

My time at Sands

Michael Opoku-Arthur



SANDS CAPITAL

Cybersecurity Intern

Matt, Naji, TerpSys



Alert Triaging & Threat Hunting

- Microsoft Sentinel (SIEM)
- Microsoft Defender (XDR)
- DarkTrace (NDR)

Collaboration

- Meeting with Ryan Bateman
- Meeting with Nick Martin
- Shadowing Andrew Hartman
- Tabletop simulation

HoxHunt

- Phishing Training Platform

Technical Skills Development

- KQL
- Python scripting

Alert Triaging & Threat Hunting

Rules and policies are established within our various security tools to protect the firm's environment. When an event triggers one of these rules or policies, our systems flag the incident, an alert is generated, and it is logged into our SIEM (Microsoft Sentinel)

- Alert Triaging
 - Reviewing, prioritizing and filtering out incidents
- Threat Hunting
 - Investigating further any incident that may stand out
- Memorable Moment:
 - Taking over the duty of monitoring Sentinel board

Alert Triaging

Microsoft Azure

Home > Microsoft Sentinel

Microsoft Sentinel | Incidents

Selected workspace: 'scm-security-sentinel'

Search

Create incident (Preview) Refresh Last 24 hours Actions Delete Security efficiency workbook Columns Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)
- SOC optimization

Content management

- Content hub
- Repositories (Preview)
- Community

Configuration

- Workspace manager (Preview)
- Data connectors
- Analytics

6 Open incidents 5 New incidents 1 Active incidents

Open incidents by severity

High (0) Medium (5) Low (1) Informational (0)

Search by ID, title, tags, owner or product

Severity: All Status: All Incident Provider name: All Alert product name: All Owner: Assigned to me

Auto-refresh incidents

Severity	Incident number	Title	Alerts	Incident provider na...	Alert product name	Created time	Last update time	Owner	Status
Medium	12987	Darktrace: 30.0 - System/Inactive Clie...	1	Azure Sentinel	Microsoft Sentinel	08/02/24, 12:10 PM	08/02/24, 01:46 PM	Michael Opoku-Art...	Closed
High	12988	Privileged Accounts - Sign in Failure ...	1	Azure Sentinel	Microsoft Sentinel	08/02/24, 12:36 PM	08/02/24, 01:45 PM	Michael Opoku-Art...	Closed
Medium	12985	Darktrace: 30.0 - System/Inactive Clie...	1	Azure Sentinel	Microsoft Sentinel	08/02/24, 11:00 AM	08/02/24, 11:10 AM	Michael Opoku-Art...	Closed
Medium	12970	Darktrace: 43.0 - Anomalous Connec...	1	Azure Sentinel	Microsoft Sentinel	08/01/24, 02:25 PM	08/02/24, 10:52 AM	Michael Opoku-Art...	Closed
Medium	12971	Darktrace: 79.0 - Antigena/Network/...	1	Azure Sentinel	Microsoft Sentinel	08/01/24, 02:25 PM	08/02/24, 10:49 AM	Michael Opoku-Art...	Closed
Low	12977	Email reported by user as malware or...	1	Azure Sentinel	Microsoft Defender f...	08/02/24, 01:26 AM	08/02/24, 10:44 AM	Michael Opoku-Art...	Active
High	12972	Possible SSL Command and Control t...	1	Azure Sentinel	Microsoft Sentinel	08/01/24, 02:30 PM	08/02/24, 10:44 AM	Michael Opoku-Art...	Closed
Medium	12984	Darktrace: 22.0 - SaaS/Access/Box Ac...	1	Azure Sentinel	Microsoft Sentinel	08/02/24, 10:05 AM	08/02/24, 10:33 AM	Michael Opoku-Art...	Closed
Medium	12978	Darktrace: 30.0 - System/Inactive Clie...	1	Azure Sentinel	Microsoft Sentinel	08/02/24, 02:50 AM	08/02/24, 10:18 AM	Michael Opoku-Art...	Closed
Medium	12974	Darktrace: 36.0 - SaaS/Access/Box Ac...	1	Azure Sentinel	Microsoft Sentinel	08/01/24, 04:30 PM	08/02/24, 10:17 AM	Michael Opoku-Art...	Closed
Medium	12973	Darktrace: 50.0 - Compromise/Tor D...	1	Azure Sentinel	Microsoft Sentinel	08/01/24, 02:55 PM	08/02/24, 10:17 AM	Michael Opoku-Art...	Closed
Medium	12975	Darktrace: 64.0 - Compromise/Doma...	1	Azure Sentinel	Microsoft Sentinel	08/01/24, 09:00 PM	08/02/24, 10:17 AM	Michael Opoku-Art...	Closed
Medium	12979	Darktrace: 60.0 - Compromise/Doma...	1	Azure Sentinel	Microsoft Sentinel	08/02/24, 03:30 AM	08/02/24, 10:15 AM	Michael Opoku-Art...	Closed

