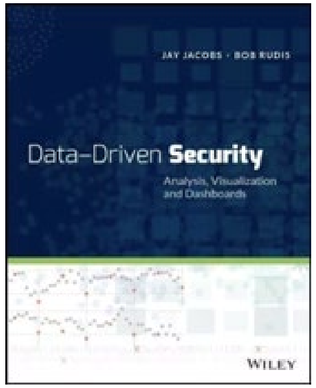
{attckr} A Toolkit for Analysis & Visualization of ATT&CK Incident Data for Service Providers & Organizations

Bob Rudis • Chief Data Scientist • Rapid7

ATT&CKcon 2019

hrbrmstr://about

30+ Years in Cybersecurity
(20+ in Fortune 50 global organizations)



Former team lead for the
Verizon Data Breach Investigations Report

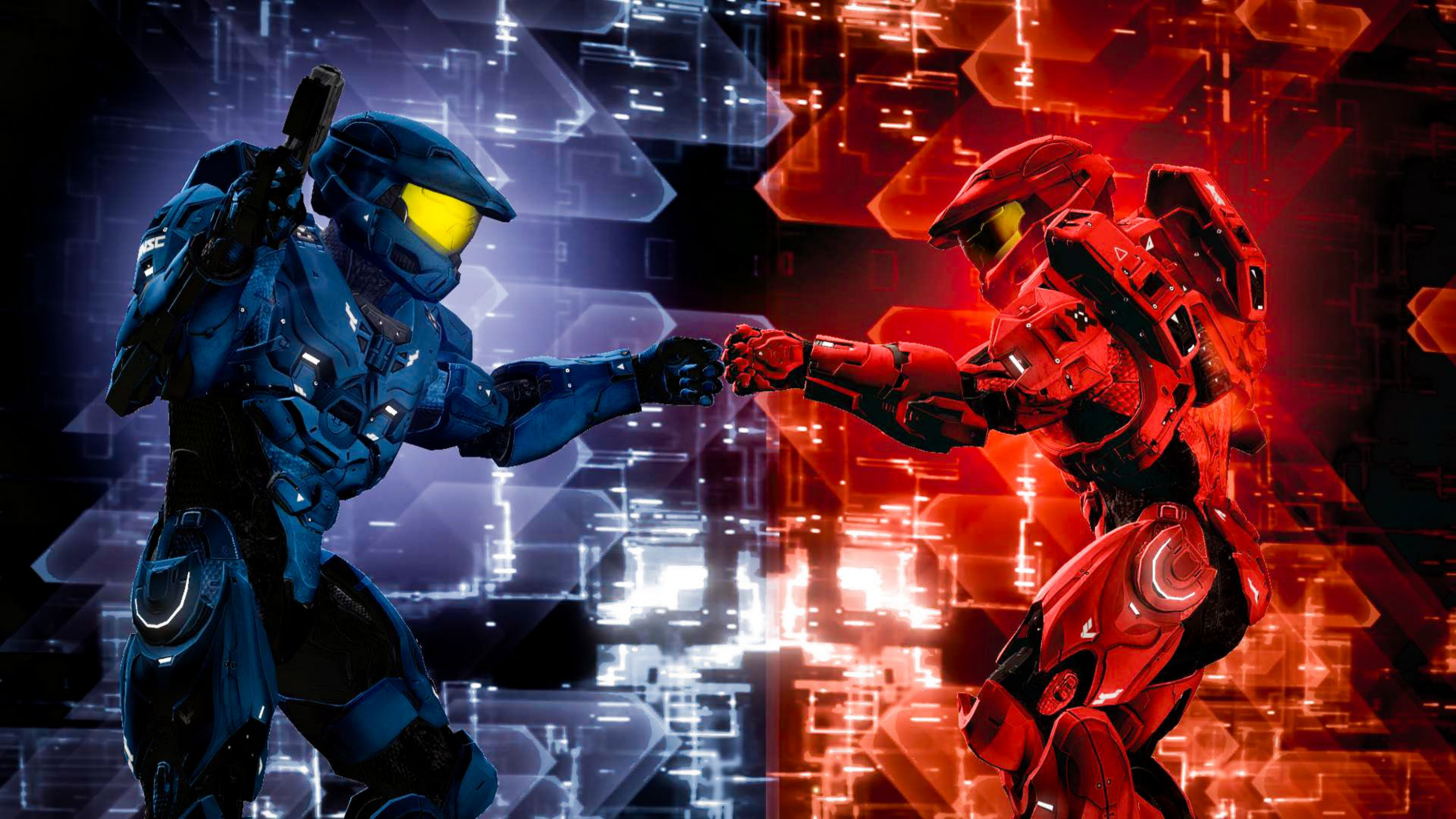
Co-author of one of the 1st books
on“doing data science” in Cybersecurity

Over a petabyte of planetary-scale
internet telemetry data analyzed daily

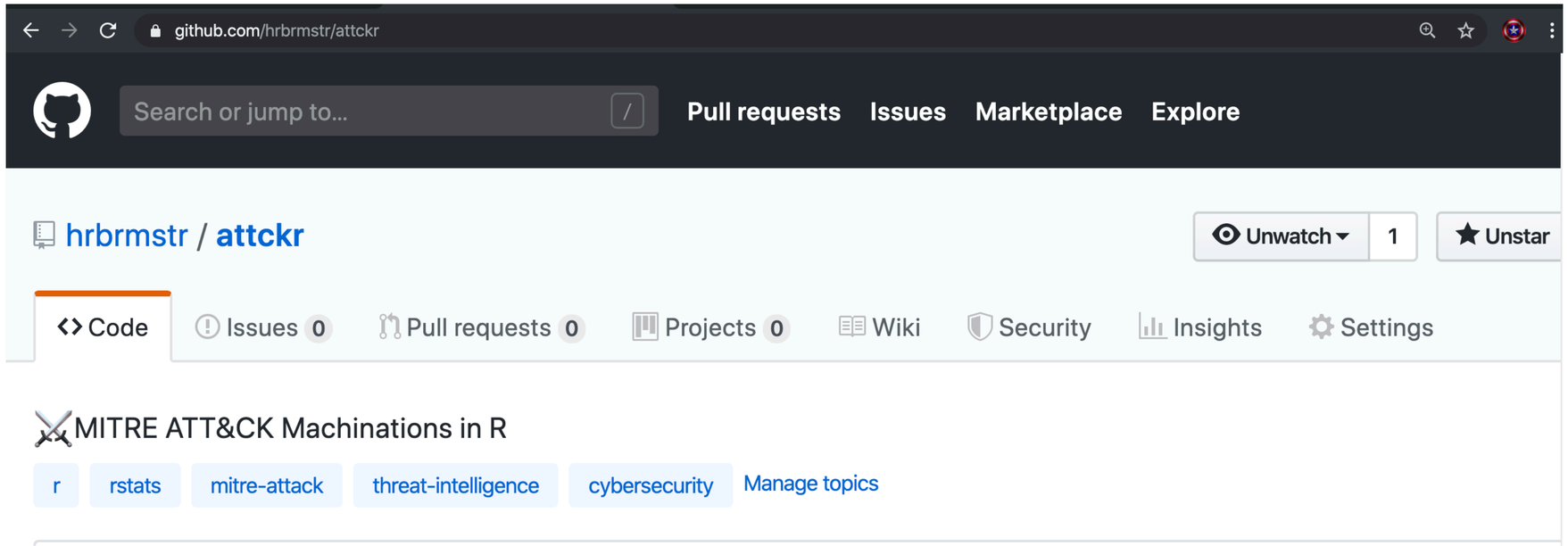
90+ packages with a focus on cybersecurity &
internet telemetry

@hrbrmstr
research@rapid7.com
bob@rud.is
https://rud.is/
https://github.com/hrbrmstr
https://blog.rapid7.com/


MITRE
ATT&CK™



github.com/hrbrmstr/attckr
gitlab.com/attckr
bitbucket.com/attckr
git.src.ht/~hrbrmstr/attckr
git.rud.is/hrbrmstr/attckr



Why  ?

r-project.org

[Home]

Download

CRAN

R Project

About R
Logo
Contributors
What's New?
Reporting Bugs
Conferences
Search
Get Involved: Mailing Lists
Developer Pages
R Blog

R Foundation

Foundation
Board
Members
Donors
Donate

Help With R

Getting Help

The R Project for Statistical Computing

Getting Started

R is a free software environment for statistical computing and graphics. It compiles and runs on a wide variety of UNIX platforms, Windows and MacOS. To **download R**, please choose your preferred CRAN mirror.

If you have questions about R like how to download and install the software, or what the license terms are, please read our answers to frequently asked questions before you send an email.

News

- **R version 3.6.1 (Action of the Toes)** has been released on 2019-07-05.
- useR! 2020 will take place in St. Louis, Missouri, USA.
- **R version 3.5.3 (Great Truth)** has been released on 2019-03-11.
- The R Foundation Conference Committee has released a call for proposals to host useR! 2020 in North America.
- You can now support the R Foundation with a renewable subscription as a supporting member
- The R Foundation has been awarded the Personality/Organization of the year 2018 award by the professional association of German market and social researchers.

