Carnegie Mellon University
Software Engineering Institute

# Insider Threat Tool Survey Results 2021

Open Source Insider Threat Information Sharing Group

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

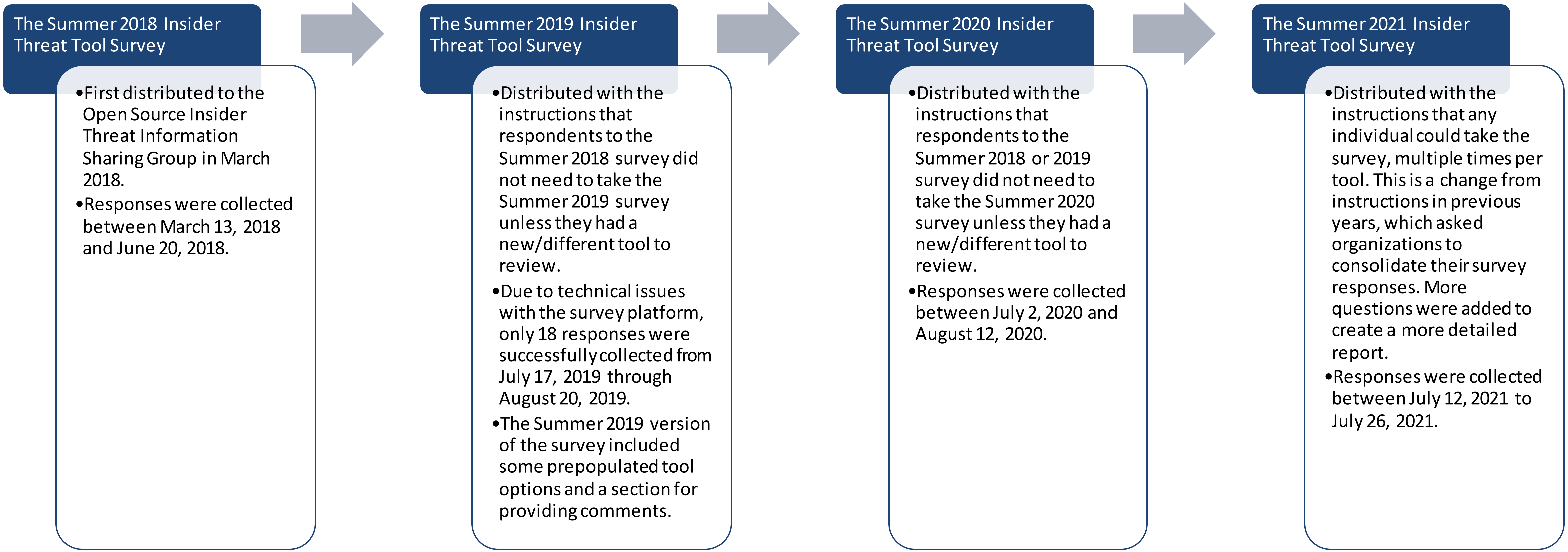
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM21-0718

# Tool Survey Timeline



**The Summer 2018 Insider Threat Tool Survey**

- First distributed to the Open Source Insider Threat Information Sharing Group in March 2018.
- Responses were collected between March 13, 2018 and June 20, 2018.

**The Summer 2019 Insider Threat Tool Survey**

- Distributed with the instructions that respondents to the Summer 2018 survey did not need to take the Summer 2019 survey unless they had a new/different tool to review.
- Due to technical issues with the survey platform, only 18 responses were successfully collected from July 17, 2019 through August 20, 2019.
- The Summer 2019 version of the survey included some prepopulated tool options and a section for providing comments.

**The Summer 2020 Insider Threat Tool Survey**

- Distributed with the instructions that respondents to the Summer 2018 or 2019 survey did not need to take the Summer 2020 survey unless they had a new/different tool to review.
- Responses were collected between July 2, 2020 and August 12, 2020.

**The Summer 2021 Insider Threat Tool Survey**

- Distributed with the instructions that any individual could take the survey, multiple times per tool. This is a change from instructions in previous years, which asked organizations to consolidate their survey responses. More questions were added to create a more detailed report.
- Responses were collected between July 12, 2021 to July 26, 2021.