< Previous 1 - 15 Next >

Darktrace: 30.0 - System/Inactive Client Sensor Agen...

Incident number 12987

Michael Opoku... Owner Closed Status Medium Severity

Description

A client sensor agent appears to be inactive. This could be a result of general failures in agent connectivity (e.g. the device may be powered down or not connected to the internet) or potential agent tampering.

Action: Review the device and determine if such behaviour was expected.

Alert product names

- Microsoft Sentinel

Reason for closing

Benign Positive - Suspicious but expected

Inactive DT agent

Evidence

1 Events 1 Alerts 0 Bookmarks

Threat Hunting

Microsoft Azure

Search resources, services, and docs (G+)

Home > Microsoft Sentinel | Incidents >

Darktrace: 66.0 - Compromise/Tor Domain DNS Requests

Incident number 12924

Refresh

Delete incident

Logs

Tasks

Activity log

This is the new, improved incident page - Now generally available. You can use the toggle to switch back.

Medium

Closed

Michael Opo...

Workspace name

scm-security-sentinel

Description

A device is making DNS requests for .onion Tor domains. This is commonly seen with malware command and control as well as ransomware payments.

Action: Review the domain being requested and the other behaviours from the device by viewing the device's activities and previous breaches.

Alert product names

Microsoft Sentinel

Reason for closing

BenignPositive - Suspicious but expected

PA performing DNS lookups for blocklists

Evidence

1 Events

1 Alerts

0 Bookmarks

Last update time

7/31/2024, 6:26:42 PM

Creation time

7/31/2024, 2:50:18 PM

Entities (1)

10.2.200.252

Tactics and techniques

Overview

Entities

Incident timeline

Jul 31 14:44:40 Darktrace: 66.0 - Compromise, Med... | Detected by Microsoft... | Ti

Similar incidents

Severity Incident number Title

Medium 12736 Darkt...