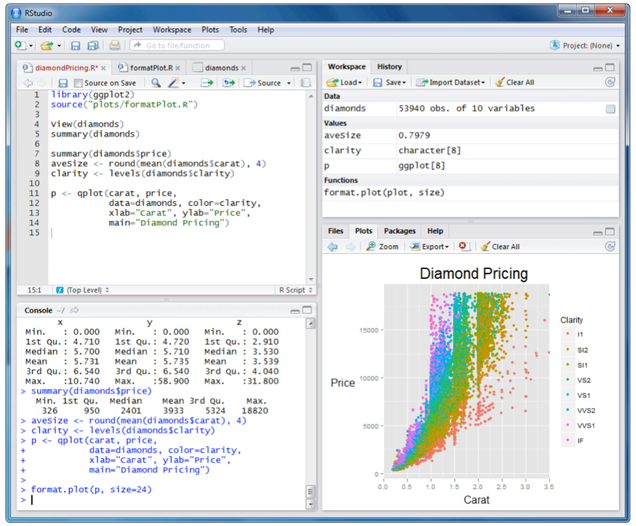
News via Twitter

News from the R Foundation

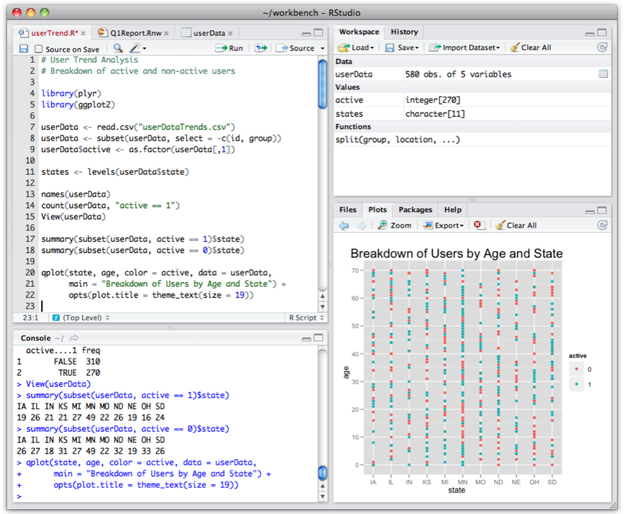
- FOSS
- Mission-built for Data Science
- Rich ecosystem for data analysis and visualization
- "Not Just R"
  - C/C++
  - Python
  - Rust
  - Go
  - Java
  - Scala
  - Wasm
  - …

RStudio®

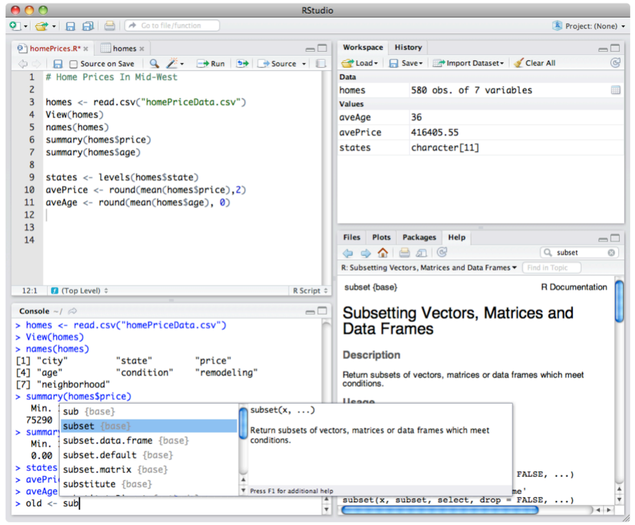
RStudio runs on most desktops or on a server and accessed over the web:



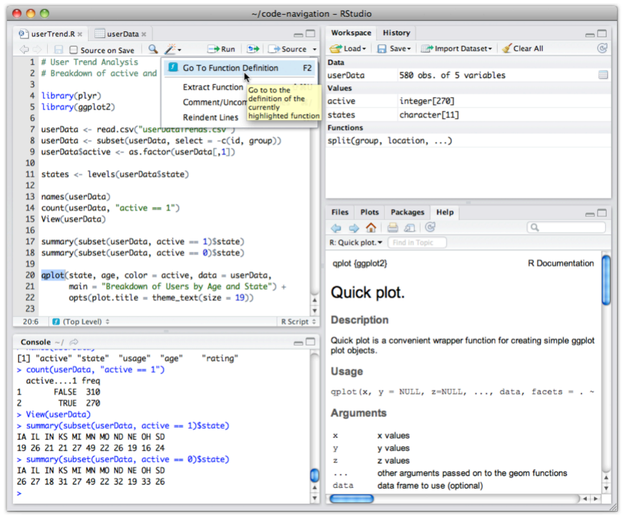
RStudio integrates the tools you use with R into a single environment:

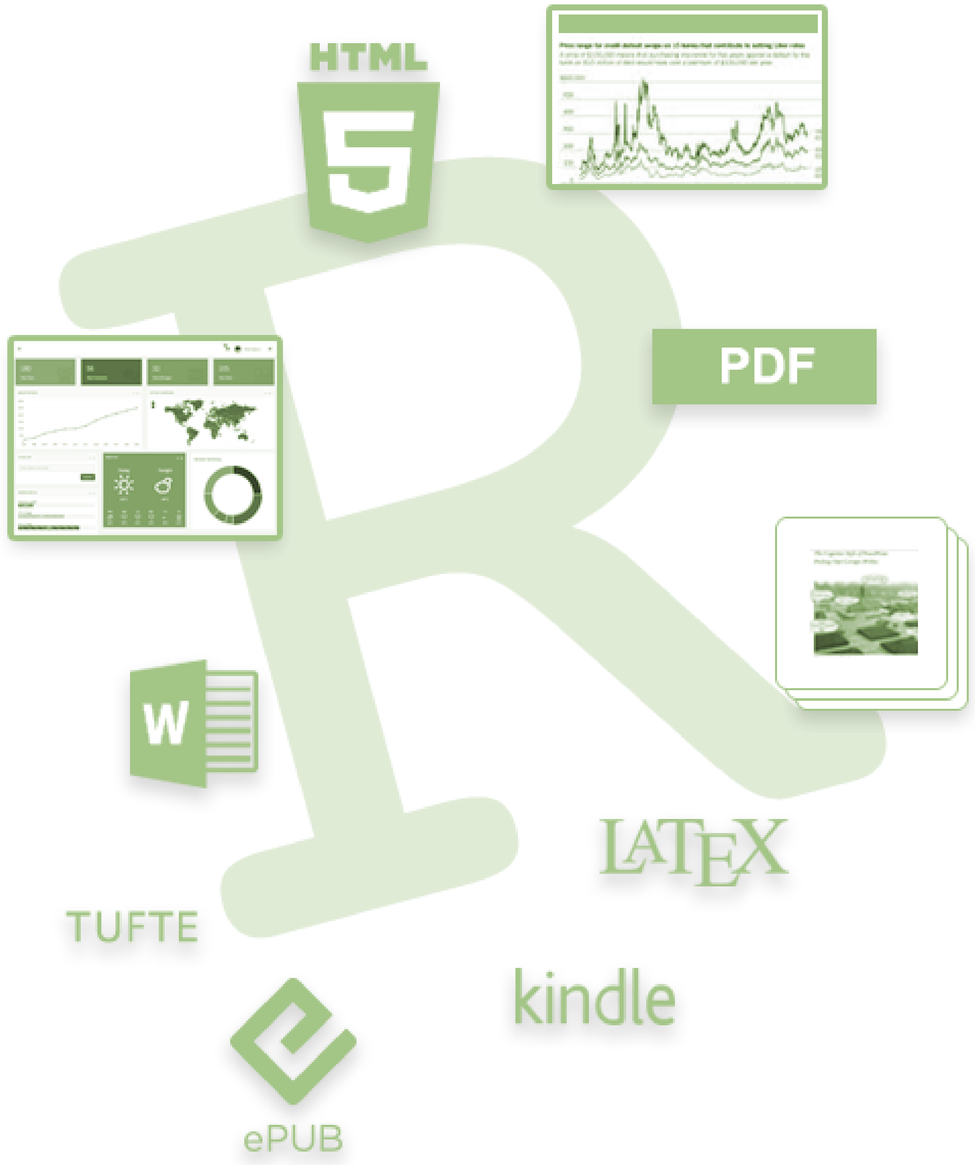


RStudio includes powerful coding tools designed to enhance your productivity:



RStudio enables rapid navigation to files and functions:

