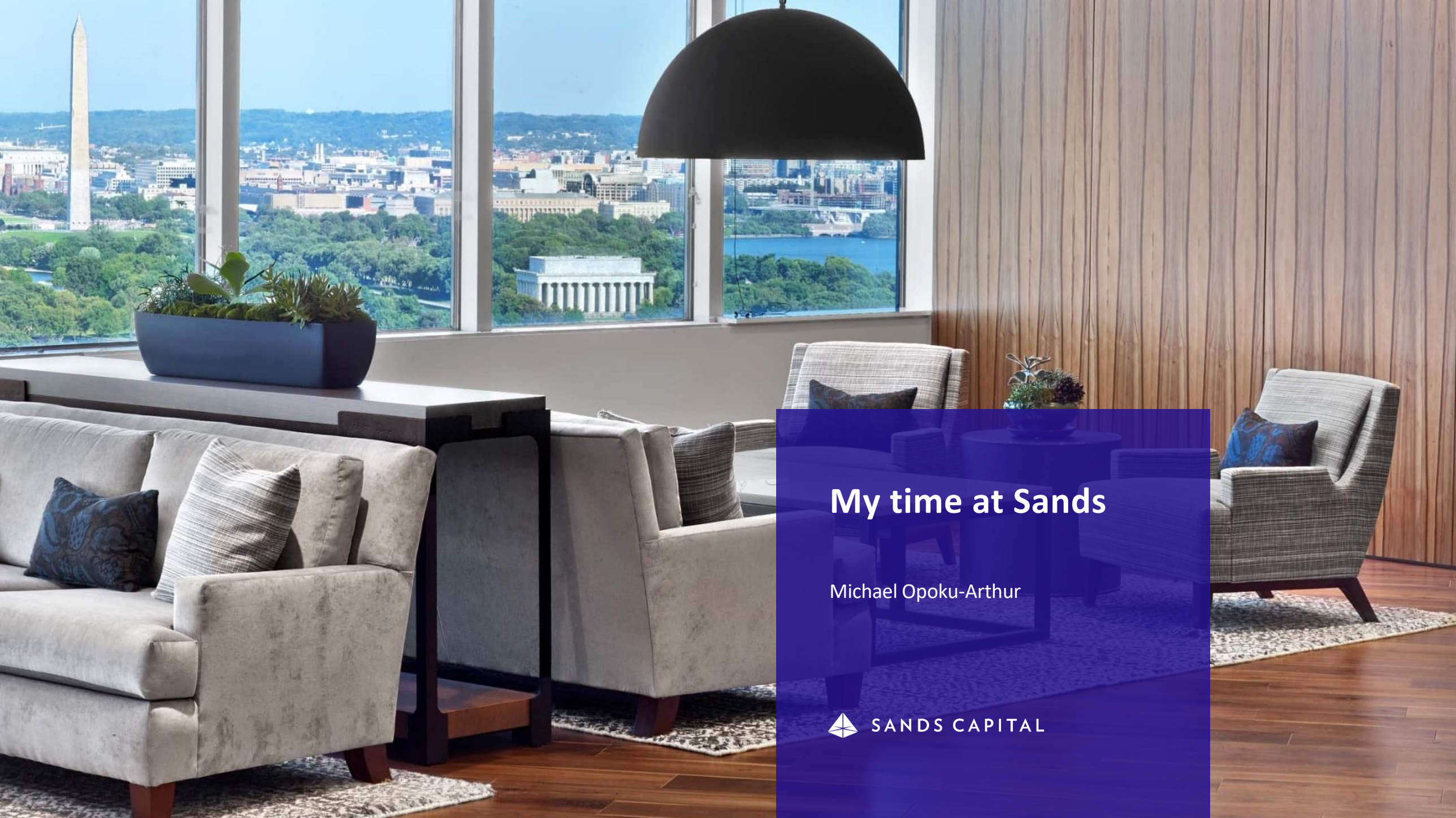


My time at Sands

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

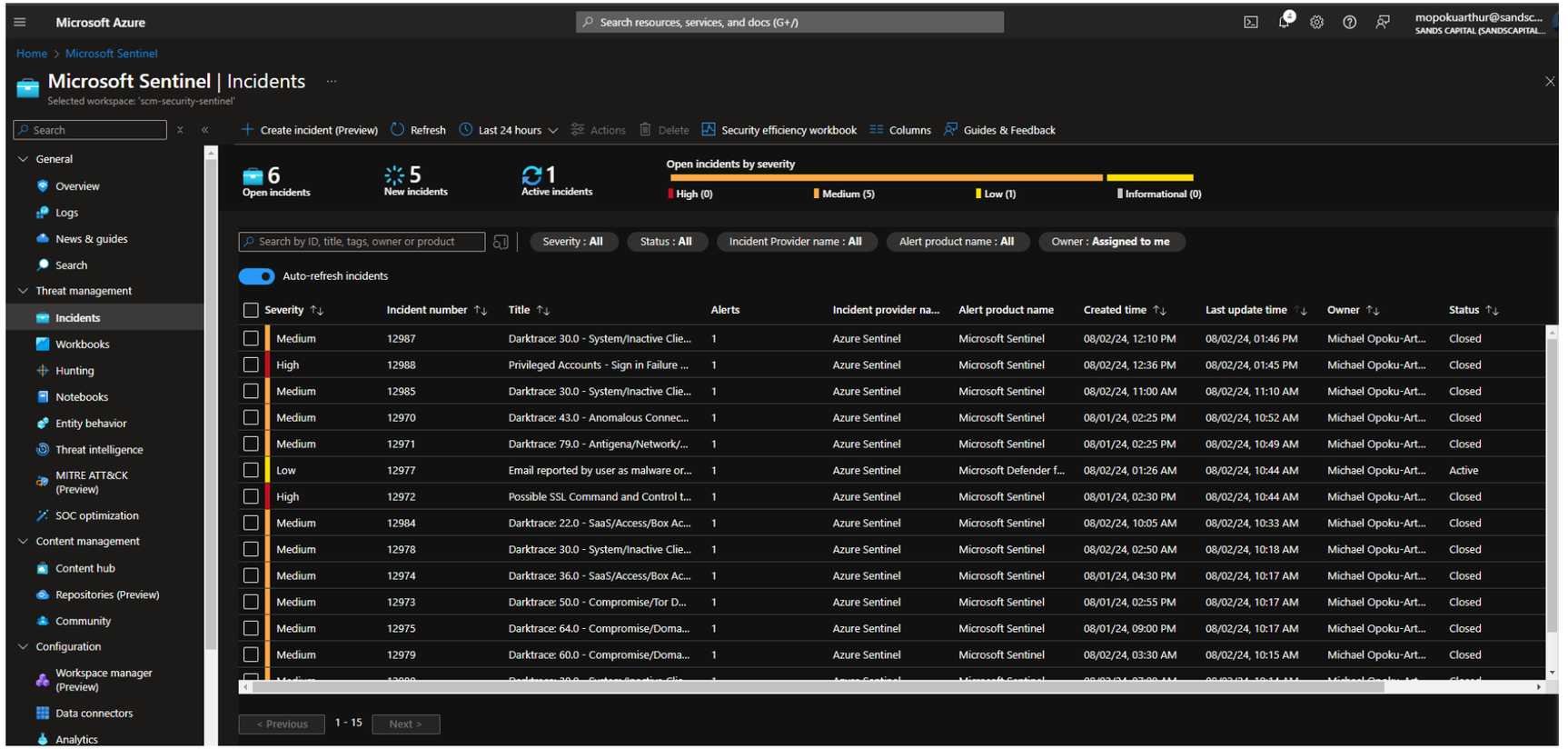