Logs

scm-security-sentinel

Run Time range: Custom Share Export

```
1 // might contain sensitive data
2 let alertedEvent = datatable(compressedRec: string)
3 [
4   eAG1V1uP4jYU/iTW+tCXDZNAHHe2GE6RZoZiAd70GWFjHMAdxw7tR3YaLX/vcd2woTZV1VVcFw5X75znG/RG1SVdp5Hk2gAyXg/Z1mcDoa70Mv2
   +5ju6TiGPq07wTB3K+Ew+hctVKUznGpjoUctJRG7XcyR8fyIR/dLT1AAAdI+a1WVL75AwFjzAh58gqYwnMN+0s/15C4ep0t0NMMySZb0smzYT9PB7yh
   +r4qysqCD8pKeZ9T5CCKB1KT1VDJ7oDsTMBKqx1FbG+WspBWMudprYugpYAMr86FkVXkop5vj0ECs8x8b7noF5Zy1w/
   cVuJTEm5uAySPlyjfkynjeh2F01KjcsHyHrLtsMVRRU1++0v3Bt7Aq9AqbW815Ch851e7PEKq3b6165XWg4cVUZzzFXrBVTGrZ5a8LT7rEPB/
   UWxQ5b0UMLDL0rPS1wLZTL9KRZMu01RR1V63UXG1XAKbyjuMLuRFBwQncueMHrbc3EcX7TnF7BnpV+X1YCKqg5bNy0R70Eo6x4aNyI3ebZPsv18WA/
   jro7JItHab6Ld0nez/
   Lb8V3az13FuryDgqR0uXhJkSnC3HMa4qDjVwVKz1xhuZEKqP2XEP2VBRAtjbnK0D2fcdhZH+VOP1b7KBs0B8GLYzQ11vp85m54JdwQw611g1s5cV0fBnhY0wZK8065mJ
   5WF3NVUCSNj6yPqIBv jKRQUlTEAEhy5vaIZs5ZavAsKnP1PkxJq5Ug1JAzCP+rKUzbeMm51m5S0exGbqRDrZITs5TA4EzsERq3ZAcuv1Y2CjYdW
```

Results

Chart

Add bookmark

TimeGenerated [UTC]

antigena_b

breachUrl_s

SrcIPAddr

10.2.200.252

SrcPortNumber

0

tags_s

AP: C2 Comms

TenantId

3e09f9c4-135b-44ff-afa9-e2cab3501055

ThreatCategory

Policy Breach

ThreatId

484553

ThreatName

Compromise/Tor Domain DNS Requests

ThreatRiskLevel

66

TimeGenerated [UTC]

2024-07-31T18:44:40.4452113Z

triggeredComponents_s

DNS Requests

Destination IP: 8.8.8.8

DNS host lookup: 76jdd2r2embyv47.onion

Type

darktrace_model_alerts_CL

typeLabel_s

Palo Alto -Ash1

uuid_g

8c6d444-93f9-4704-81db-b0d2d469712d

google.com

GOOGLE, US

Seen 20000+ times between August 2nd, 2024 and August 2nd, 2024.

Live Screenshot

Bevor Sie zu Google weitergehen

General Info

Geo: United States (US)

AS: AS15169 - GOOGLE US

Registrar: ARIN

Route: 142.250.0.0/15

PTR: fra2404-in-f14.1e100.net

IPv4: 142.250.186.46

IPv6: 2a00:1450:4001:808::200e

Direct hits

Summary of pages hosted on this domain

Recent scans (10000 total)

URL Age Size IPs

Incoming hits

Summary of pages that talked to this domain

Recent scans (10000 total)

URL Age Size IPs

google.com

1 / 93

Community Score

1/93 security vendor flagged this domain as malicious

Home > Sands Capital | Devices > Devices

Devices | All devices

Sands Capital - Microsoft Entra ID

searchengines search engines search engines and portals top-1K

DETECTION

DETAILS

RELATIONS

COMMUNITY 30+

Recorded Future

THREATRECOPIES Sandbox

Submit Organization Reports

Static static 1 URLScan urlscan

Live Monitor

Select an active session to interact with or open the report of a completed analysis.

https://www.google.com

macos-10.15-amd64

https://www.google.com

Chrome

File Edit View History Bookmarks Profiles Tab Window Help

Google

Google Chrome isn't your default browser

About Store

Sign in to Google

Google Search I'm Feeling Lucky

Discover what sports fans are searching for

Our third decade of climate action: join us

Extend analysis

Terminate

Mouse Simulation

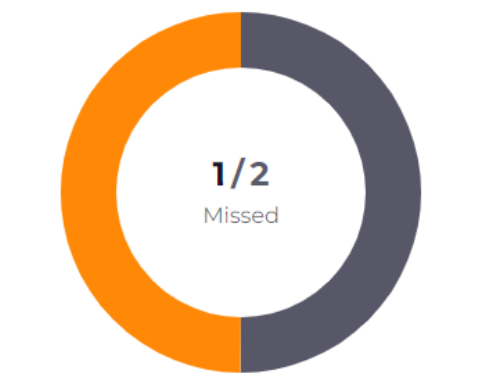
Fullscreen

HoxHunt

Benchmark overview

Created: 7/16/2024
Scheduled for: 10:00 7/17/2024
Target: 2 users
Simulation: [service.microsoft.yammer.discover.lp.AD](#)