# Reminders

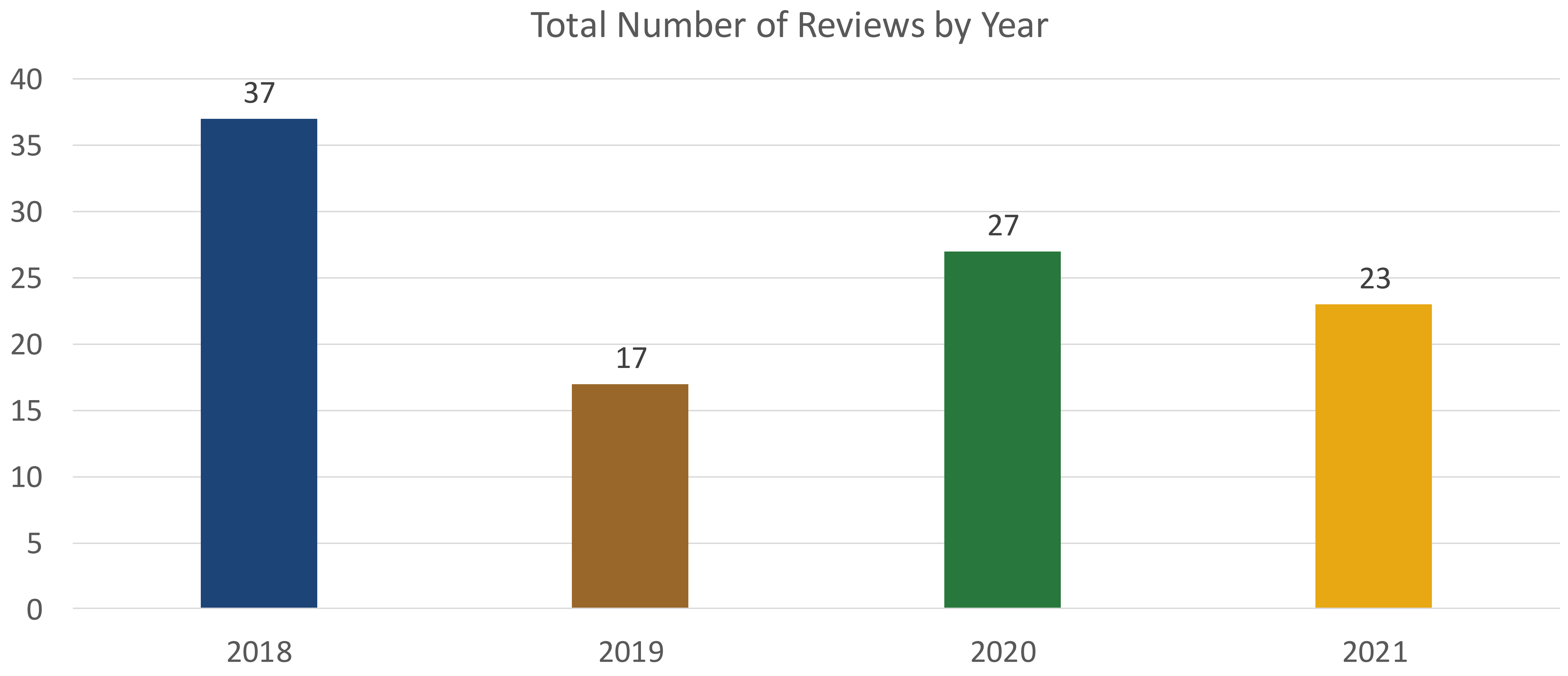
- All survey responses were collected anonymously.
- While the 2018 results included demographics for organizations that responded but did not have a complete tool review, those are not included for the 2019 or 2020 results, or this summary document.
- Do not distribute these results outside of the Open Source Insider Threat Information Sharing Group or Data Analytics Special Interest Group.
- The Chatham House Rules apply to the results and discussion of this survey.
- **The results of the survey should not be interpreted as an endorsement by the CERT, Software Engineering Institute, Carnegie Mellon University, or any other entity.**