- KQL
- Python scripting

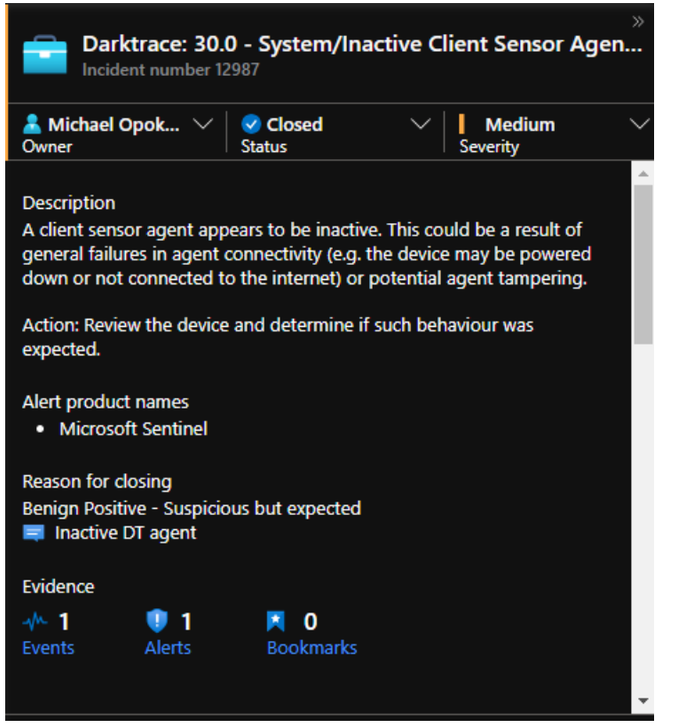
Alert Triaging & Threat Hunting

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)

