RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **OST-T11**

Open Source Tooling for Threat Analysis and Attack Surface Management

Rey Bango & Gabe Stocco

Microsoft Corporation

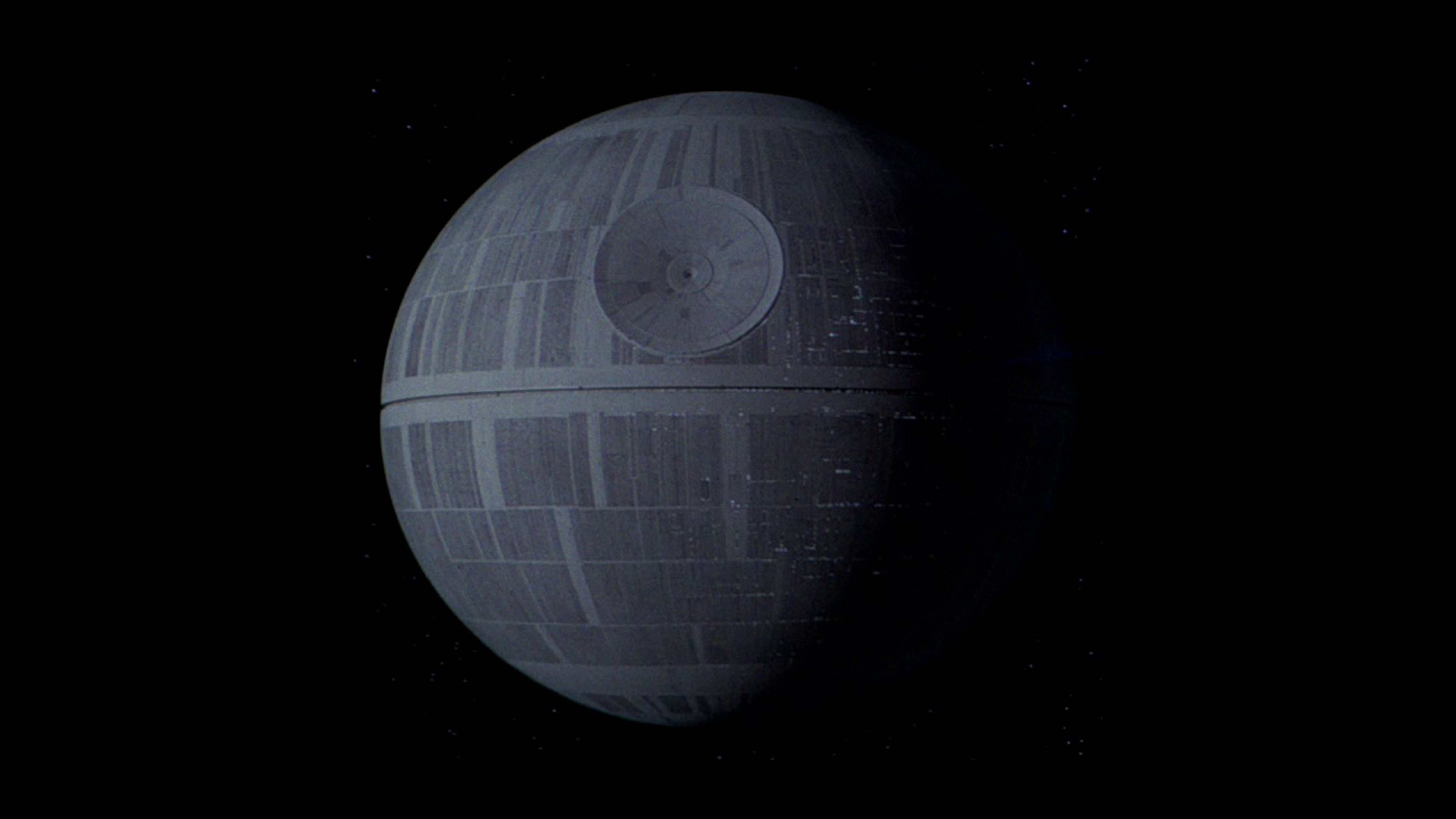
Keynote: Collaborating to Improve Open Source Security: How the Ecosystem Is Stepping Up