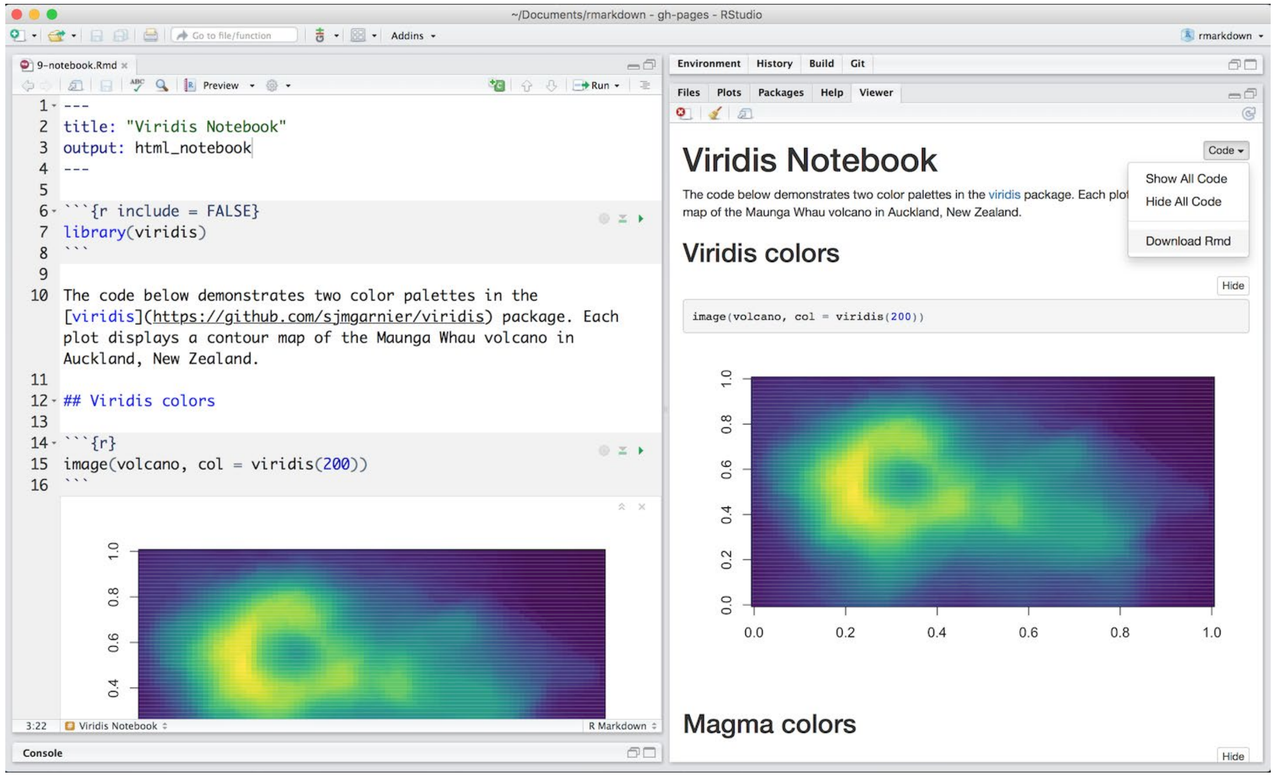




{rmarkdown}

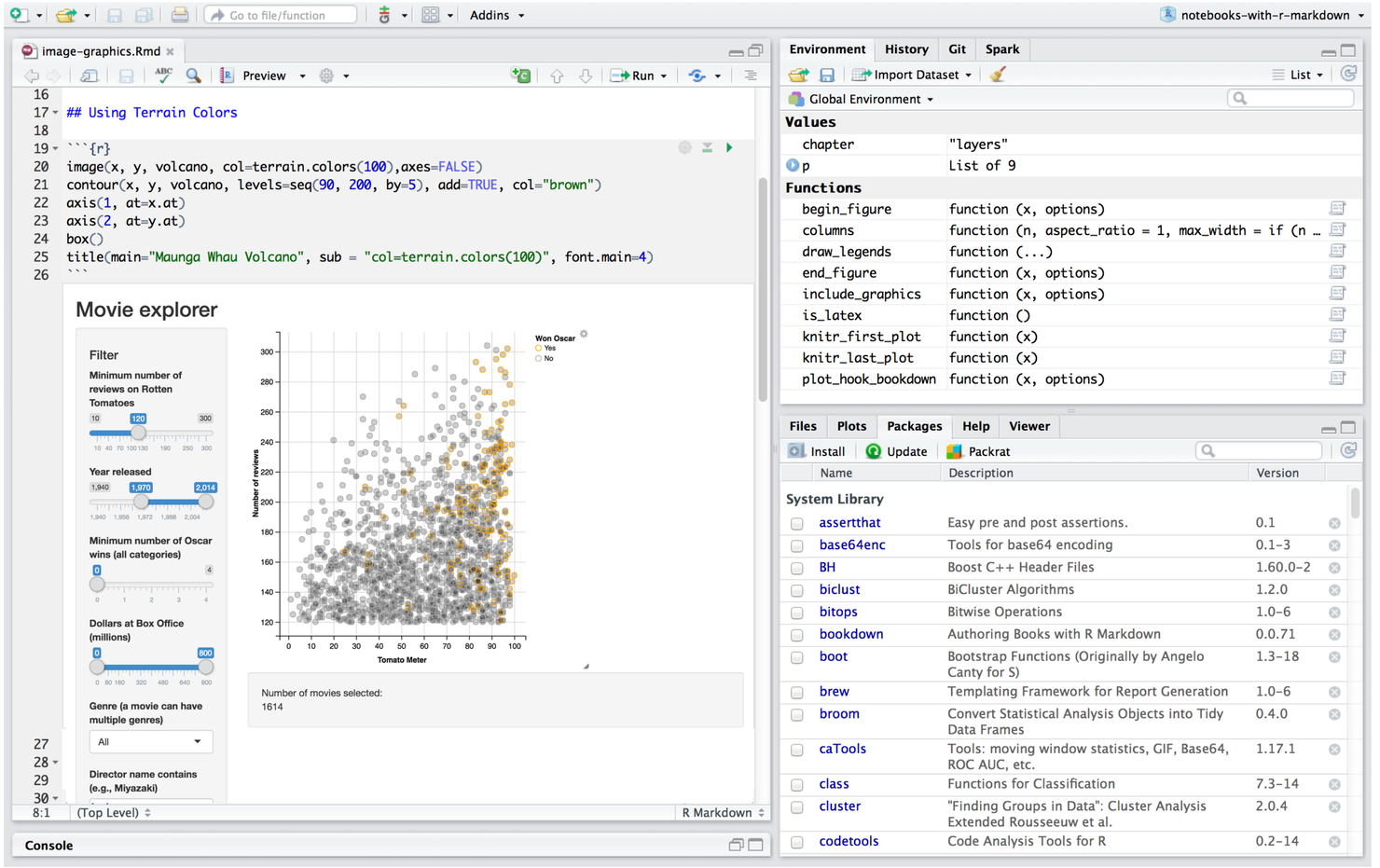
- Combine HTML, markdown, LaTeX and code (not just R code!) to create static or interactive reports.

- Can also work just like Jupyter Notebooks



R {shiny}

Create server-backed, highly dynamic reporting and data exploration applications that can be turned into standalone apps locally or served at scale on the internet.



What does the distribution of Tactics & Techniques look like?

Where do we have technology gaps?

Where do we have workforce gaps?

Where should we invest our limited defense budget?

How does X compare with Y?

How does X compare with Y over time?

What’s the Dwell Time trend?

What's Inside The Tin?

- `fct_tactic`: Make an ordered Tactics factor with optional better labelling
- `tactics_f`: Tactics factors (generally for sorting & pretty-printing)

- `validate_tactics`: Validate Tactics strings against MITRE authoritative source
- `validate_technique_ids`: Validate Technique IDs
- `validate_techniques`: Validate Techniques strings against MITRE authoritative source

Validation

- `attck_cdf_tactic`: Product an ATT&CK Cumulative Distribution Function by Tactic
- `attck_map`: Generate an ATT&CK heatmap
- `theme_enhance_atkmap`: Remove cruft from ATT&CK heatmaps

Visualization

The following datasets are included:

- `enterprise_attack`: Enterprise Attack Taxonomy v2.0
- `mobile_attack`: Mobile Attack Taxonomy v2.0
- `pre_attack`: Pre-Attack Taxonomy v2.0
- `tactics_f`: Tactics factors (generally for sorting & pretty-printing)
- `tidy_attack`: Combined ATT&CK Matrices Tactics, Techniques and Technique detail

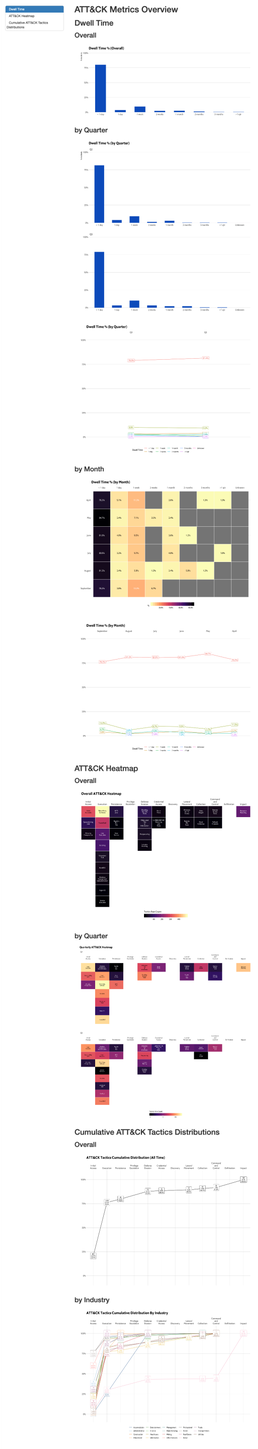
Data Source/Normalization
`https://github.com/mitre/cti/`