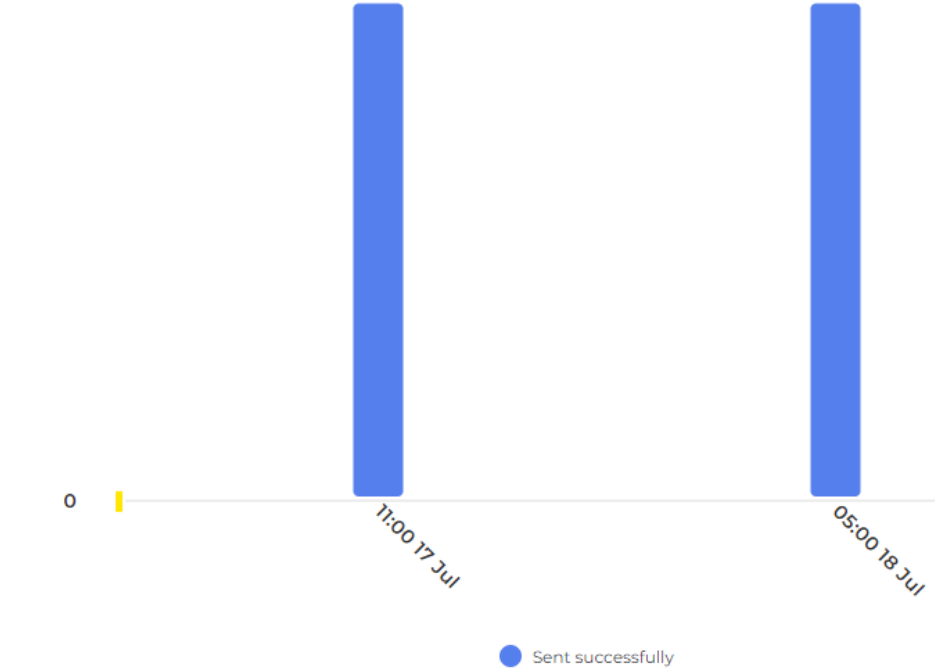
Delivery Performance



- 50% Missed
- 50% Attempts at entering credentials

Scheduled sending times

Overview of benchmarks sent to users each hour ⓘ



[TEST] Discover what's happening across your organization.

Frank Sands on Yammer <notifications@yammer.company>
To: @ Michael Opoku-Arthur [Intern] Tue 7/16/2024 3:22 PM

Sands Capital Management Yammer

Posted in All Company

FS Frank Sands

Hello all, I'm excited to share the news about the future of our organization with you. Over the past few months, we have been carefully considering how we can structure our company to better align with our goals and values. After much consideration, we have decided to...

[Go to conversation](#)

Explore communities today

HoxHunt



Intern Phish 3

Waiting for results

Benchmark overview

Created: 7/31/2024

Scheduled for: 13:00 7/31/2024

Target: 5 users

Simulation: [service.microsoft.mailboxExpiry.AD](#)