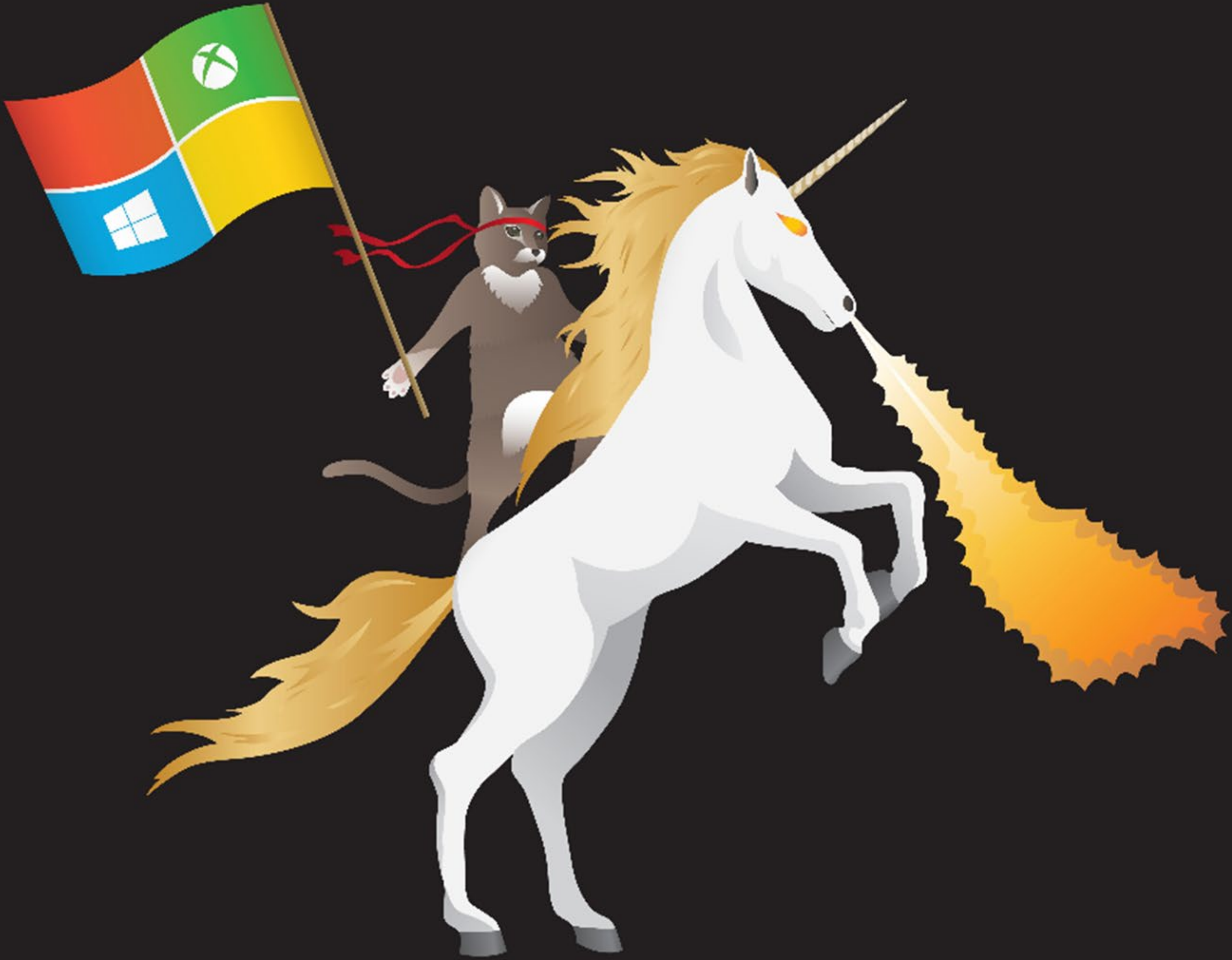
Session ID: KEY-F02S

Moscone South

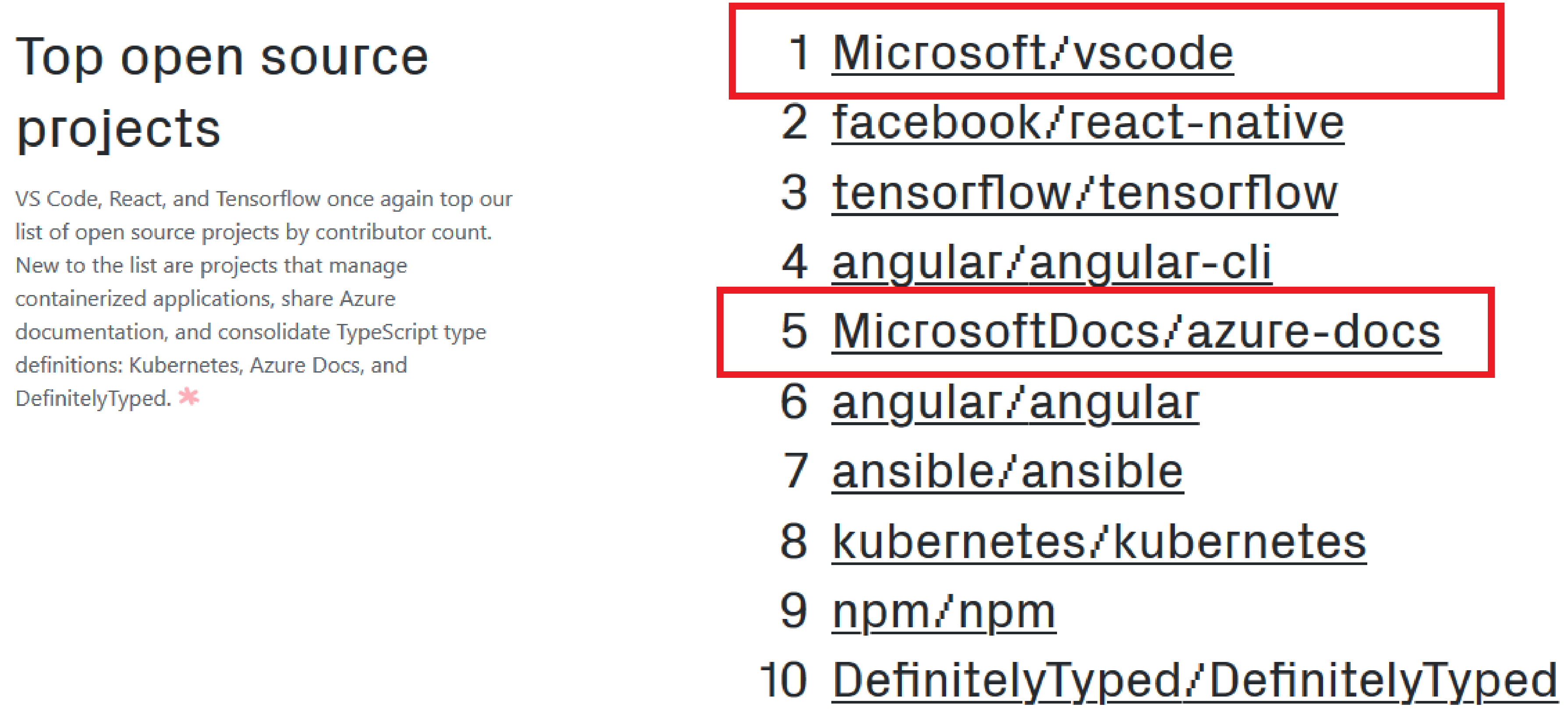
February 28, 2020 9:50am – 10:40am

Mark Russinovich
Chief Technology Officer
Microsoft Azure





State of the Octoverse Report 2018

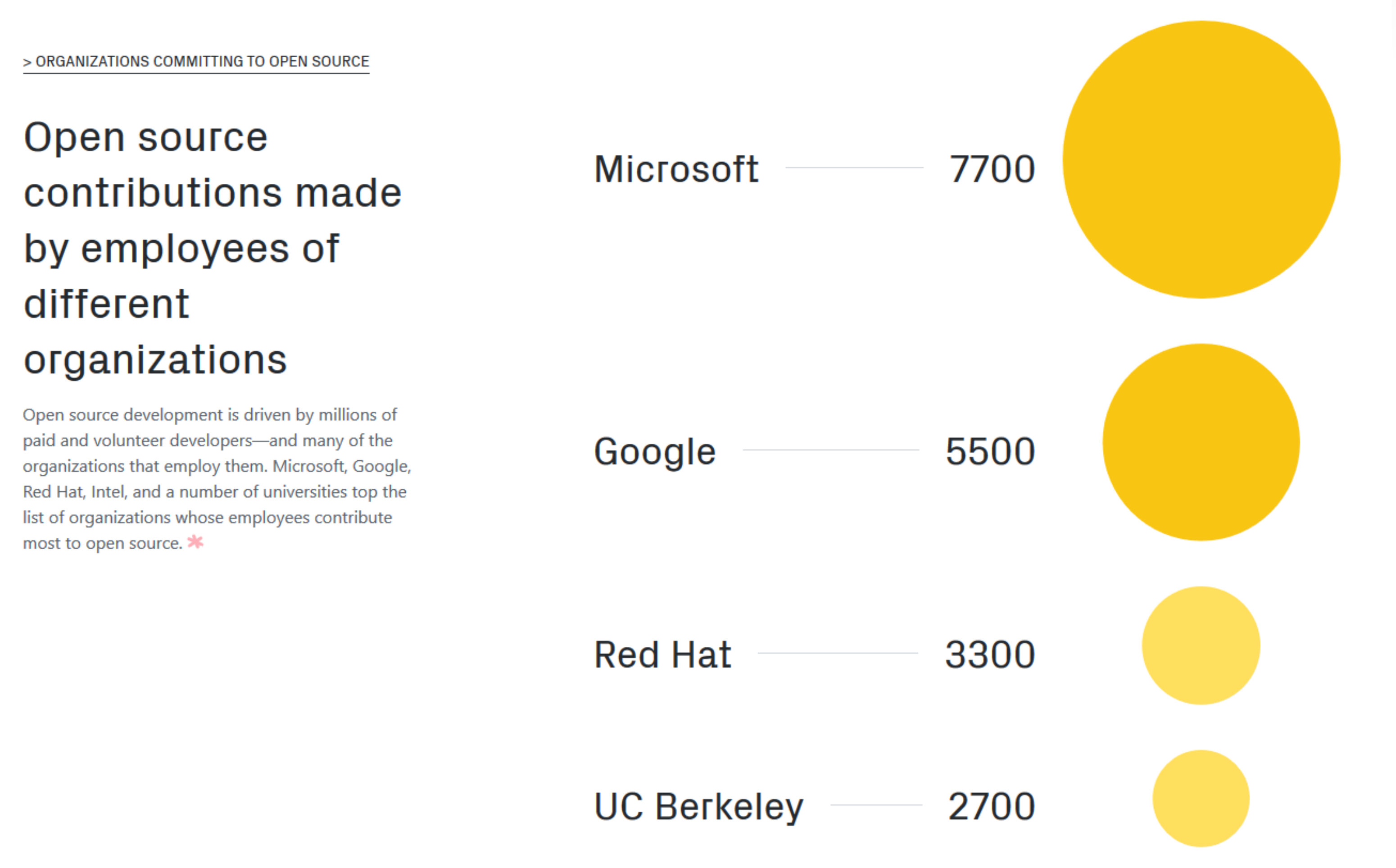


Top open source projects