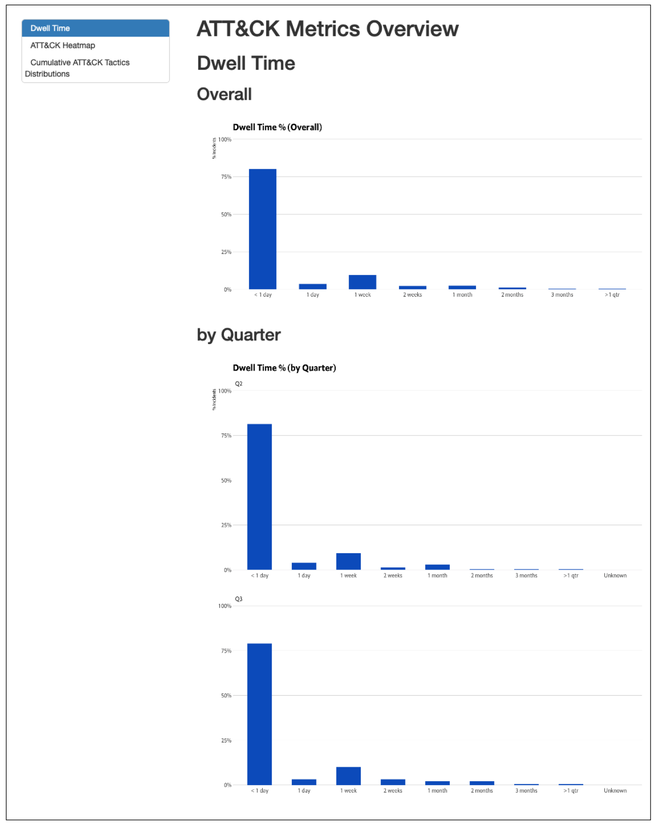
+ ATT&CK Summary Reporting R Markdown Base Template &
Real-world Data Sampled From Real Incident Distributions

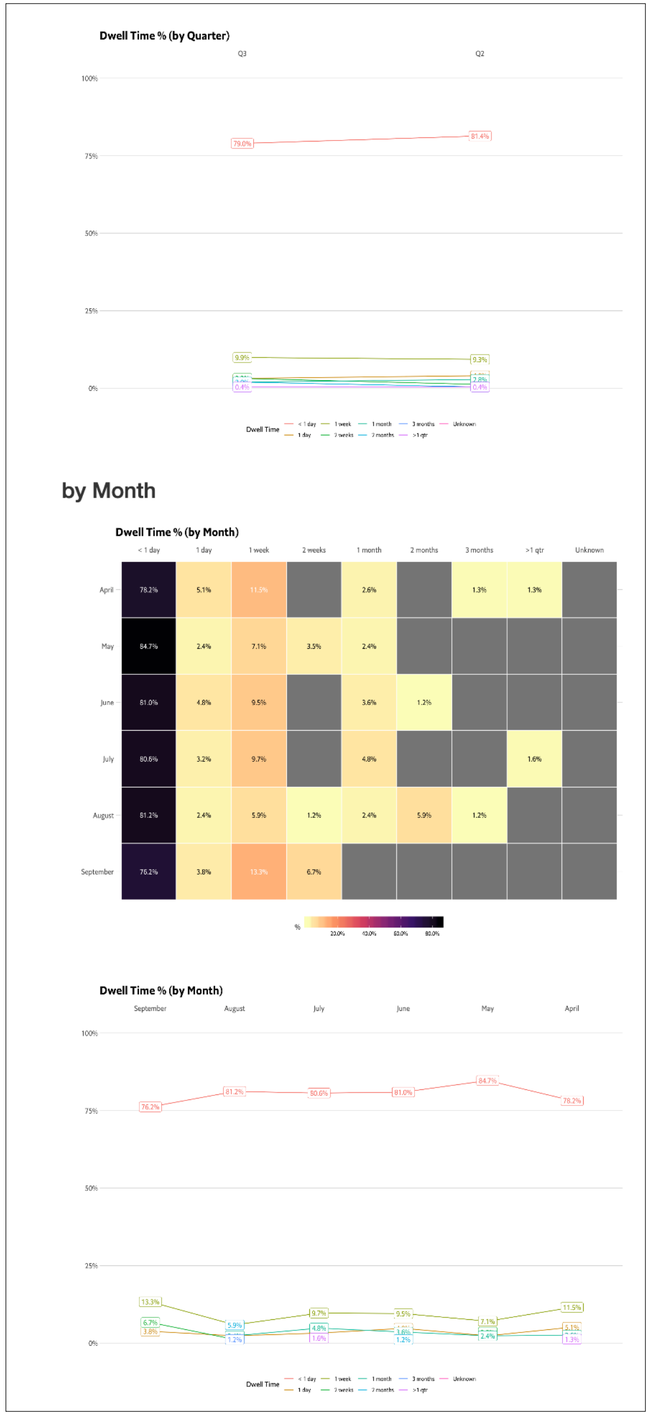
```
[
  {
    "first_event_ts": "2019-05-21 13:54:03",
    "first_alert_ts": "2019-05-21 13:54:03",
    "containment_ts": "2019-05-21 14:02:38",
    "org": "ac33b693",
    "mitre_attack": [
      {
        "tactic": "Execution",
        "technique": "Third-Party Software",
        "id": "T1072"
      },
      {
        "tactic": "Execution",
        "technique": "Third-Party Software",
        "id": "T1072"
      },
      {
        "tactic": "Persistence",
        "technique": "BITS Jobs",
        "id": "T1197"
      },
      {
        "tactic": "Execution",
        "technique": "Third-Party Software",
        "id": "T1072"
      },
      {
        "tactic": "Persistence",
        "technique": "BITS Jobs",
        "id": "T1197"
      },
      {
        "tactic": "Execution",
        "technique": "Third-Party Software",
        "id": "T1072"
      }
    ],
    "industry": "Manufacturing"
  }
]
```

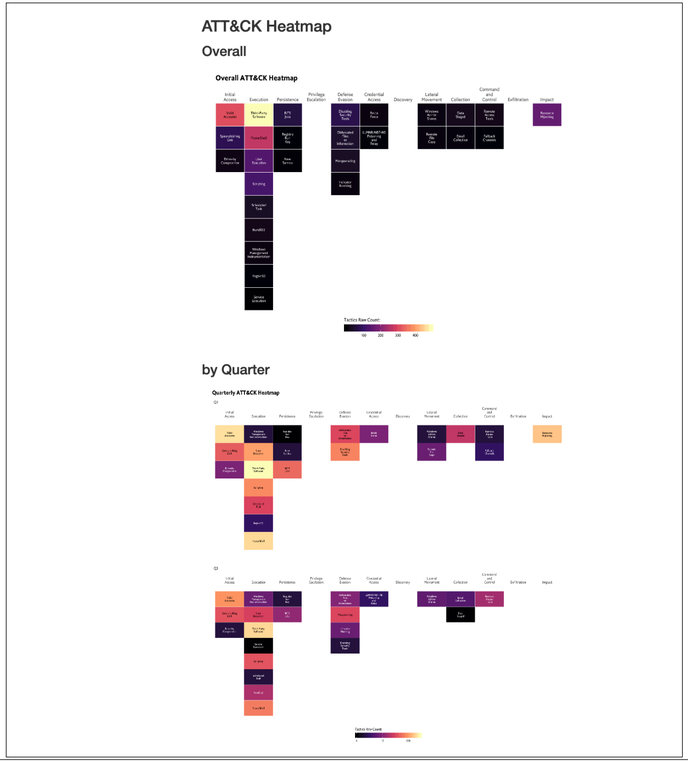
{attckr} v0.2.0

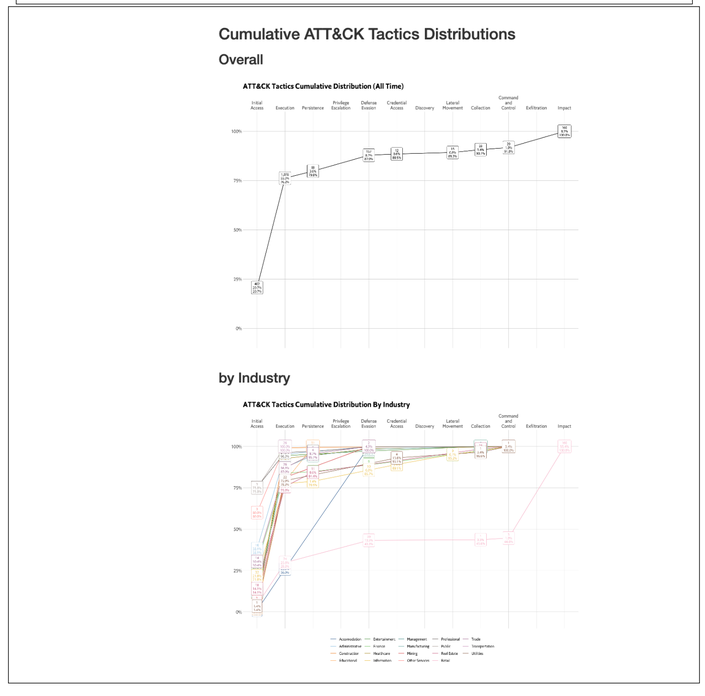
- Dwell time Metrics
- ATT&CK Heatmaps
- Cumulative ATT&CK Tactics Distributions