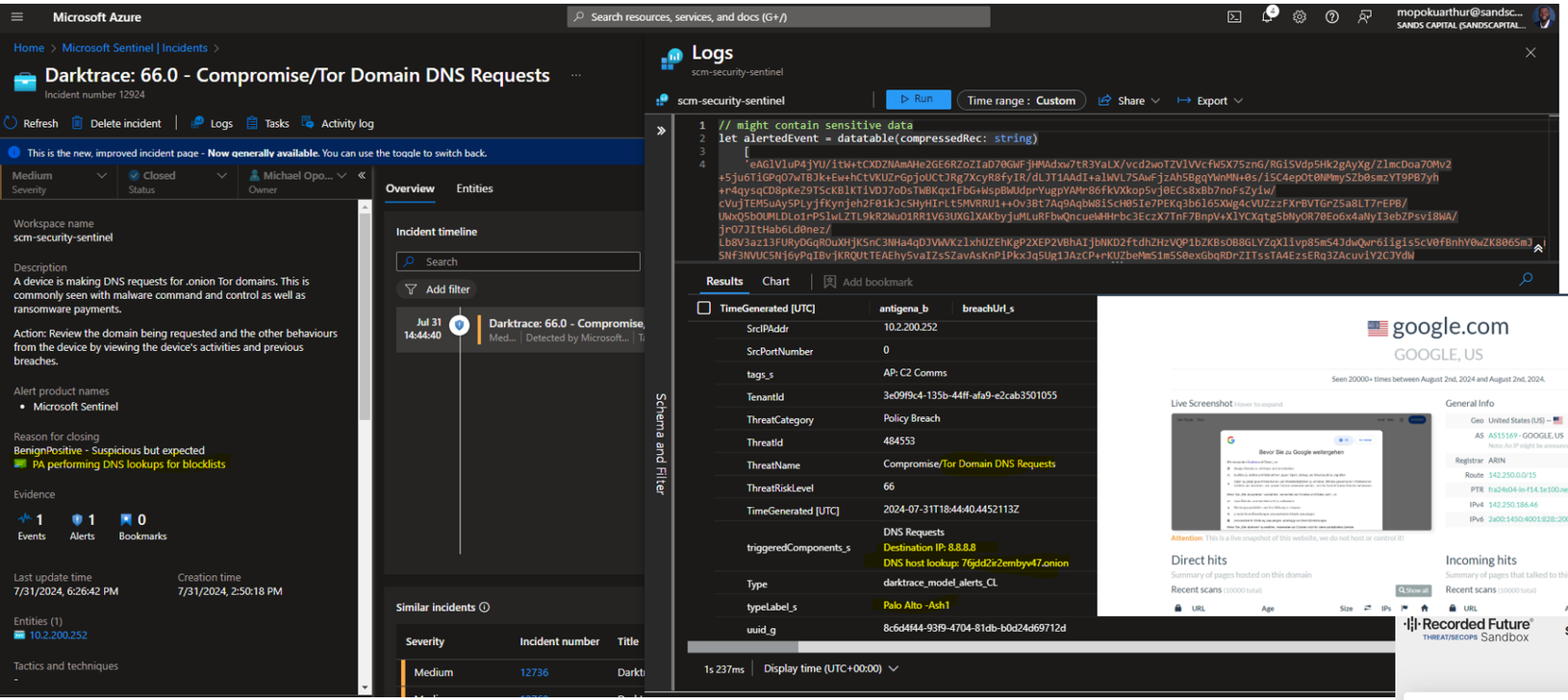
- Alert Triaging
  - Reviewing, prioritizing and filtering out incidents
- Threat Hunting
  - Investing further any incident that may stand out
- Memorable Moment:
  - Taking over the duty of monitoring Sentinel board