Delivery

Performance

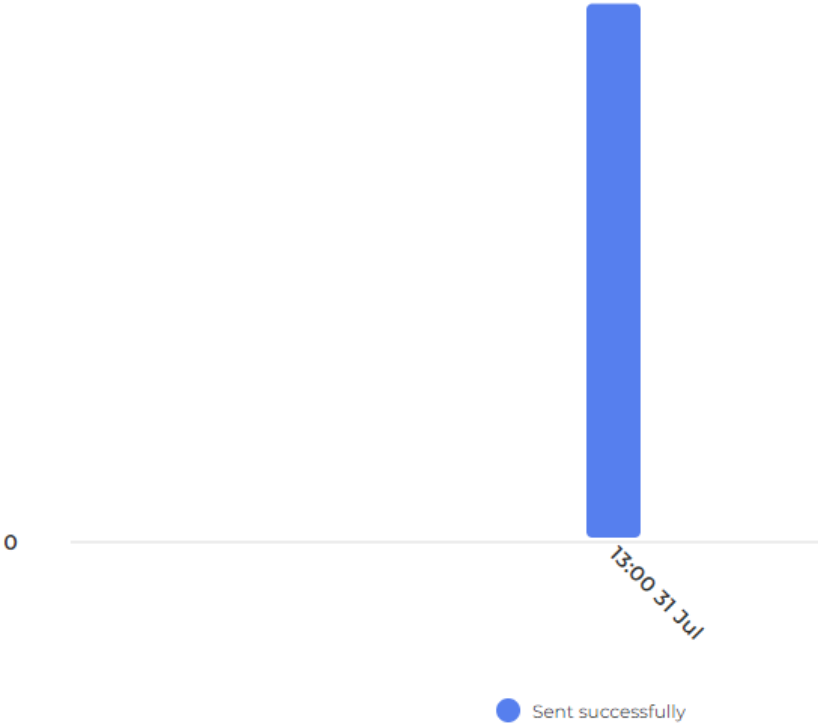


40% Succeeded

60% Pending

Scheduled sending times

Overview of benchmarks sent to users each hour ⓘ

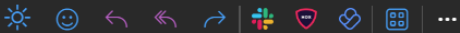


[TEST] Michael Opoku-Arthur: Your Mailbox is expiring soon.



Microsoft <noreply@mirconsoft.com>

To: ☹ Michael Opoku-Arthur [Intern]



Mon 8/5/2024 10:00 AM



Your Mailbox is expiring soon.

Dear Michael Opoku-Arthur:

Your Sands Capital Management mailbox will expire on Wednesday, Aug 7, 2024. To avoid losing any important emails or data, please upgrade your mailbox below.

[Upgrade Your Mailbox](#)

Please take action before the expiry date to avoid any disruption to your email service. If you have any questions or concerns, please contact our [Support Team](#).

[f](#) [t](#) [v](#) [in](#)

[Privacy Statement](#)