VS Code, React, and Tensorflow once again top our list of open source projects by contributor count. New to the list are projects that manage containerized applications, share Azure documentation, and consolidate TypeScript type definitions: Kubernetes, Azure Docs, and DefinitelyTyped. *

1 Microsoft/vscode
2 facebook/react-native
3 tensorflow/tensorflow
4 angular/angular-cli
5 MicrosoftDocs/azure-docs
6 angular/angular
7 ansible/ansible
8 kubernetes/kubernetes
9 npm/npm
10 DefinitelyTyped/DefinitelyTyped

State of the Octoverse Report 2018



> ORGANIZATIONS COMMITTING TO OPEN SOURCE

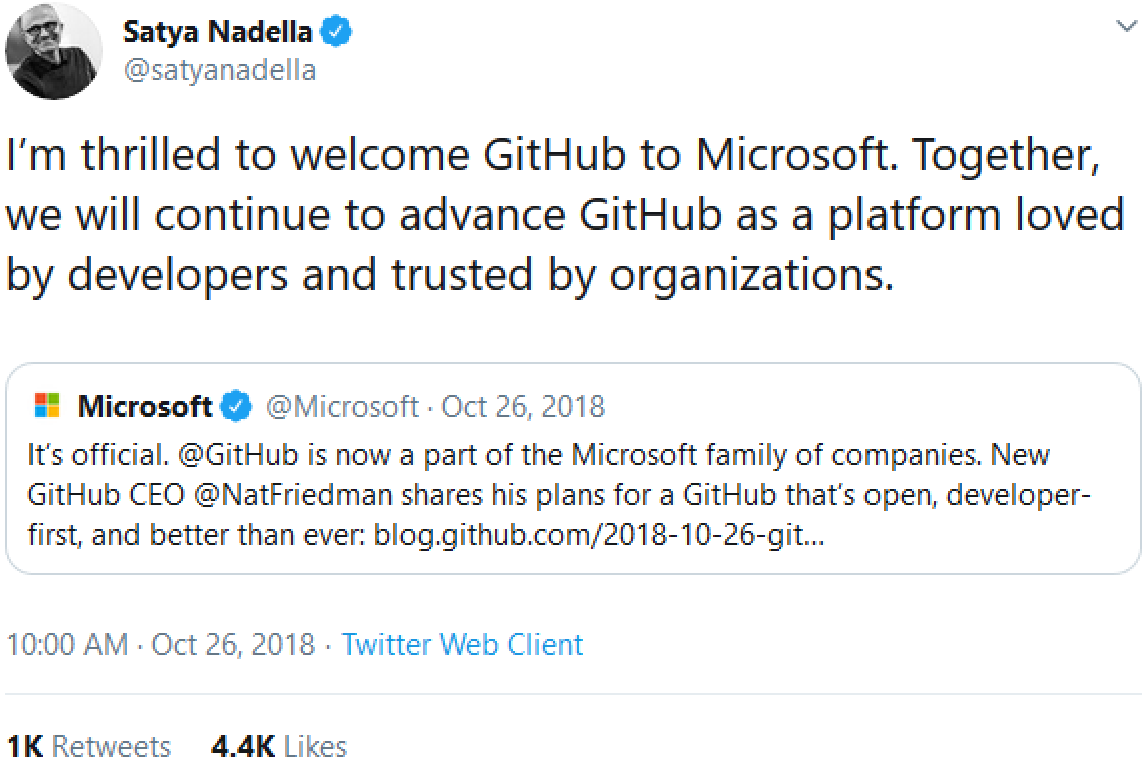
Open source contributions made by employees of different organizations