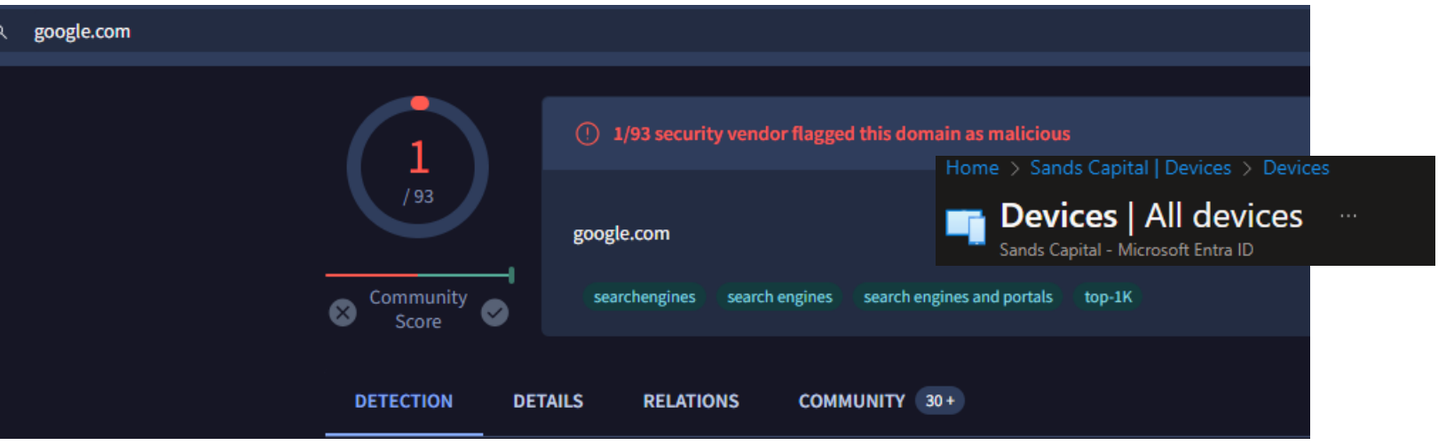
Alert Triaging

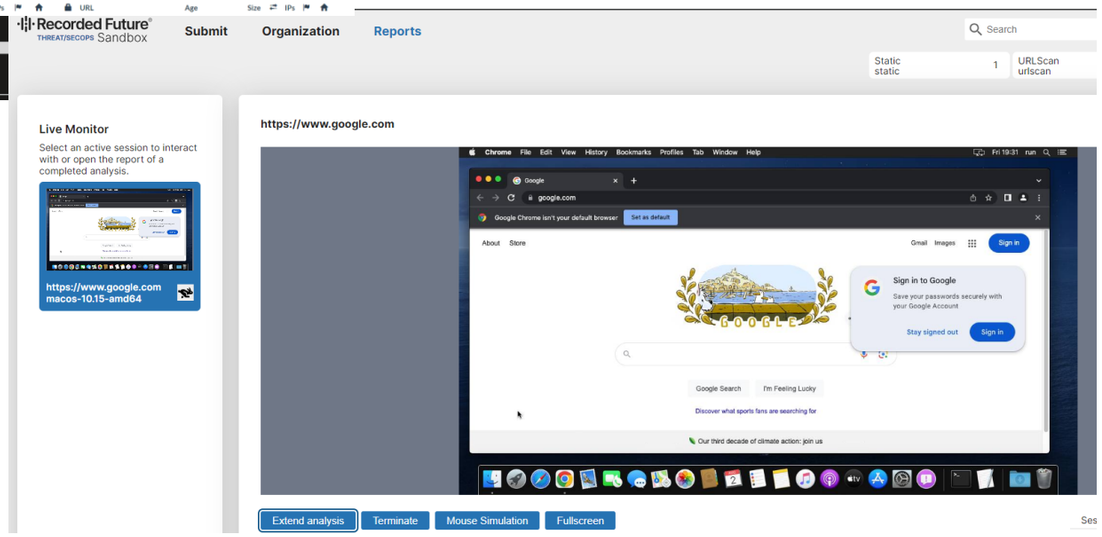




Threat Hunting







HoxHunt

Benchmark overview

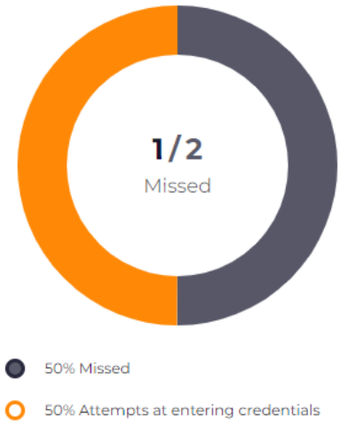
Created: 7/16/2024

Scheduled for: 10:00 7/17/2024

Target: 2 users

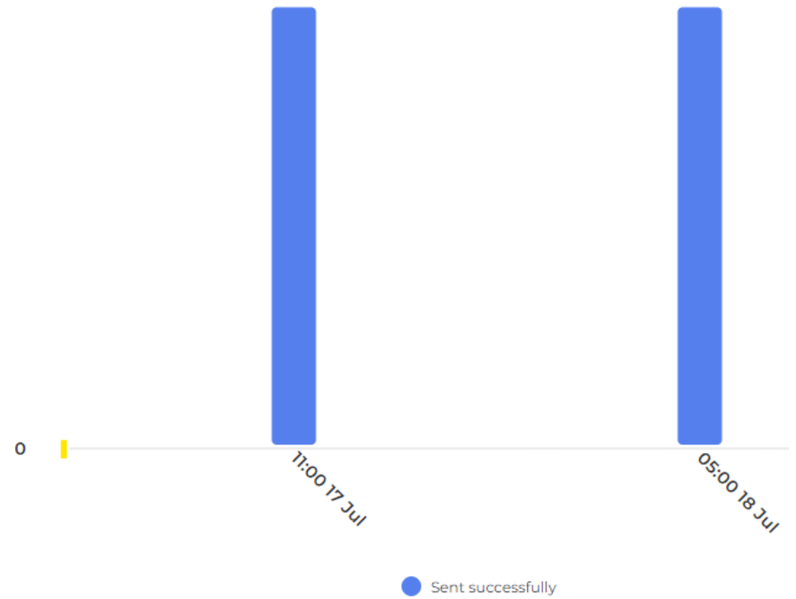
Simulation: service.microsoft.yammer.discover.lp.AD