Insider Threat Tool Survey Results
2018 - 2021

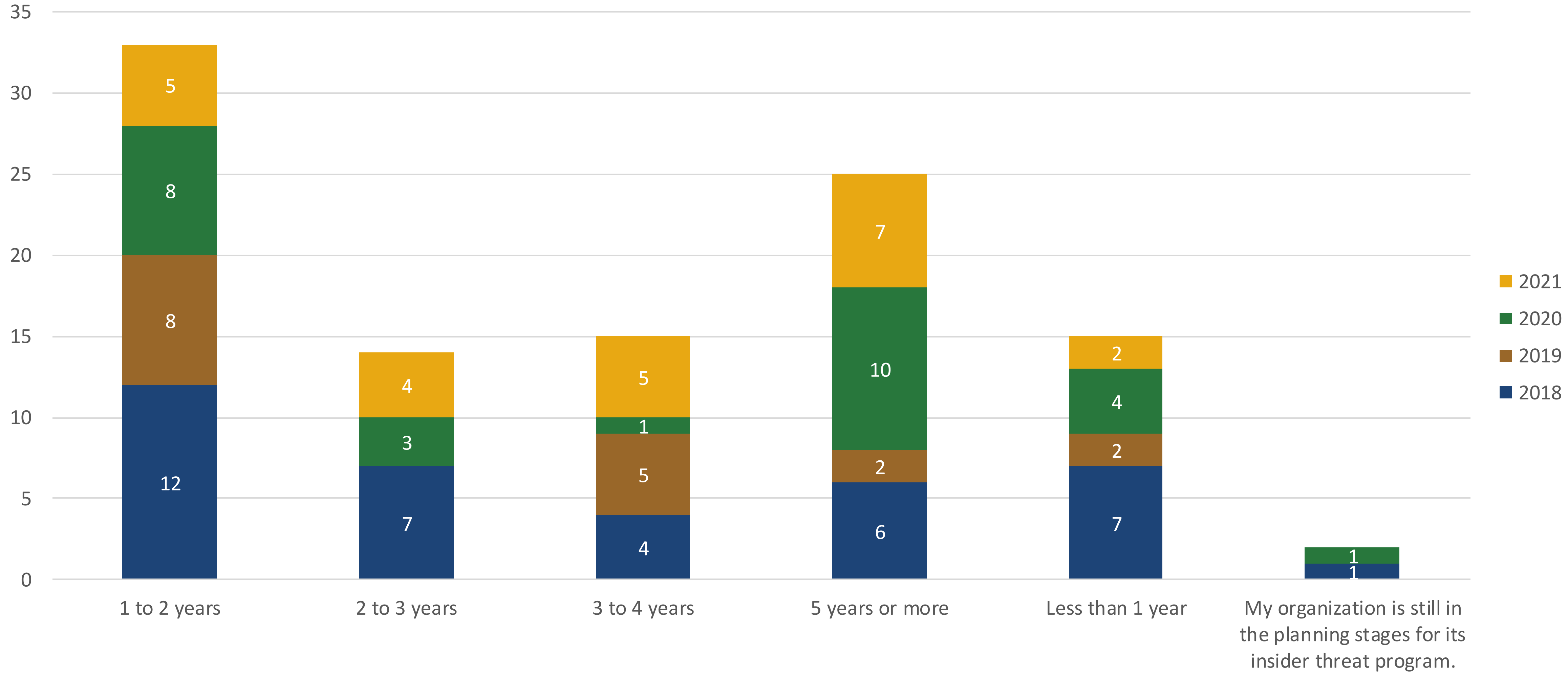
# Contextual Information,

# Comparing 2018 through 2021

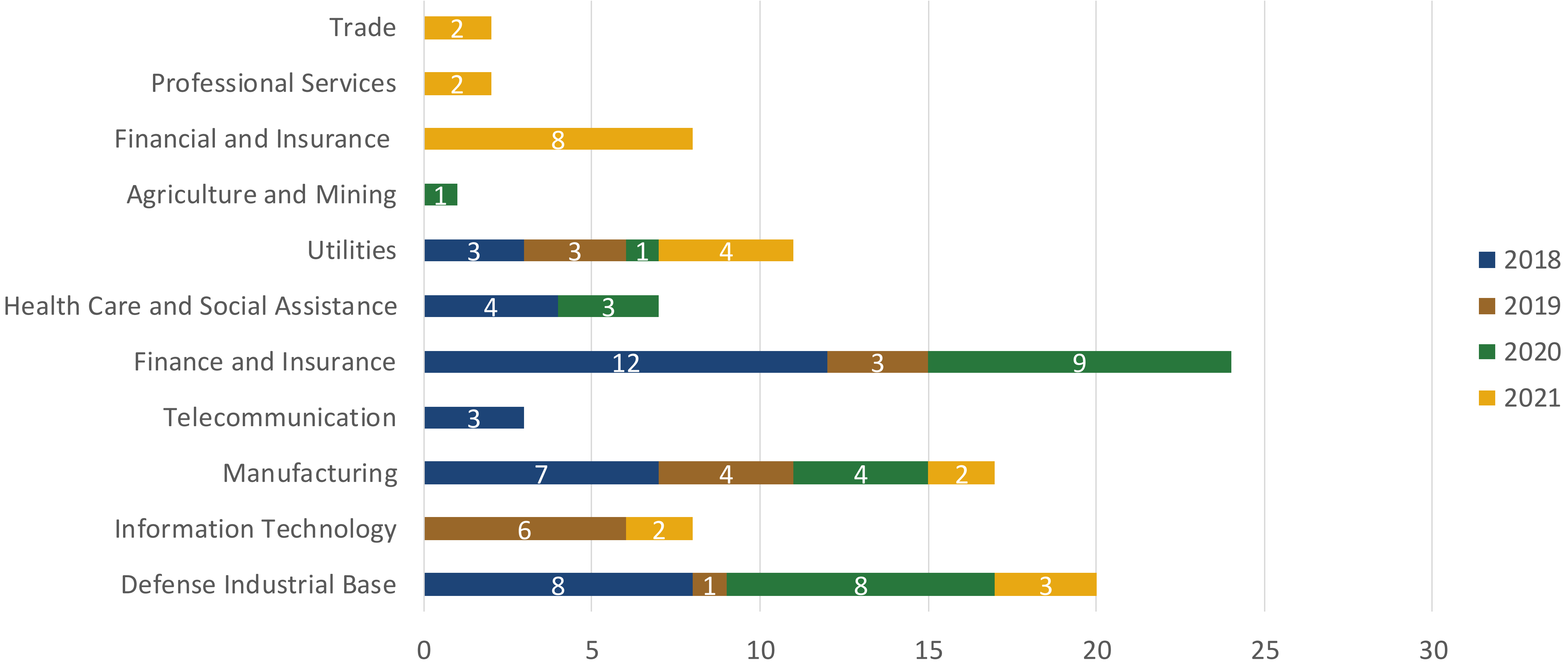
# Total Annuals Reviews by Year



# Annual Reviews by Age of Insider Threat Program



# Annual Reviews by Industry



Insider Threat Tool Survey Results 2021