Open source development is driven by millions of paid and volunteer developers—and many of the organizations that employ them. Microsoft, Google, Red Hat, Intel, and a number of universities top the list of organizations whose employees contribute most to open source. *

Microsoft	7700
Google	5500
Red Hat	3300
UC Berkeley	2700

Microsoft

GitHub



Satya Nadella
@satyanadella

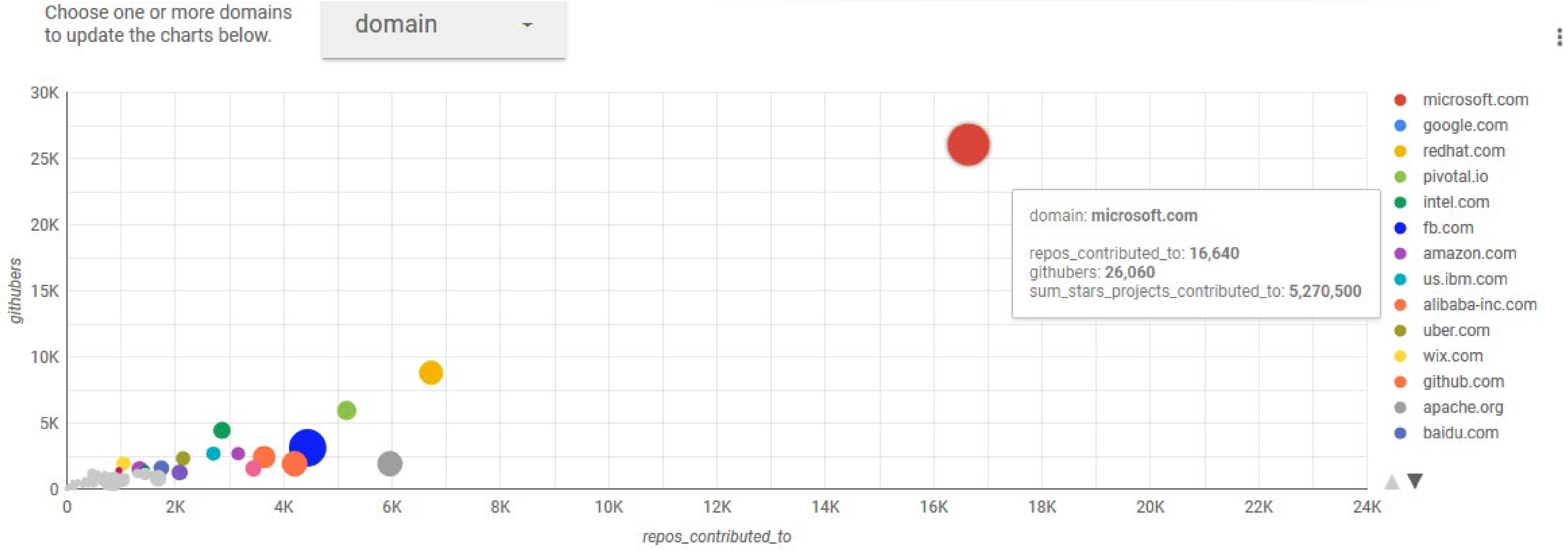
I'm thrilled to welcome GitHub to Microsoft. Together, we will continue to advance GitHub as a platform loved by developers and trusted by organizations.

> **Microsoft** @Microsoft · Oct 26, 2018
> It's official. @GitHub is now a part of the Microsoft family of companies. New GitHub CEO @NatFriedman shares his plans for a GitHub that's open, developer-first, and better than ever: blog.github.com/2018-10-26-git...

10:00 AM · Oct 26, 2018 · Twitter Web Client

1K Retweets **4.4K** Likes

GitHub Data To-Date



Choose one or more domains to update the charts below.