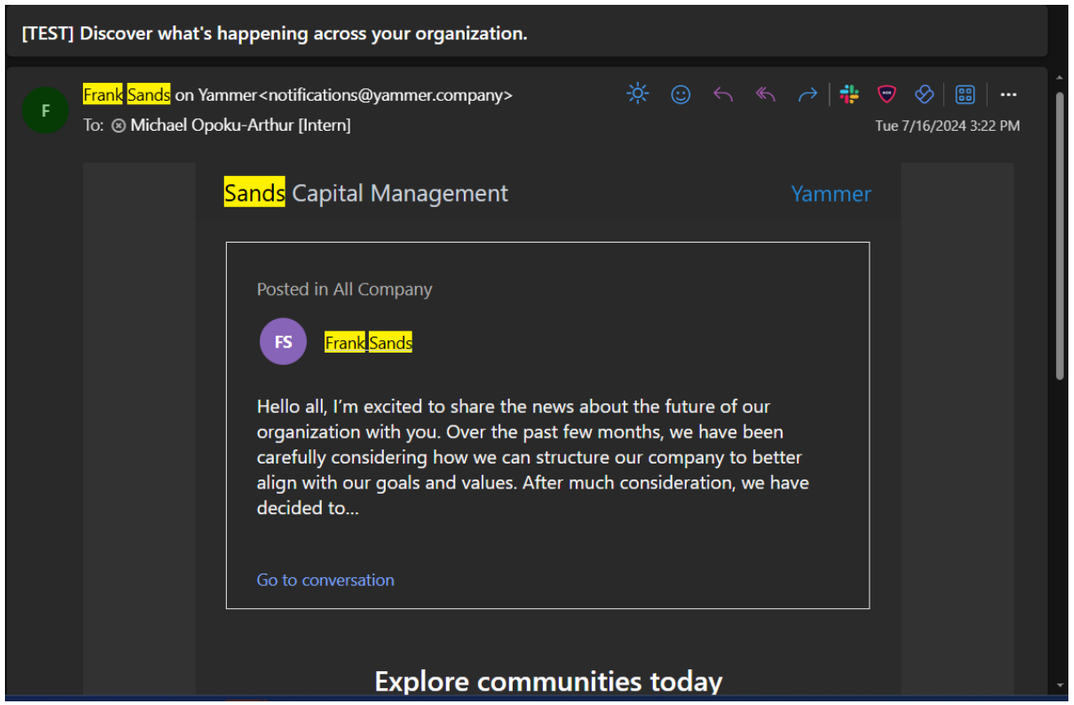
Delivery | Performance



Scheduled sending times

Overview of benchmarks sent to users each hour





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

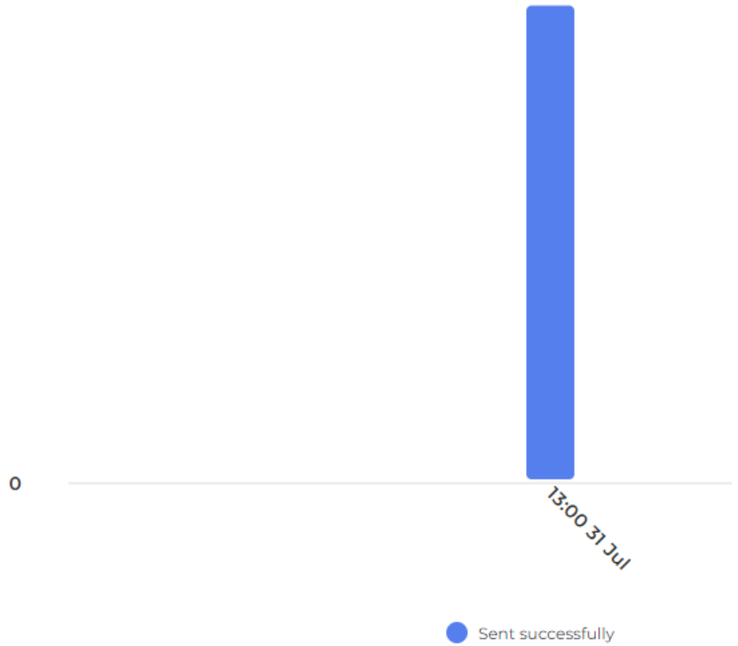
Delivery | Performance

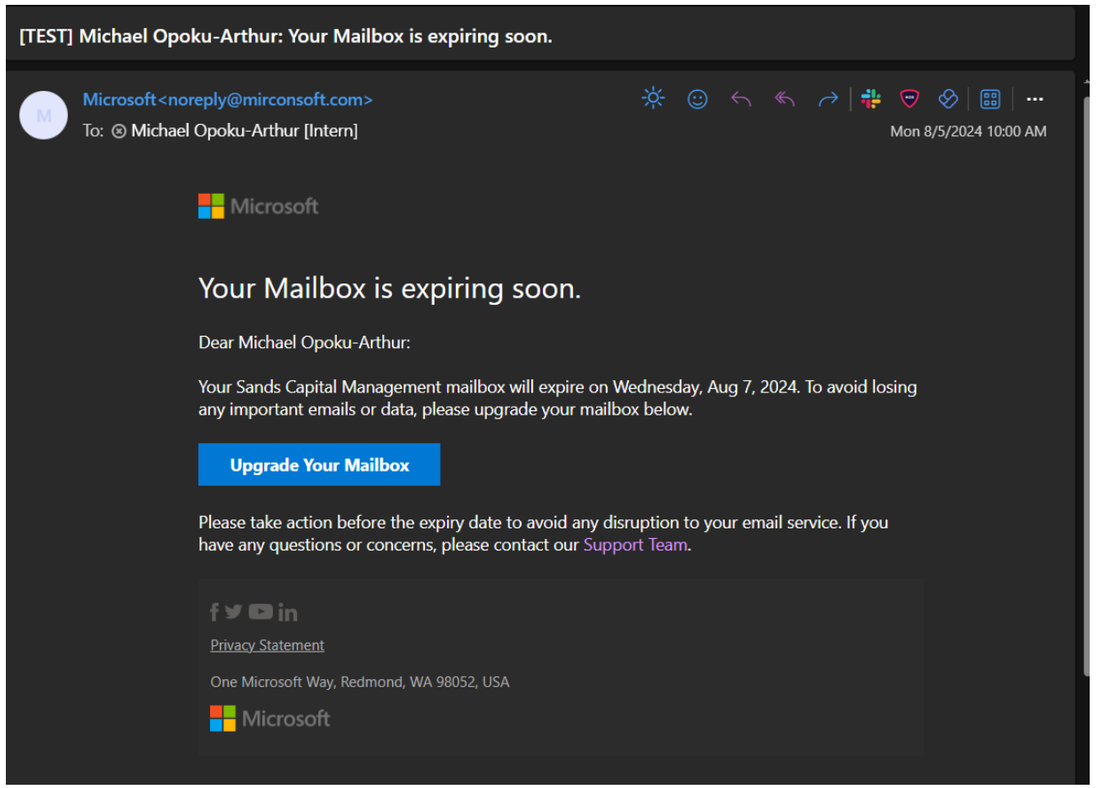
40% Succeeded

60% Pending