Dwell Time
ATT&CK Heatmap
Cumulative ATT&CK Tactics Distributions
ATT&CK Metrics Overview
Dwell Time
Overall
Dwell Time % (Overall)
by Quarter
by Month
ATT&CK Heatmap
Overall
by Quarter
Cumulative ATT&CK Tactics Distributions
Overall
by Industry

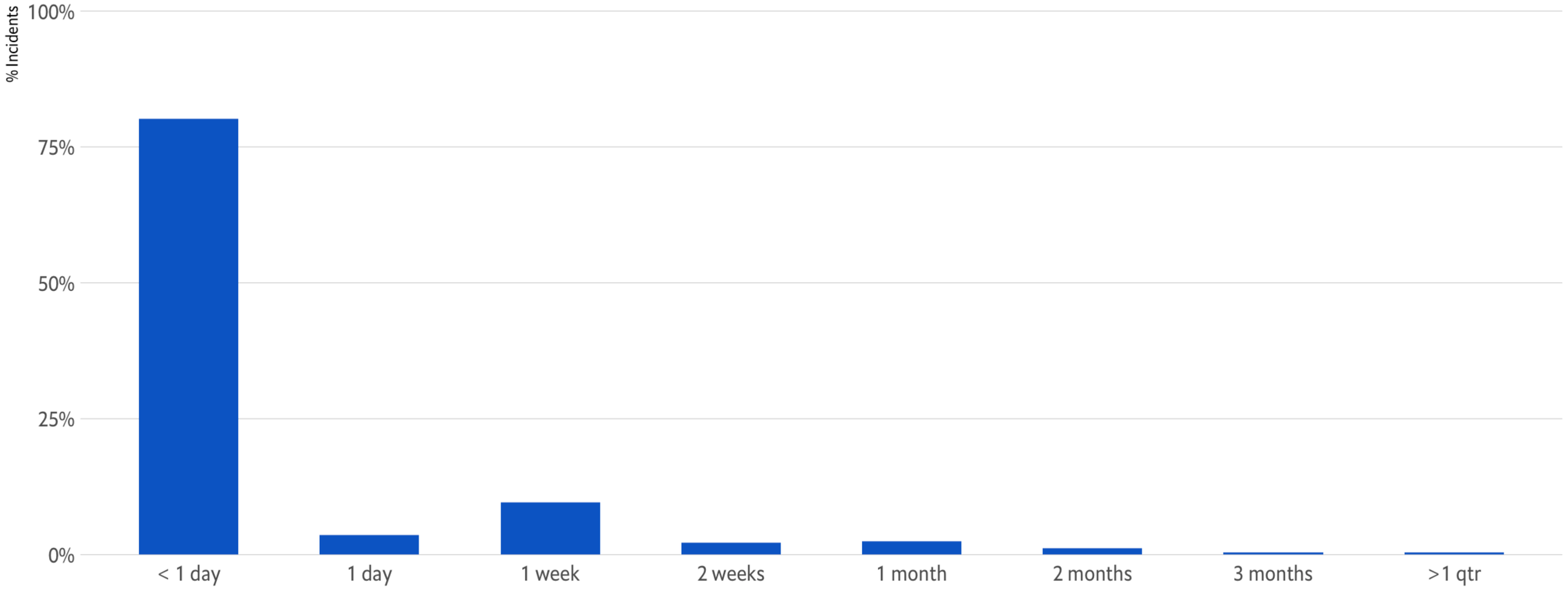

Dwell Time
ATT&CK Heatmap
Cumulative ATT&CK Tactics Distributions
ATT&CK Metrics Overview
Dwell Time
Overall
Dwell Time % (Overall)
by Quarter
Dwell Time % (by Quarter)
Q2
Q3
< 1 day
1 day
1 week
2 weeks
1 month
2 months
3 months
>1 qtr
Unknown

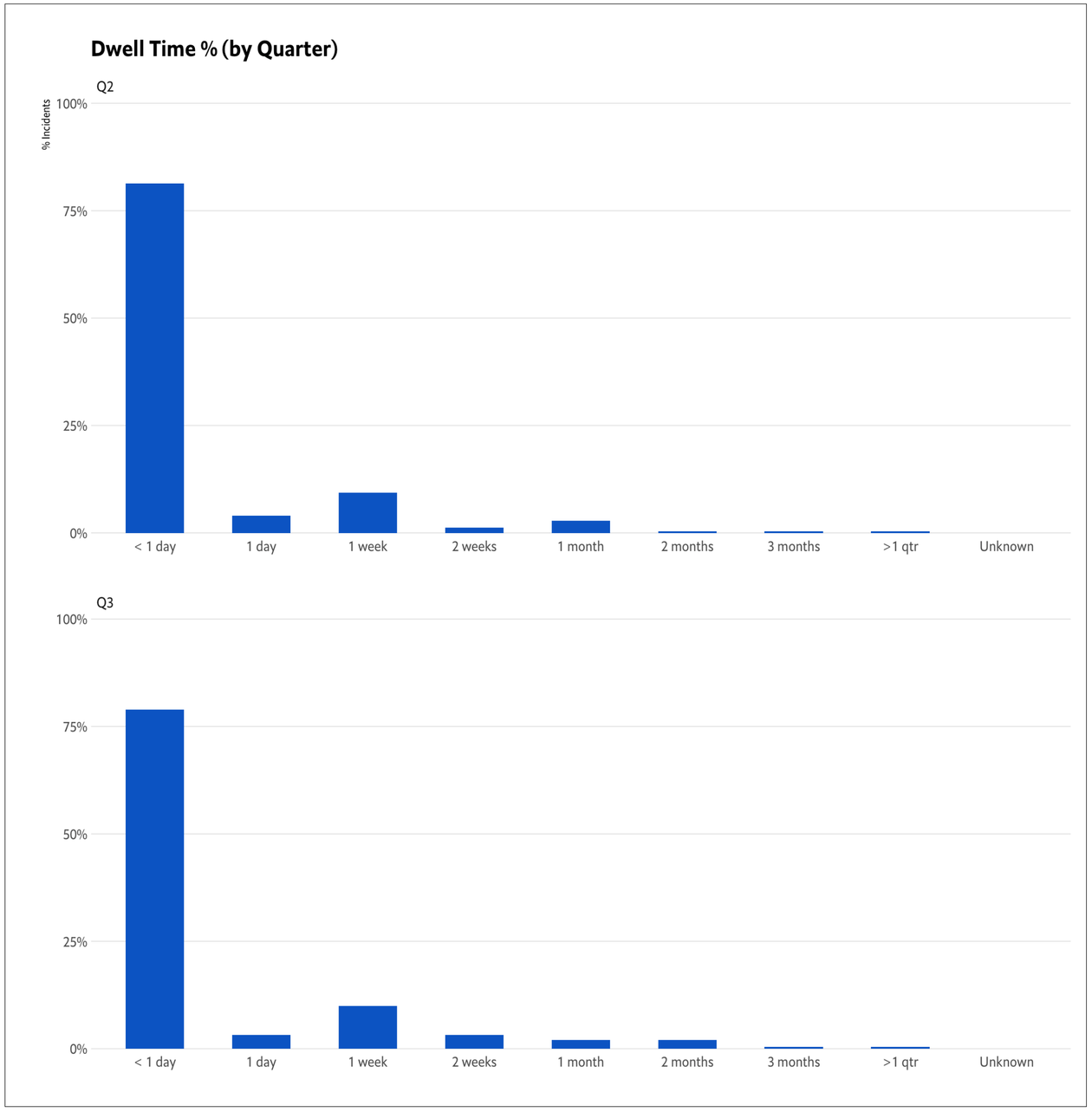

Dwell Time % (by Quarter)
Q3
Q2
79.0%
81.4%
9.9%
9.3%
6.8%
2.8%
6.8%
2.4%
Dwell Time
< 1 day
1 day
1 week
2 weeks
1 month
2 months
3 months
>1 qtr
Unknown
by Month
Dwell Time % (by Month)
April
May
June
July
August
September
78.2%
5.1%
11.5%
2.6%
1.3%
1.3%
84.7%
2.4%
7.1%
3.5%
2.4%
81.0%
4.8%
9.5%
3.6%
1.2%
80.6%
3.2%
9.7%
4.8%
1.6%
81.2%
2.4%
5.9%
1.2%
2.4%
5.9%
1.2%
76.2%
3.8%
13.3%
6.7%
%
23.0%
43.0%
63.0%
83.0%
Dwell Time % (by Month)
September
August
July
June
May
April
76.2%
81.2%
80.6%
81.0%
84.7%
78.2%
13.3%
6.7%
3.8%
5.9%
1.2%
9.7%
4.8%
1.6%
9.5%
1.6%
1.2%
7.1%
2.4%
11.5%
5.1%
1.3%