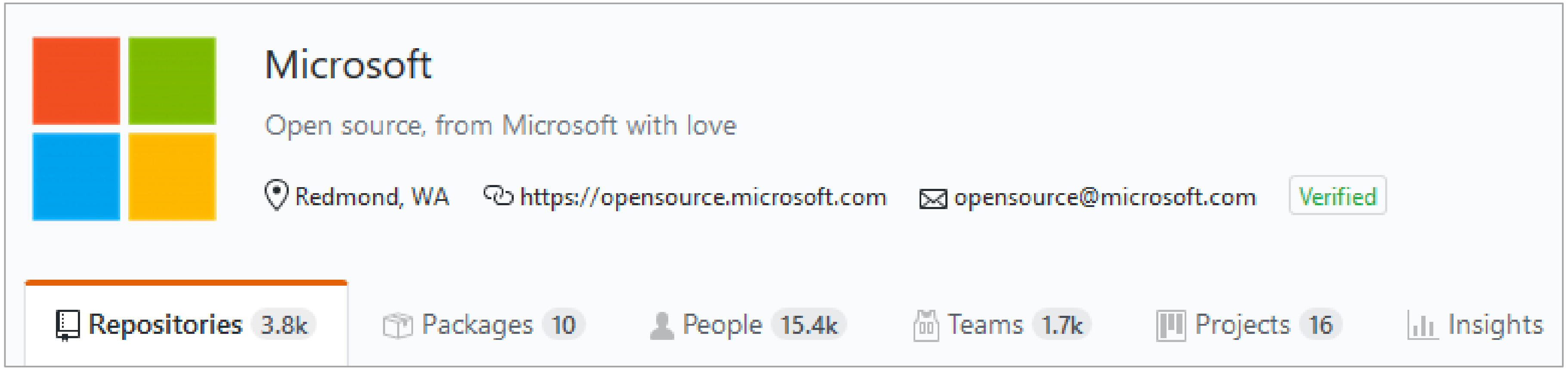
domain: **microsoft.com**

repos_contributed_to: **16,640**
githubers: **26,060**
sum_stars_projects_contributed_to: **5,270,500**

Source: https://datastudio.google.com/u/0/reporting/0ByGAKP3QmCjLU1JzUGtJdTlNOG8/page/Q3DM

OSS Projects @ Microsoft

- Visual Studio Code
- TypeScript
- Microsoft Edge
- PowerShell
- The Windows Terminal
- Webhint



Microsoft

Open source, from Microsoft with love

Redmond, WA https://opensource.microsoft.com opensource@microsoft.com Verified

Attack Surface Analyzer

msticpy - Jupyter and Python Security Tools

Attack Surface Analyzer

Attack Surface Analyzer 2

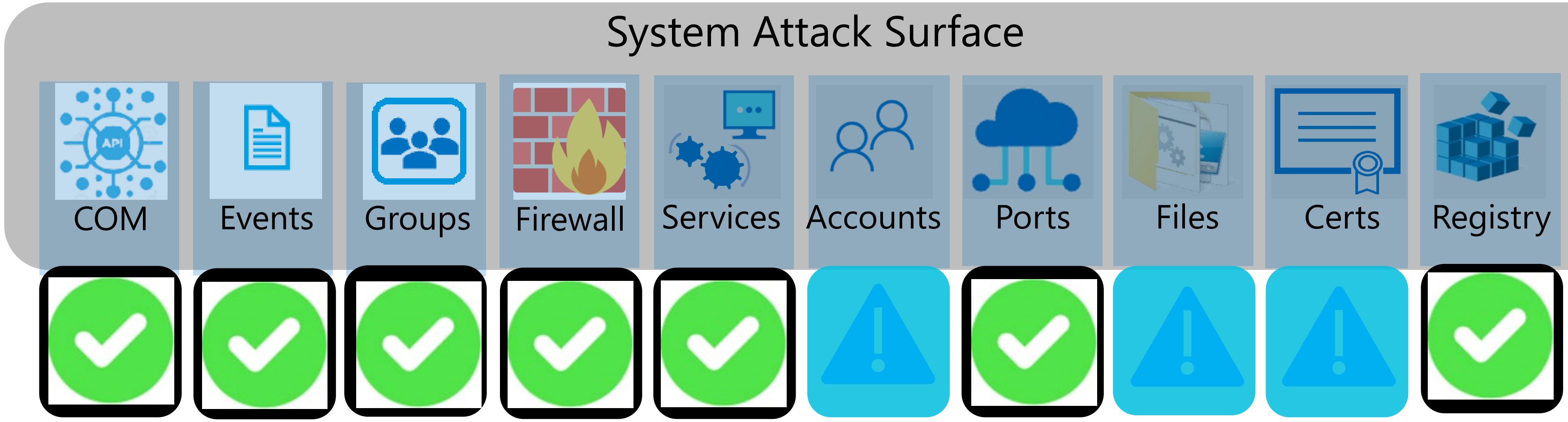
- Microsoft Attack Surface Analyzer (ASA) detects system configuration changes resulting from software installations*
- ASA 2 is a rewrite of the original tool available since 2012 that has helped IT professionals secure their systems for years
- Now includes support for Windows 10, Linux and macOS
- Released in April 2019 as Open Source on GitHub