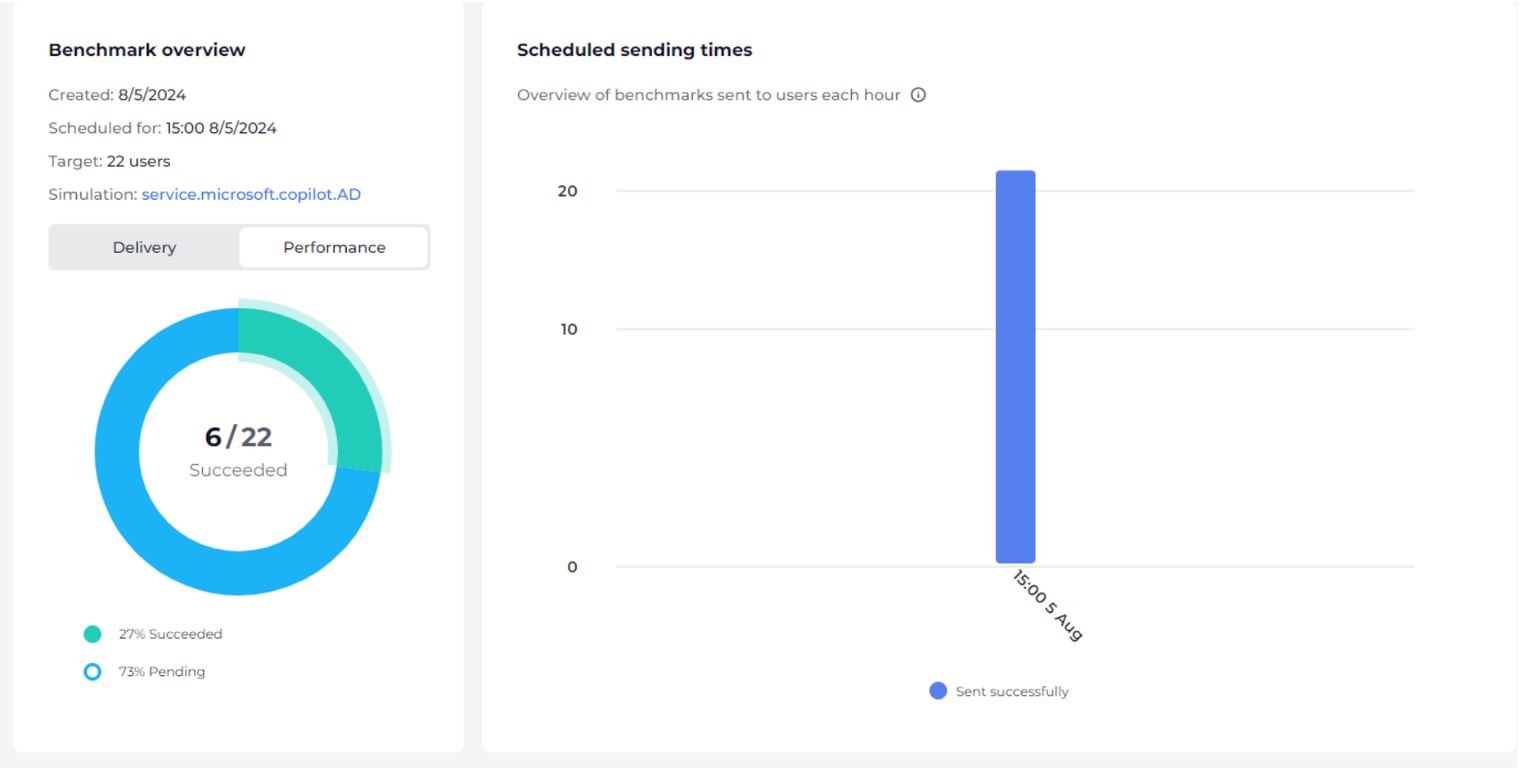
Scheduled sending times

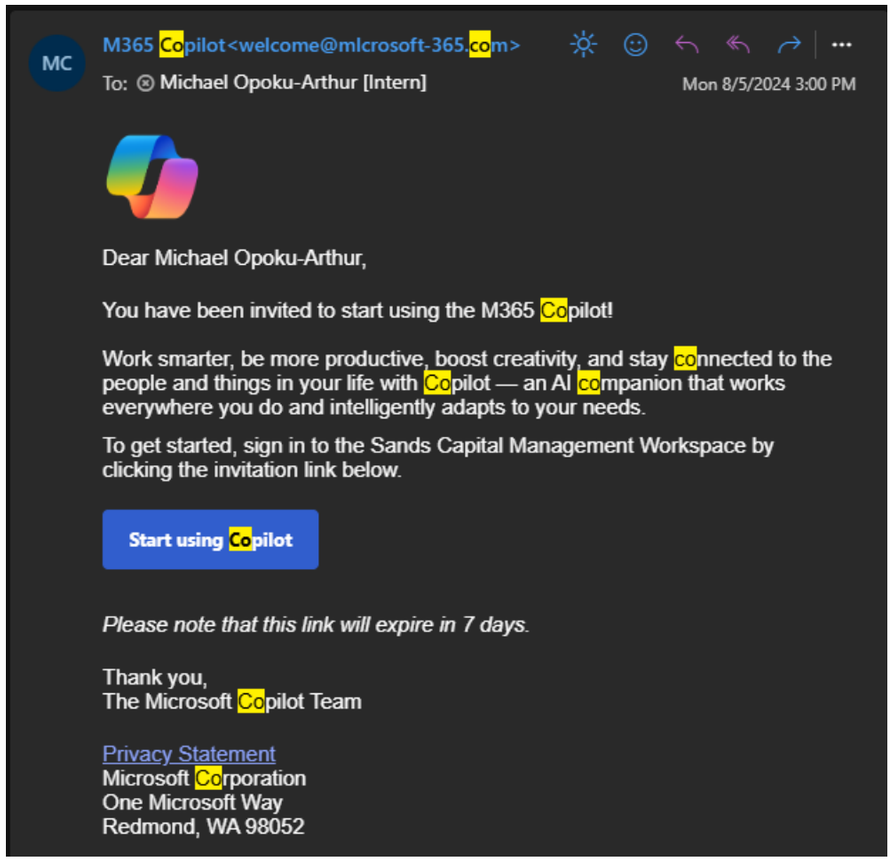
Overview of benchmarks sent to users each hour





HoxHunt


Benchmark overview
Created: 8/5/2024
Scheduled for: 15:00 8/5/2024
Target: 22 users
Simulation: service.microsoft.copilot.AD
Delivery
Performance
6/22
Succeeded
27% Succeeded
73% Pending
Scheduled sending times