ATT&CK Heatmap
Overall
Overall ATT&CK Heatmap
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Tactics Raw Count:
by Quarter
Quarterly ATT&CK Heatmap
Q4
Q3


Cumulative ATT&CK Tactics Distributions
Overall
ATT&CK Tactics Cumulative Distribution (All Time)
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
by Industry
ATT&CK Tactics Cumulative Distribution By Industry
Accomodation
Administrative
Construction
Educational
Entertainment
Finance
Healthcare
Information
Management
Manufacturing
Mining
Office Services
Professional
Public
Real Estate
Retail
Trade
Transportation
Utilities

Dwell Time % (Overall)

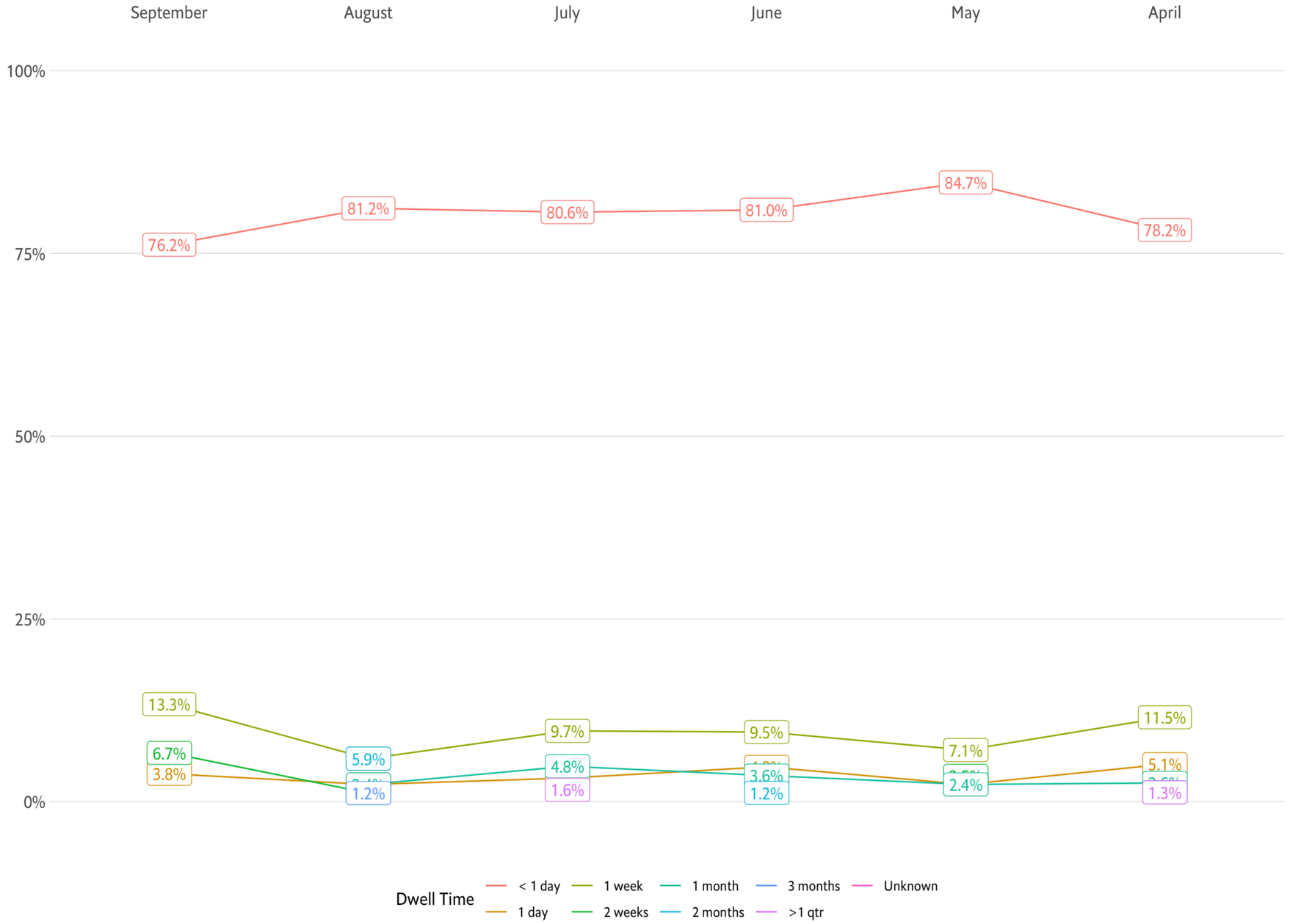



Dwell Time % (by Quarter)
Q2
% Incidents
100%
75%
50%
25%
0%
< 1 day
1 day
1 week
2 weeks
1 month
2 months
3 months
>1 qtr
Unknown
Q3
100%
75%
50%
25%
0%
< 1 day
1 day
1 week
2 weeks
1 month
2 months
3 months
>1 qtr
Unknown

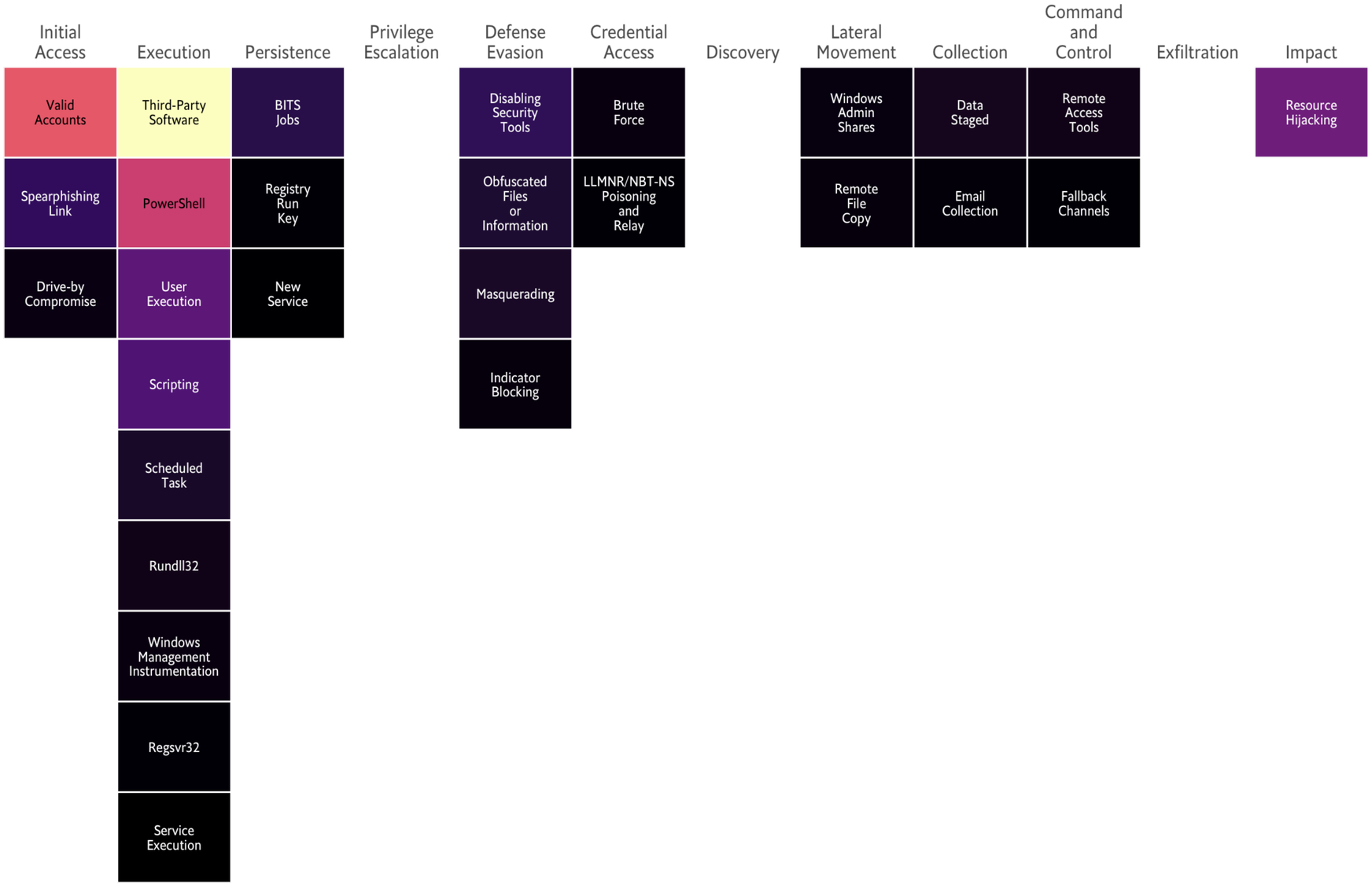

Dwell Time % (by Quarter)
Q3
Q2
100%
75%
50%
25%
0%
79.0%
81.4%
9.9%
9.3%
2.8%
0.4%
0.4%
Dwell Time
< 1 day
1 day
1 week
2 weeks
1 month
2 months
3 months
>1 qtr
Unknown