System Attack Surface Risks

- **File System** – malicious or inadvertent changes can corrupt system files that make up key functions of your system or grant access to private data
- **User Accounts** – persistent rogue elevated accounts can grant access to hijack your system
- **System Services** – background processes may be introduced that perform rogue operations like capturing sensitive data and even shut down existing key security modules
- **Network Ports** – can expose your system to unknown remote entities
- **Digital Certificates** – determine what remote domains and package signatures are trusted
- **Registry** –controls system startup actions, device drivers, services, and more

Attack Surface Analyzer Coverage

Each one requires special tools and knowledge to identify changes made



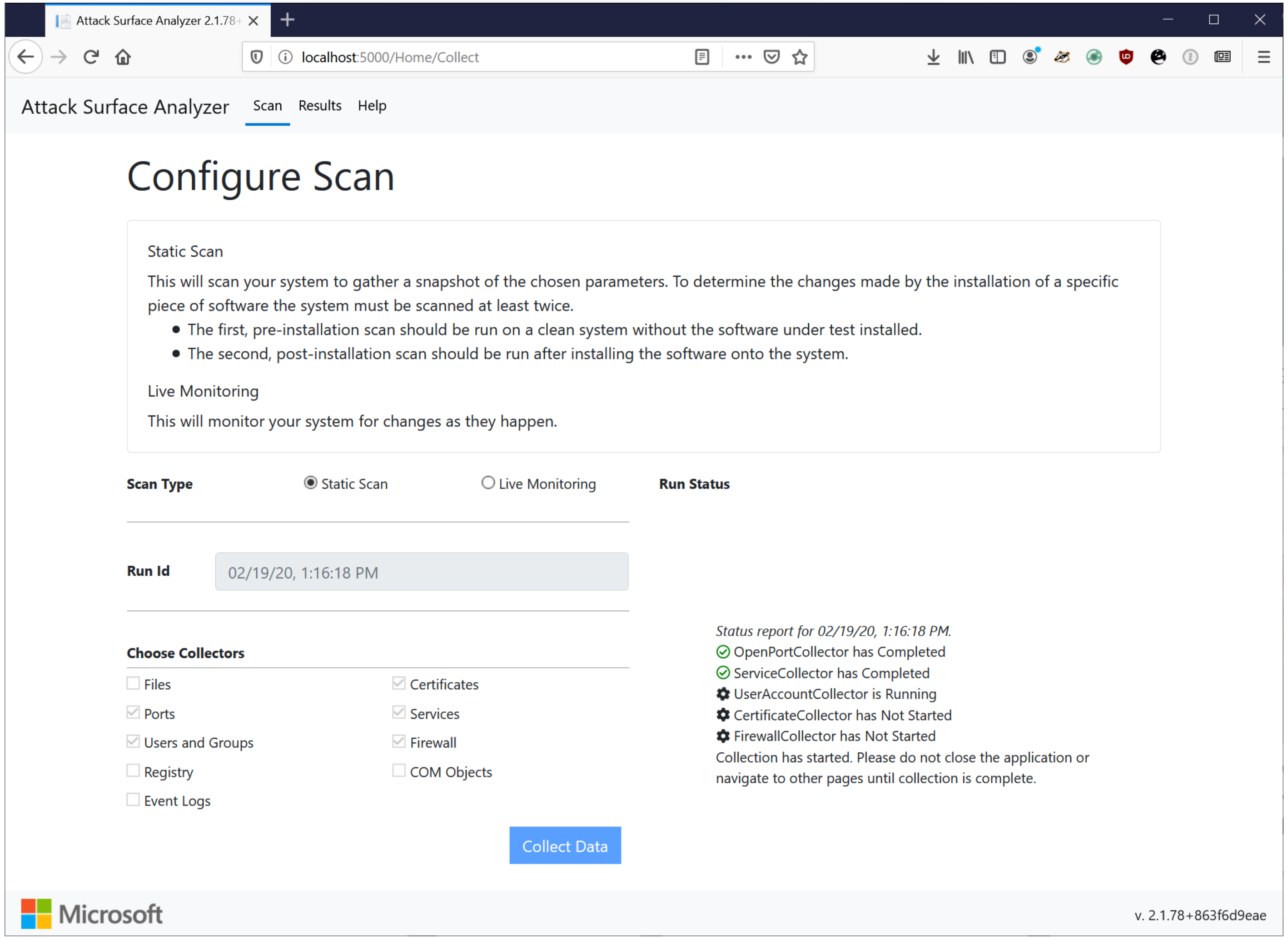
System Attack Surface

COM	Events	Groups	Firewall	Services	Accounts	Ports	Files	Certs	Registry
✓	✓	✓	✓	✓	⚠	✓	⚠	⚠	✓

Microsoft Attack Surface Analyzer Reports Help

Using Attack Surface Analyzer

1. Create a base or initial scan on a clean system.
2. Install and run your product or application.
3. Take another scan.
4. Use the results analysis to identify system changes



Configure Scan

Static Scan

This will scan your system to gather a snapshot of the chosen parameters. To determine the changes made by the installation of a specific piece of software the system must be scanned at least twice.