# 2021 Tool Review Summary

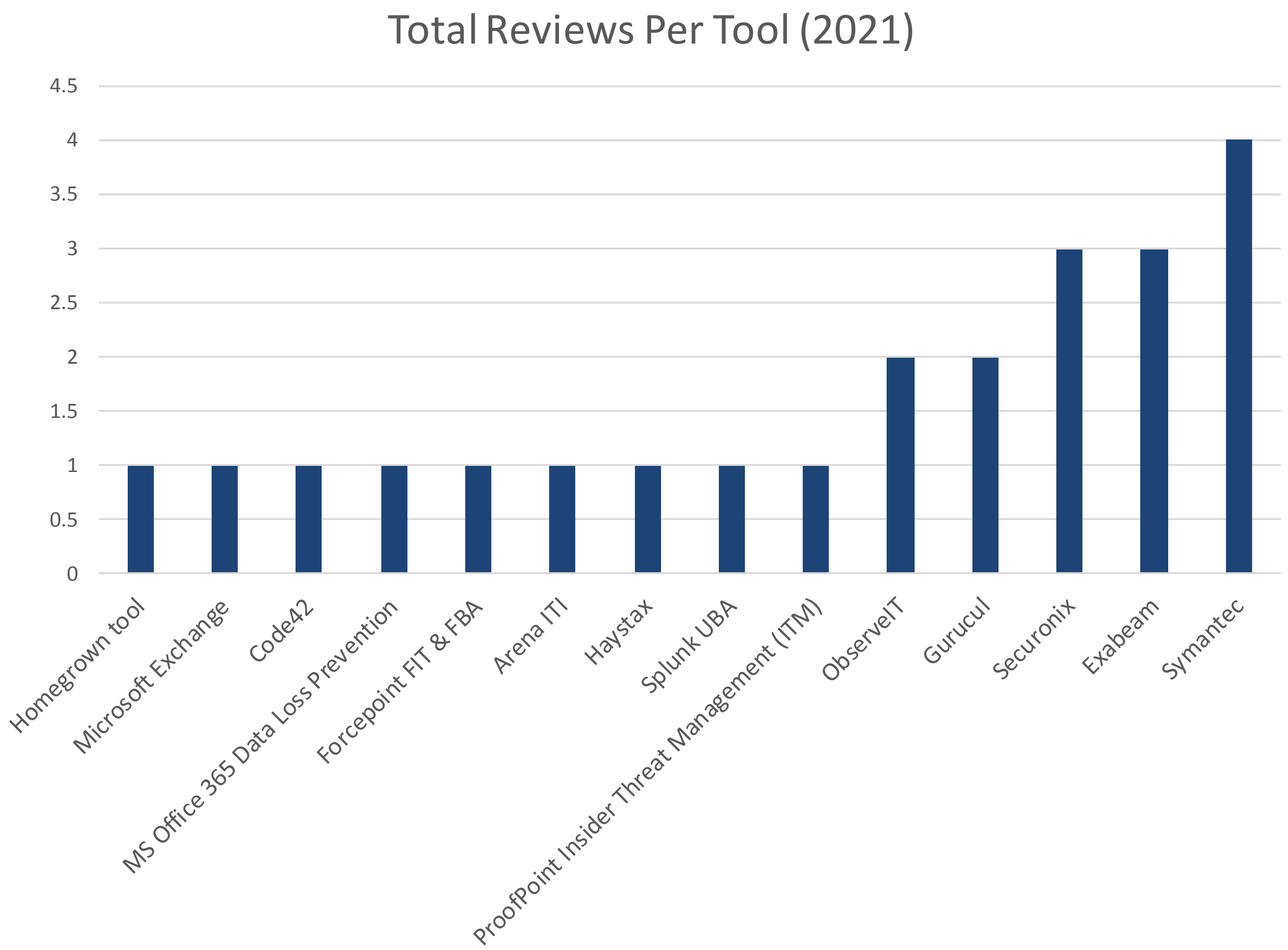
# Reviews by the Numbers

Overall, we had **23** reviews across **13** industry tools and **1** home grown tool.

Symnatec was the most commonly reviewed, followed by Exabeam and Securonix tied for second.

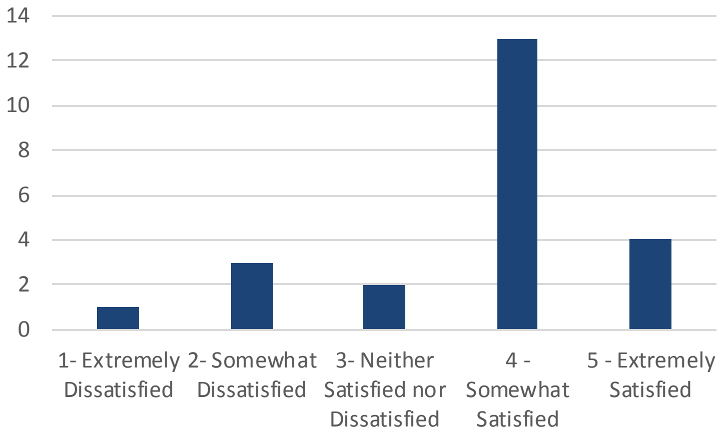
# Tools Reviewed, Total Reviews per Tool

| Tool Name | Number of Responses |
|---|---|
| Arena ITI | 1 |
| Code42 | 1 |
| Exabeam | 3 |
| Forcepoint FIT & FBA | 1 |
| Gurucul | 2 |
| Haystax | 1 |
| Homegrown tool | 1 |
| Microsoft Exchange | 1 |
| MS Office 365 Data Loss Prevention | 1 |
| ObserveIT | 2 |
| ProofPoint Insider Threat Management (ITM) | 1 |
| Securonix | 3 |
| Splunk UBA | 1 |
| Symantec | 4 |
| **Grand Total** | **23** |