Overview of benchmarks sent to users each hour
20
10
0
15:00 5 Aug
Sent successfully


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

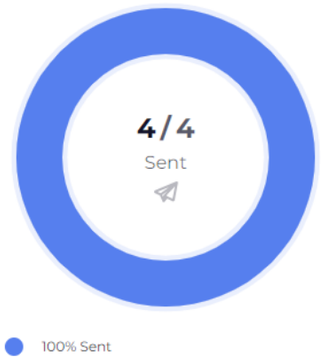
Created: 8/5/2024

Scheduled for: 15:03 8/5/2024

Target: 4 users

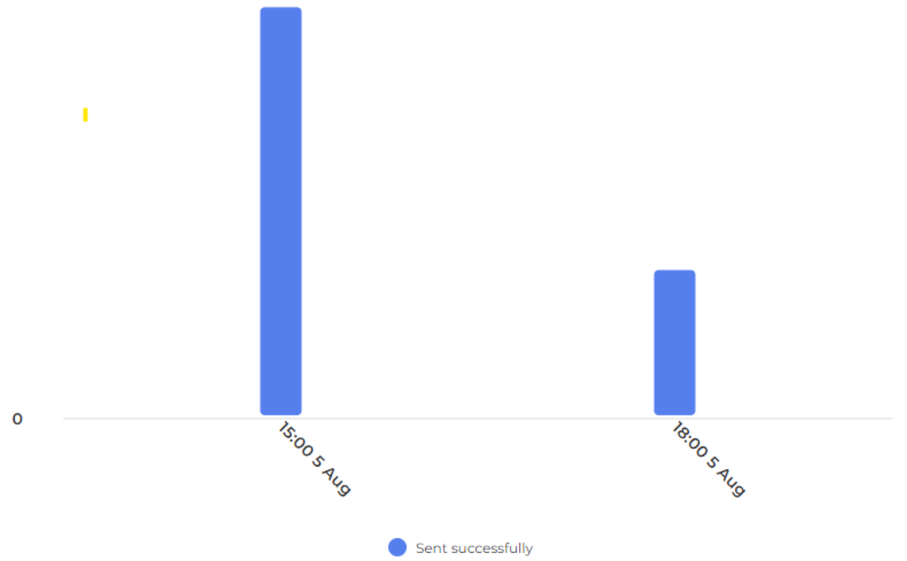
Simulation: service.github.vulnerabilityFound.lp