Dwell Time % (by Month)

Dwell Time % (by Month)

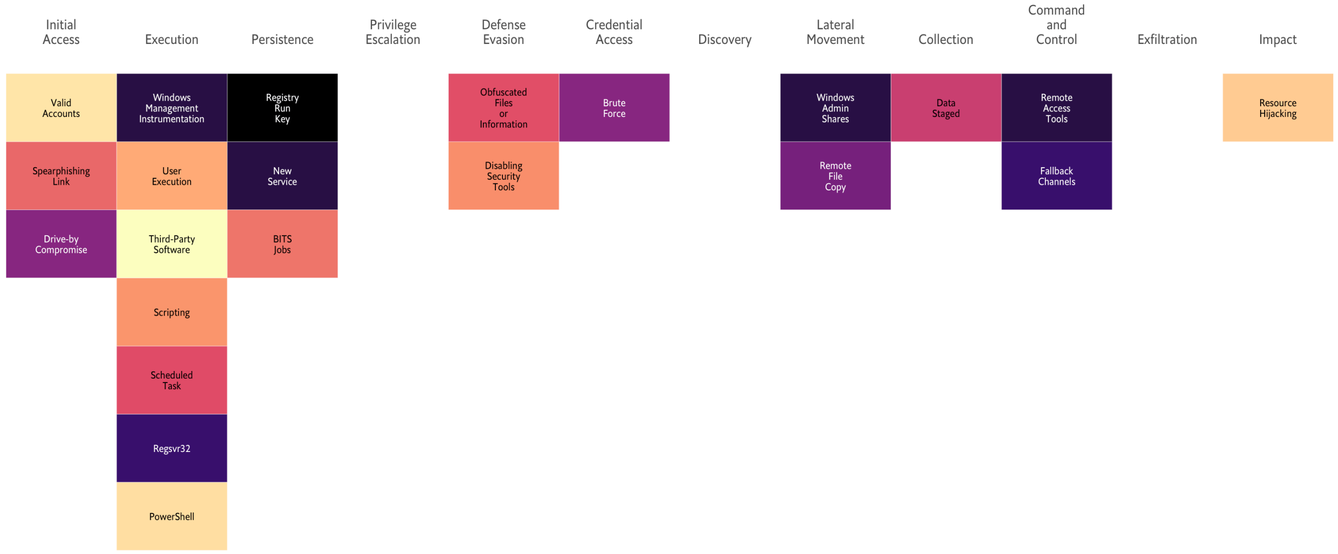


Overall ATT&CK Heatmap

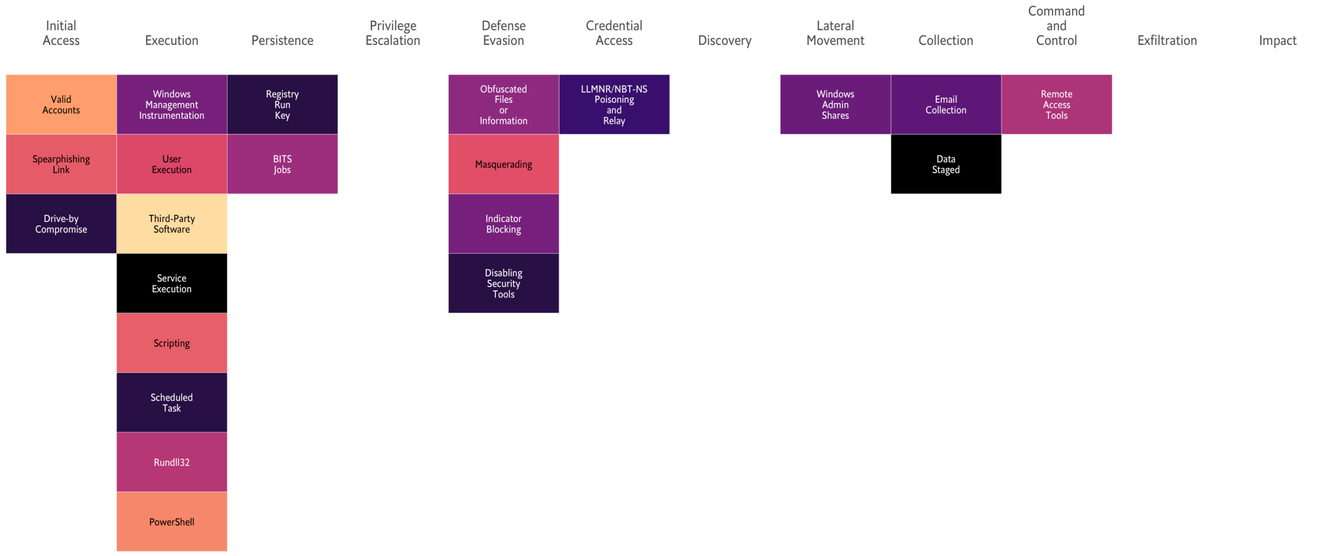


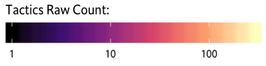
Quarterly ATT&CK Heatmap

Q2

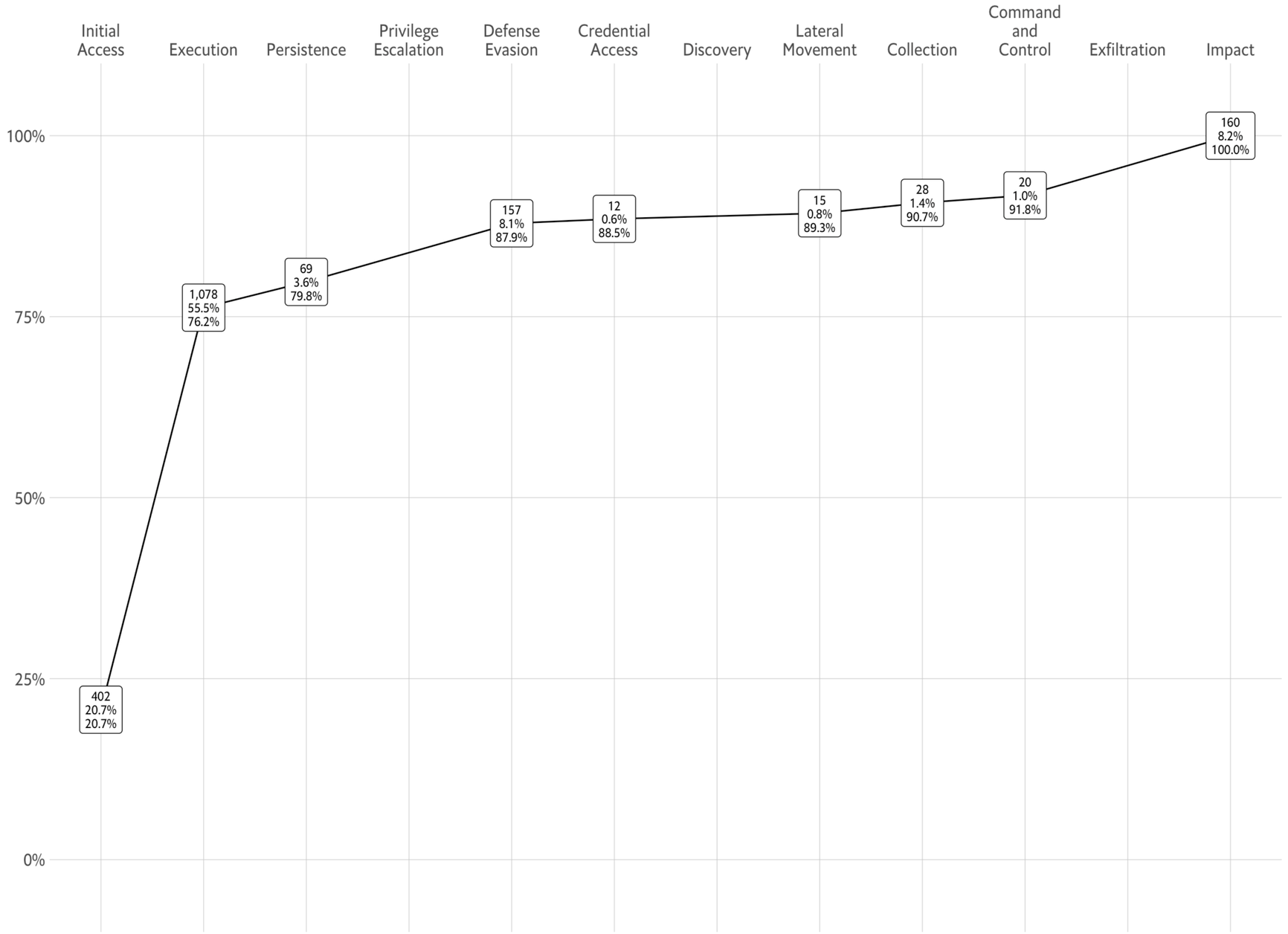


Q3

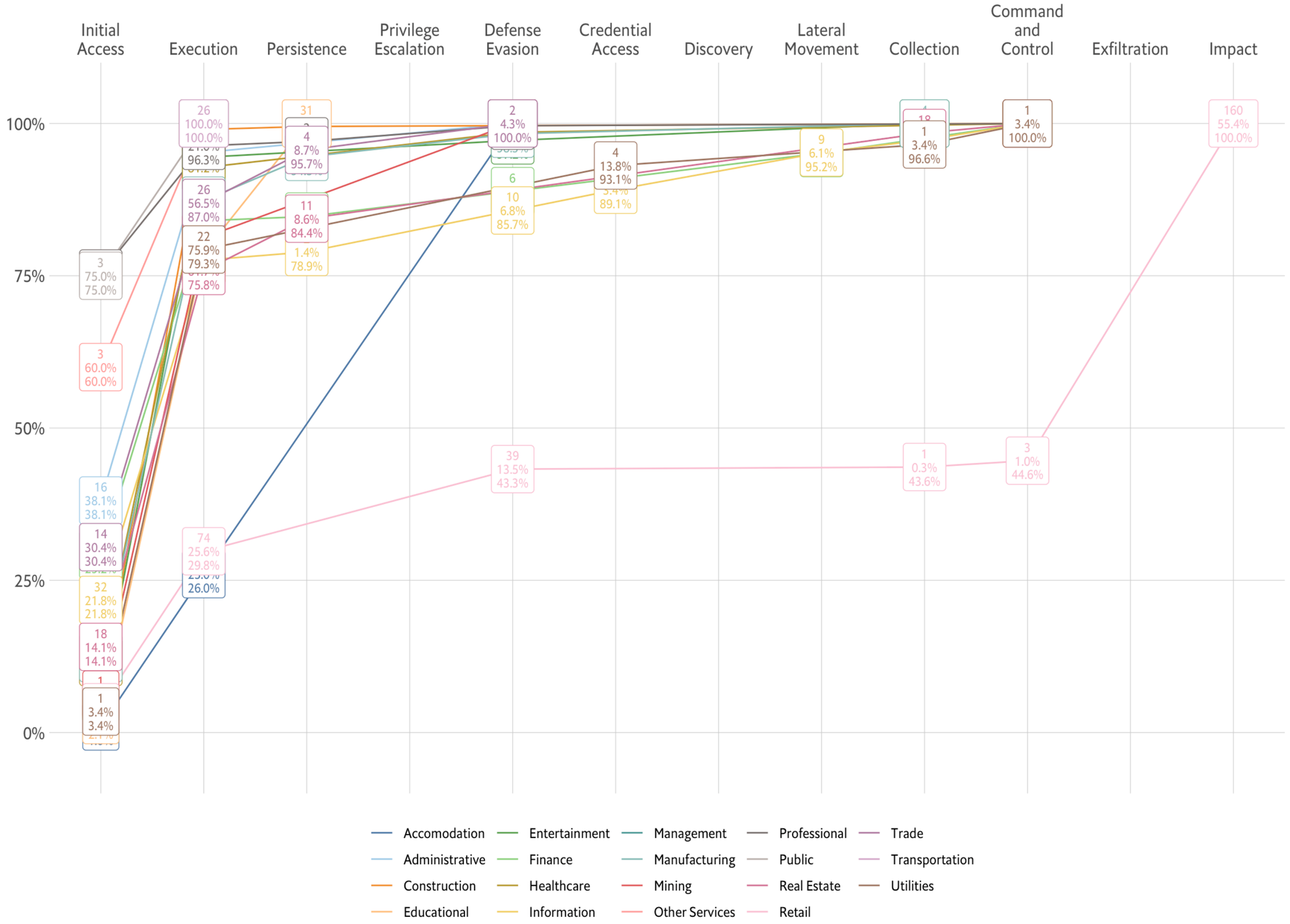




ATT&CK Tactics Cumulative Distribution (All Time)



ATT&CK Tactics Cumulative Distribution By Industry



{attckr} v0.3.0

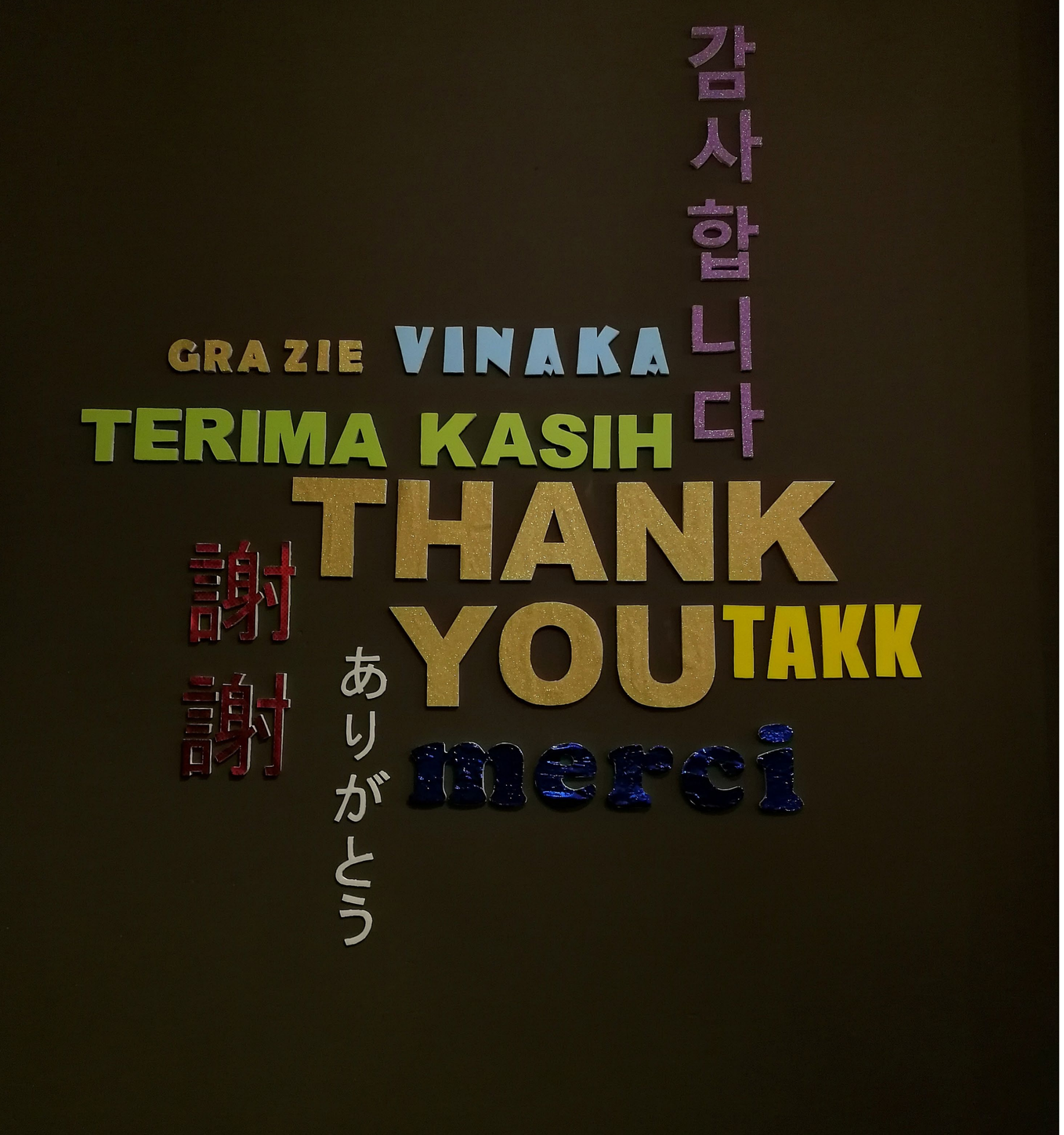
- More standard charts
- ATT&CK Tactic + Technique event timestamp support
- Functions and R Markdown template for interactive charts

{attckr} v0.4.0

- 0 coding skills required Shiny App
- {flexdashboard} R Markdown template

{attckr} v0.5.0

- ATT&CK Tactic + Technique Event Stream Analysis & Visualization



@hrbrmstr
research@rapid7.com
bob@rud.is
https://rud.is/
https://github.com/hrbrmstr
https://blog.rapid7.com/

Photo by Lip on Unsplash