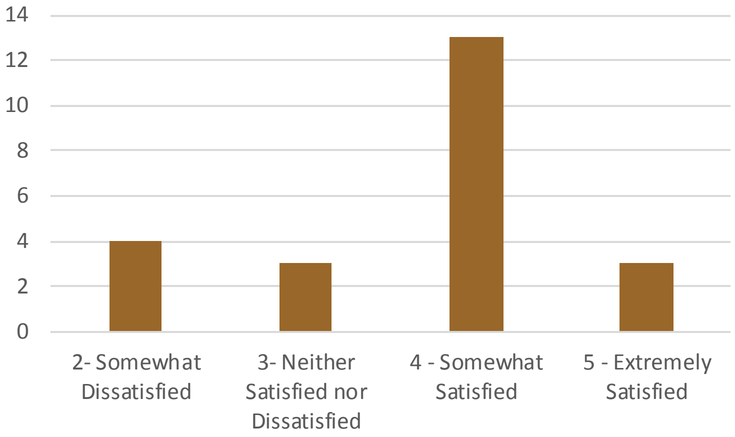


# Of those reviewed, most were Satisfactory with good Usability and Fit, and Configurability. Maintenance Requirements were average.

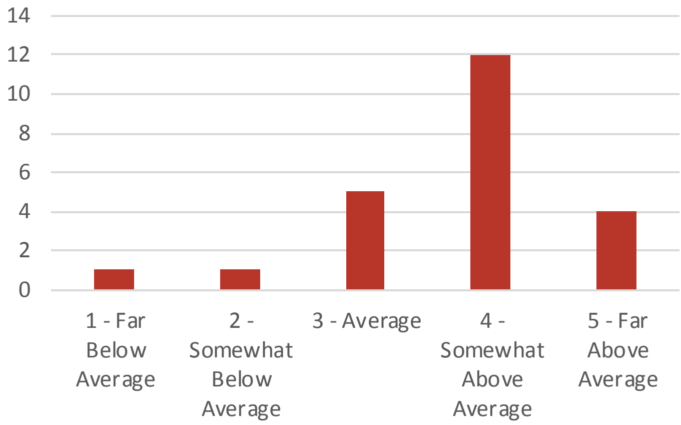
Total Satisfaction Across Tools