One Microsoft Way, Redmond, WA 98052, USA



HoxHunt

Benchmark overview

Created: 8/5/2024

Scheduled for: 15:00 8/5/2024

Target: 22 users

Simulation: service.microsoft.copilot.AD

Delivery

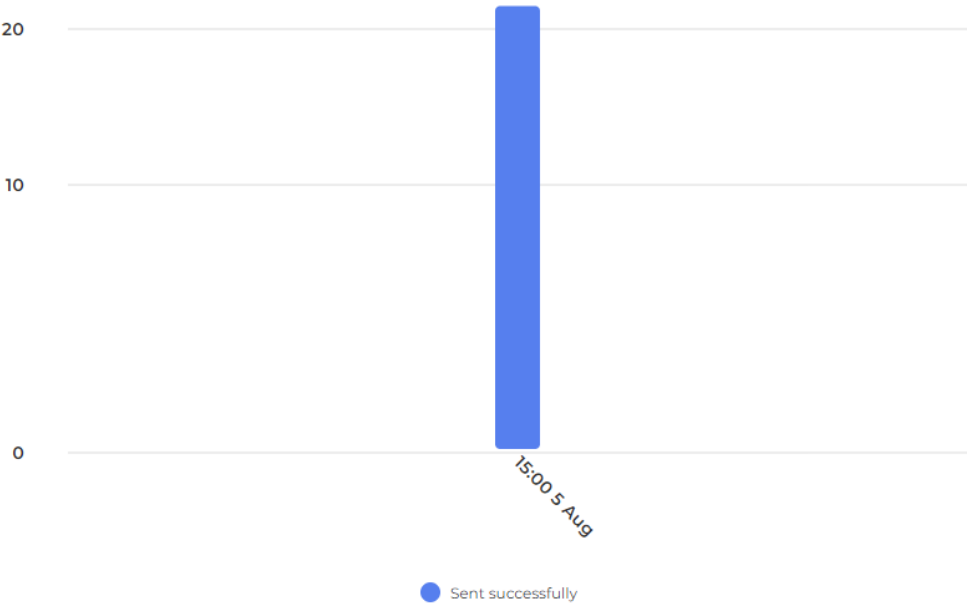
Performance



- 27% Succeeded
- 73% Pending

Scheduled sending times

Overview of benchmarks sent to users each hour ⓘ



MC

M365 Copilot <welcome@microsoft-365.com>

To: @ Michael Opoku-Arthur [Intern]

Mon 8/5/2024 3:00 PM



Dear Michael Opoku-Arthur,

You have been invited to start using the M365 Copilot!

Work smarter, be more productive, boost creativity, and stay connected to the people and things in your life with Copilot — an AI companion that works everywhere you do and intelligently adapts to your needs.

To get started, sign in to the Sands Capital Management Workspace by clicking the invitation link below.

Start using Copilot

Please note that this link will expire in 7 days.

Thank you,
The Microsoft Copilot Team

[Privacy Statement](#)
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

HoxHunt

Benchmark overview

Created: 8/5/2024
Scheduled for: 15:03 8/5/2024
Target: 4 users
Simulation: [service.github.vulnerabilityFound.lp](#)

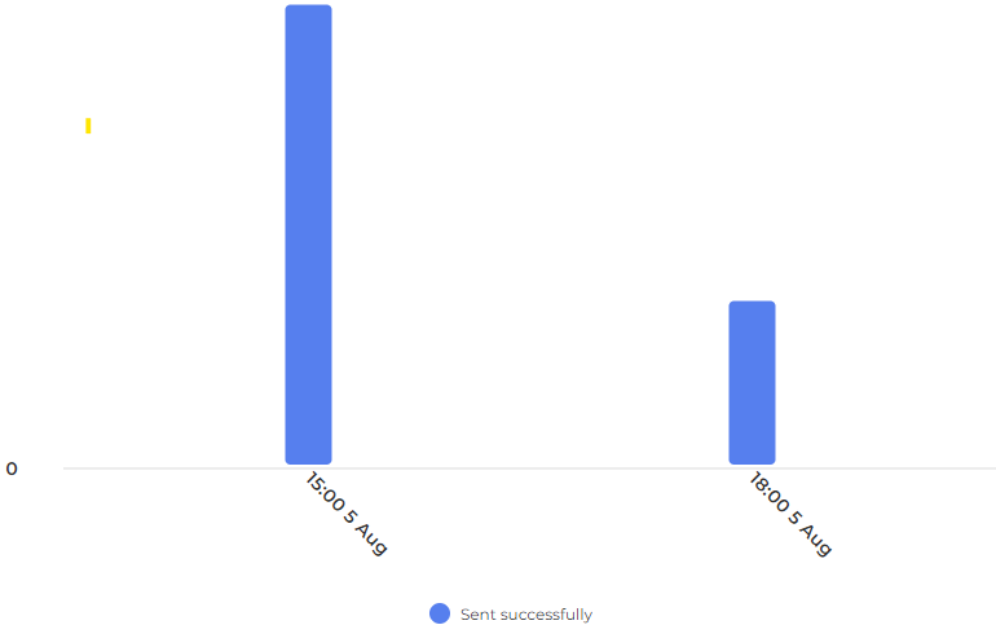
Delivery Performance



100% Sent

Scheduled sending times

Overview of benchmarks sent to users each hour ⓘ



GN

Github Notification<notifications@email-github.com>

To: ⓘ Michael Opoku-Arthur [Intern]