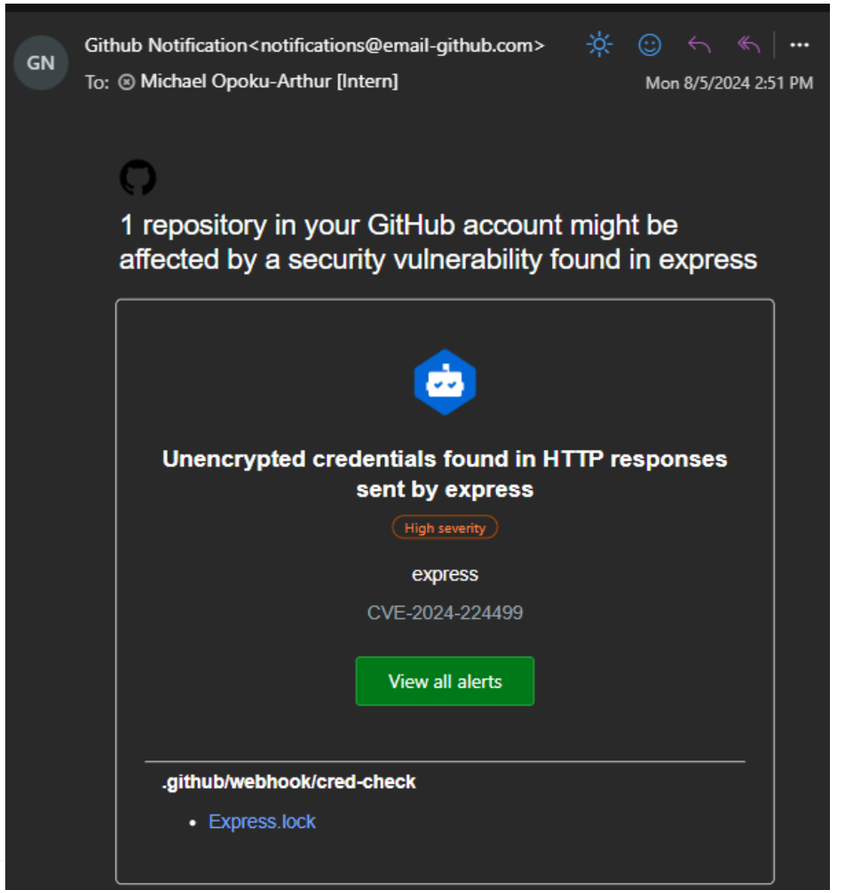
Delivery | Performance



Scheduled sending times

Overview of benchmarks sent to users each hour





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

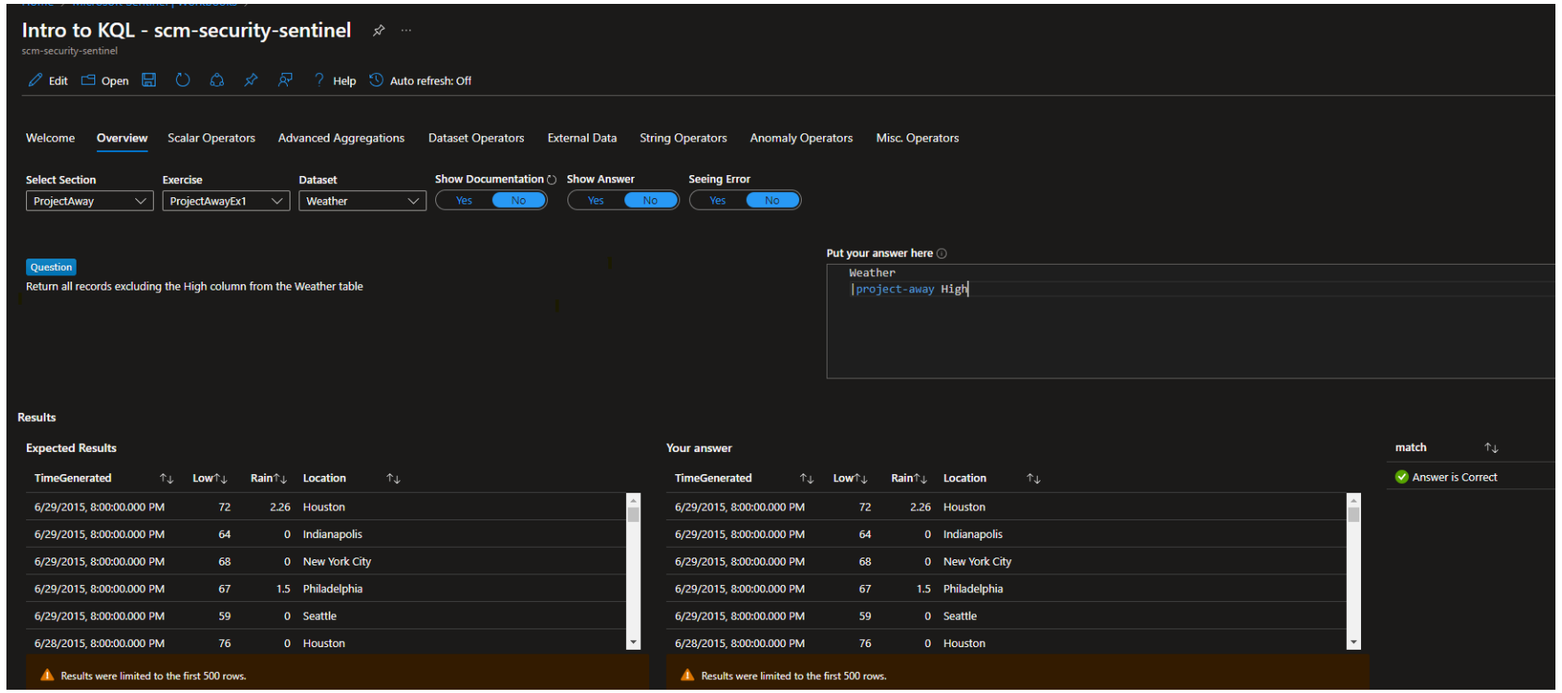
- Key Takeaways
  - Director of AI Solutions
  - Crash course of AI
  - Addressed common misconceptions
  - Discussed how he has implemented AI within the firm and how he plans to continue

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



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