasks, Services & AutorunsPersistenceEvent LogsYara ScansPowerShell & Unusual ExecutionThreat Hunting IdeasThreat IntelligenceMitre Indicators

TechniqueSigned

```
serverHost='PersistenceSniper'
Value contains '1.exe'
| columns Hostname, Technique, Path, Value
```

All Data

columns • filter • group • inner join • join • left join • let • limit • lookup • parse • sort • transpose • union

Table Actions10:16 am - 2:16 pmSearch

2 rows returned

Hostname	Technique	Path	Value
win10-1.ad.testlab	Registry Run Key	HKEY_USERS\5-1-5-18\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Test	\\?\%TEMP%\1.exe
win10-1.ad.testlab	Registry Run Key	HKEY_USERS\DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Test	\\?\%TEMP%\1.exe

1Registry Run Key"C:\Users\user2.AD\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

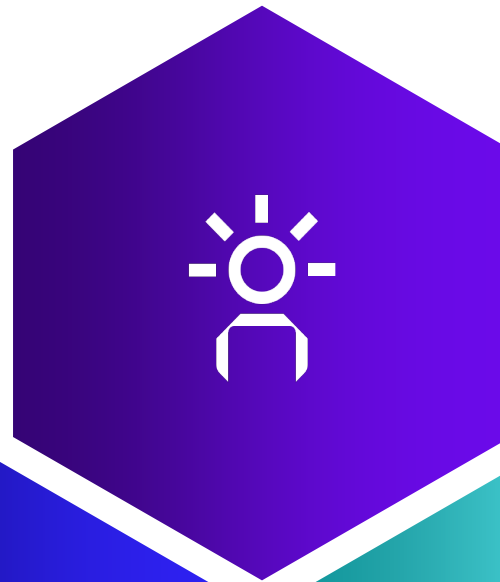
1Registry Run Key"C:\Users\user2.AD\AppData\Local\Microsoft\EdgeUpdate\1.3.173.49\MicrosoftEdgeUpdateCore.exe"

Schedul...73.0%

Value-Add For KPMG Clients

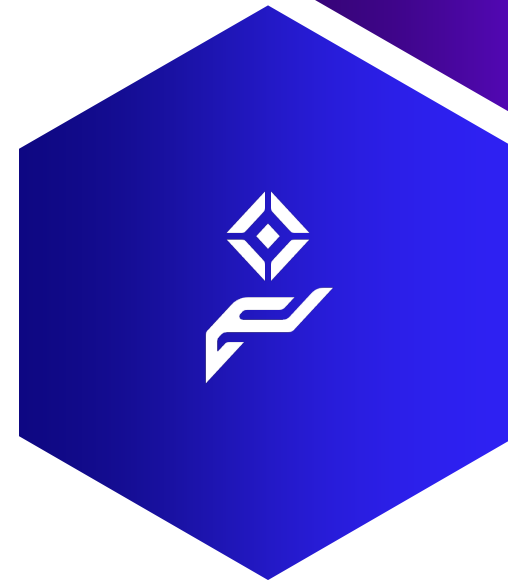
Creative

Possibilities are limitless



Simple

**As simple as a few clicks
within the console**



Powerful

**Collect and analyze data
within minutes**



Thank You

Contact Us

David Nides, Principal – dnides@kpmg.com

Jonathan Fairtlough, Principal – jfairtlough@kpmg.com

Dennis Labossiere, Manager – dlabossiere@kpmg.com



SentinelOne[®]



sentinelone.com
kpmg.com/us/cyber