Mon 8/5/2024 2:51 PM



1 repository in your GitHub account might be affected by a security vulnerability found in express



Unencrypted credentials found in HTTP responses sent by express

High severity

express

CVE-2024-224499

View all alerts

`.github/webhook/cred-check`

• [Express.lock](#)

Collaboration – Ryan Bateman

- Key takeaways:
 - CISO & CTO
 - History of Sands IT Team
 - Received advice as an aspiring cyber professional
 - Learned about his journey into IT within the Financial Services Industry
 - Tabletop Simulation

Collaboration – Nick Martin

- Key Takeaways
 - Director of AI Solutions
 - Crash course of AI
 - Addressed common misconceptions
 - Discussed how he has implemented AI within the firm and how he plans to continue

Collaboration – Andrew Hartman

- Key Takeaways:
 - DMZ Takedown
 - Setup of Canary Honeypots
 - Sentinel alert deep dive

Technical Skill Development

- **KQL (Kusto Query Language)**
 - a query language used to interact and analyze data sets within Microsoft products
 - KQL training allowed me to understand the common functions, operators, and statements to efficiently query our datasets and logs

Intro to KQL - scm-security-sentinel

scm-security-sentinel

EditOpenSaveRefreshShareHelpAuto refresh: Off

WelcomeOverviewScalar OperatorsAdvanced AggregationsDataset OperatorsExternal DataString OperatorsAnomaly OperatorsMisc. Operators

Select SectionProjectAway

ExerciseProjectAwayEx1

DatasetWeather

Show DocumentationNo

Show AnswerNo

Seeing ErrorNo

Question

Return all records excluding the High column from the Weather table

Put your answer here

Weather
|project-away High

Results

Expected Results

TimeGenerated	Low	Rain	Location
6/29/2015, 8:00:00.000 PM	72	2.26	Houston
6/29/2015, 8:00:00.000 PM	64	0	Indianapolis
6/29/2015, 8:00:00.000 PM	68	0	New York City
6/29/2015, 8:00:00.000 PM	67	1.5	Philadelphia
6/29/2015, 8:00:00.000 PM	59	0	Seattle
6/28/2015, 8:00:00.000 PM	76	0	Houston

Your answer

TimeGenerated	Low	Rain	Location
6/29/2015, 8:00:00.000 PM	72	2.26	Houston
6/29/2015, 8:00:00.000 PM	64	0	Indianapolis
6/29/2015, 8:00:00.000 PM	68	0	New York City
6/29/2015, 8:00:00.000 PM	67	1.5	Philadelphia
6/29/2015, 8:00:00.000 PM	59	0	Seattle
6/28/2015, 8:00:00.000 PM	76	0	Houston

match

Answer is Correct

Results were limited to the first 500 rows.

Results were limited to the first 500 rows.

Technical Skill Development

- Script Refactoring - Mini project that I worked on with Naji
 - Refactor the script we use to generate the data for our weekly security meetings
 - Eliminate Tech Debt/Reliance on Python 3.7
 - One objective was to integrate the Azure Key Vault API into the script so that we are securely storing our secret keys and pulling for Azure compared to storing keys in the code

```
with open("config.json") as item_to_read:
    json_config_object = json.load(item_to_read)
    TOP_PATH = json_config_object["TOP_PATH"]
    TODAY_PATH = os.path.join(TOP_PATH, DATE_COMMON)
    ATP_SECRET = json_config_object["TOP_PATH"]
```

```
34 credential = DefaultAzureCredential()
35 secret_client = SecretClient(vault_url="https://[REDACTED].vault.azure.net/", credential=credential)
36
37 Tenant_ID = secret_client.get_secret("TenantID").value
38 App_ID = secret_client.get_secret("AppID").value
39 App_Secret = secret_client.get_secret("AppSecret").value
```



sandscapital.com