- The first, pre-installation scan should be run on a clean system without the software under test installed.
- The second, post-installation scan should be run after installing the software onto the system.

Live Monitoring

This will monitor your system for changes as they happen.

Scan Type ● Static Scan ○ Live Monitoring

Run Status

Run Id 02/19/20, 1:16:18 PM

Choose Collectors

☐ Files
☑ Ports
☑ Users and Groups
☐ Registry
☐ Event Logs
☑ Certificates
☑ Services
☑ Firewall
☐ COM Objects

Status report for 02/19/20, 1:16:18 PM.
✓ OpenPortCollector has Completed
✓ ServiceCollector has Completed
⚙ UserAccountCollector is Running
⚙ CertificateCollector has Not Started
⚙ FirewallCollector has Not Started
Collection has started. Please do not close the application or navigate to other pages until collection is complete.

RSAConference2020

ASA Demo

Built for Everyone

- Microsoft uses the Attack Surface Analyzer as part of our security development lifecycle practices (SDL)
- The *classic* version of the tool is still available with limited Windows support
- Attack Surface Analyzer 2.1 runs on Windows 10, Linux, and macOS
- Command line and browser based GUI interfaces.

Typical Users

DevOps Engineers that want to reduce the system attack surface introduced by their own software

IT Security Auditors that want to evaluate risks from third-party software

Attack Surface Analyzer 2.1

- Collects Many Different Verticals
  - ✓ Firewall settings
  - ✓ System Services
  - ✓ System Logs
  - ✓ COM Objects (Windows)
  - ✓ Files
  - ✓ Registry
  - ✓ Network Ports
  - ✓ Users and Groups
- New user defined analysis rules system
  - ✓ Define analysis rules on any collected field using choice of operator
- Default ruleset
  - ✓ e.g. flags executables without ASLR enabled
  - ✓ Community contributions for default rules are encouraged.
- Docker-based detonation chamber available

Other tools from Microsoft Security

- Application Inspector reports on what types of functionality source code implements allowing you to identify any unexpected functionality.
  - Github.com/Microsoft/ApplicationInspector
- DevSkim is a security linter available as an extension for both Visual Studio and Visual Studio Code.
  - Github.com/Microsoft/DevSkim

RSAConference2020

msticpy

AKA MSTIC Jupyter and Python Security Tools

What is msticpy?

- Python tools for security investigations and hunting
- Built for interactive Jupyter notebook environment
- Addresses the following needs:
  - Data Acquisition
  - Data Enrichment
  - Data Analysis
  - Visualization
- Open source and agnostic to the data source

Why use Jupyter for Security Investigations?

- Access to sophisticated data processing, machine learning and visualization
- Extends & complements SIEM dashboards and data
- Pull external data into your investigation
- Offers fine-grain capabilities
- Scripting and programming environment for repeatability
- Auto-saves your investigation into shareable HTML document

4 Core Aspects of msticpy

- Data Acquisition
  - Single-line parameterized functions vs. complex queries
  - Results are returned as *pandas* DataFrames
- Data Enrichment
  - Dig granularly into data (e.g.: IP geolocation)
  - Connect to threat intel providers like VirusTotal, OTX, X-Force
- Visualization
  - Methods for plotting, building timelines, GeoIP mapping & more

4 Core Aspects of msticpy

- Data Analysis
  - Reshape data to gain new insights
    - IOC extractor – extract IP addresses, URLs, hashes, etc. from data
    - Decode/unpack obfuscated data from base64, zip, tar, etc.
  - Search for specific patterns
  - Cluster events to find unusual activity
  - Automate these to streamline workflow – pandas DataFrames make it easy to chain acquisition->enrichment->analysis->visualization components

RSA®Conference2020

msticpy Demo

Call to Action

- Use Microsoft Attack Surface Analyzer 2.0 as part of your secure development lifecycle
  - Get it at: https://github.com/Microsoft/AttackSurfaceAnalyzer
- Start analyzing your threat data with msticpy & Jupyter Notebooks
  - msticpy Project: https://github.com/Microsoft/msticpy
- Contribute back:
  - Help shape the projects by giving back fixes and cool new features