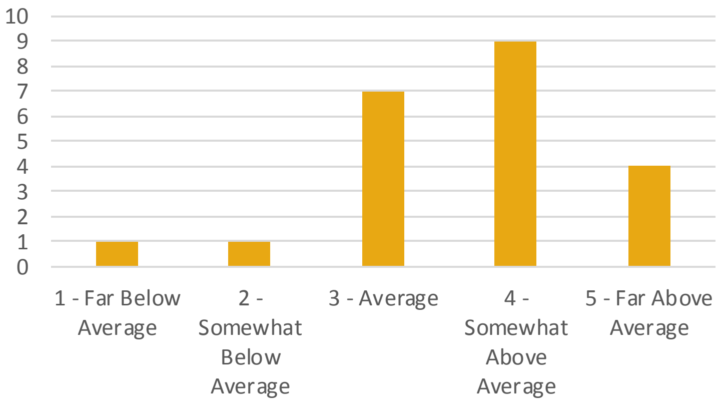
Total Fit Across Tools Across Tools



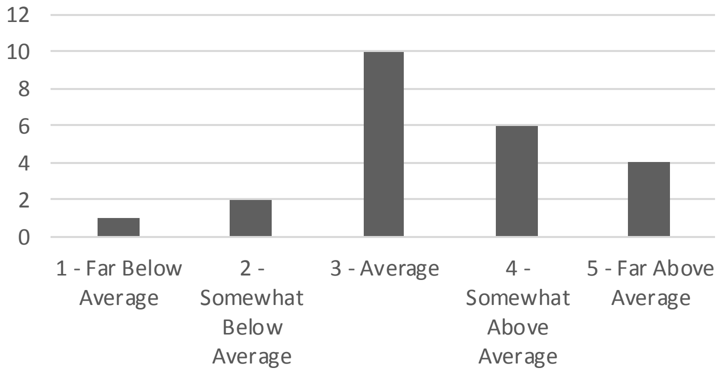
Total Usability Across Tools



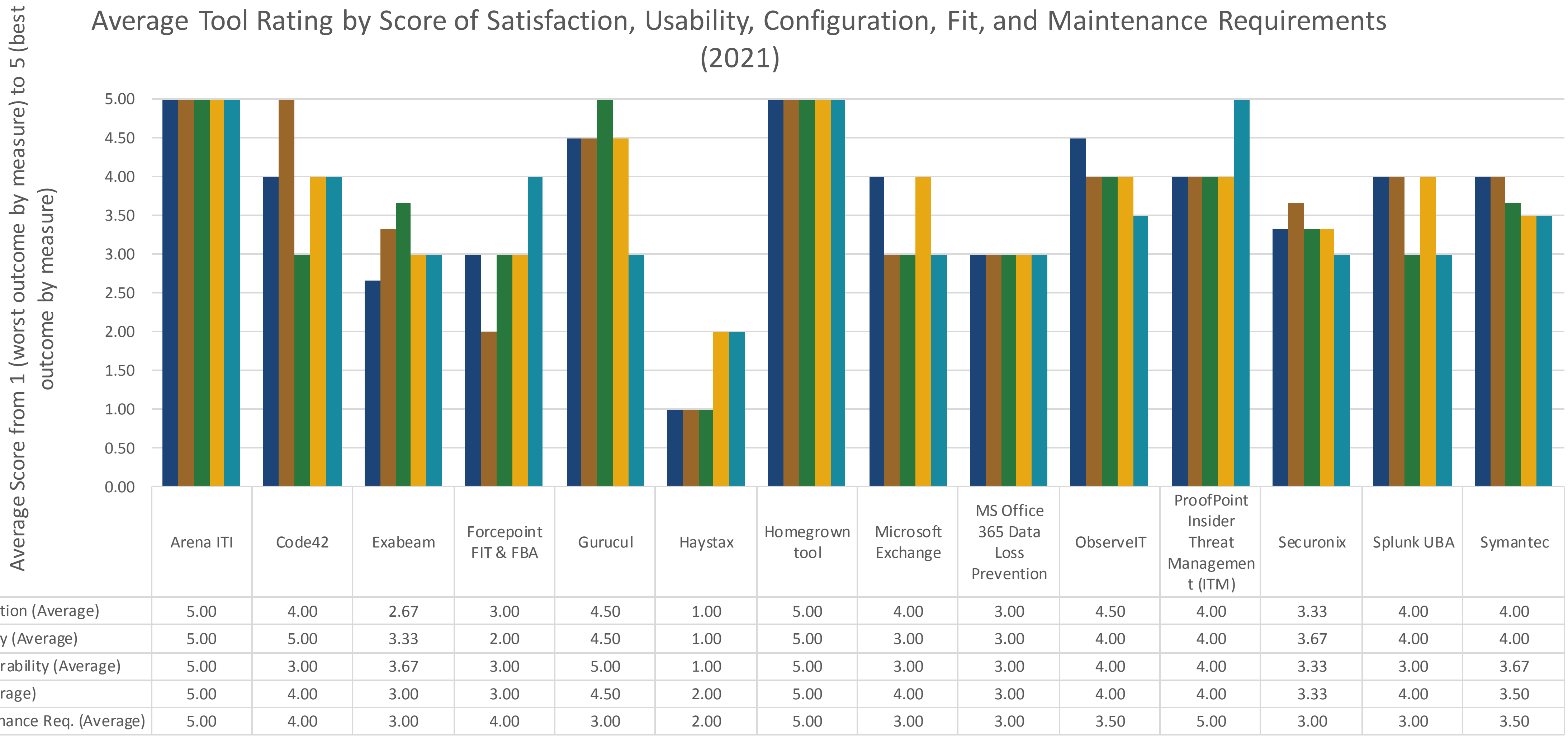
Total Configurability Across Tools



Total Maintenance Requirements Across Tools



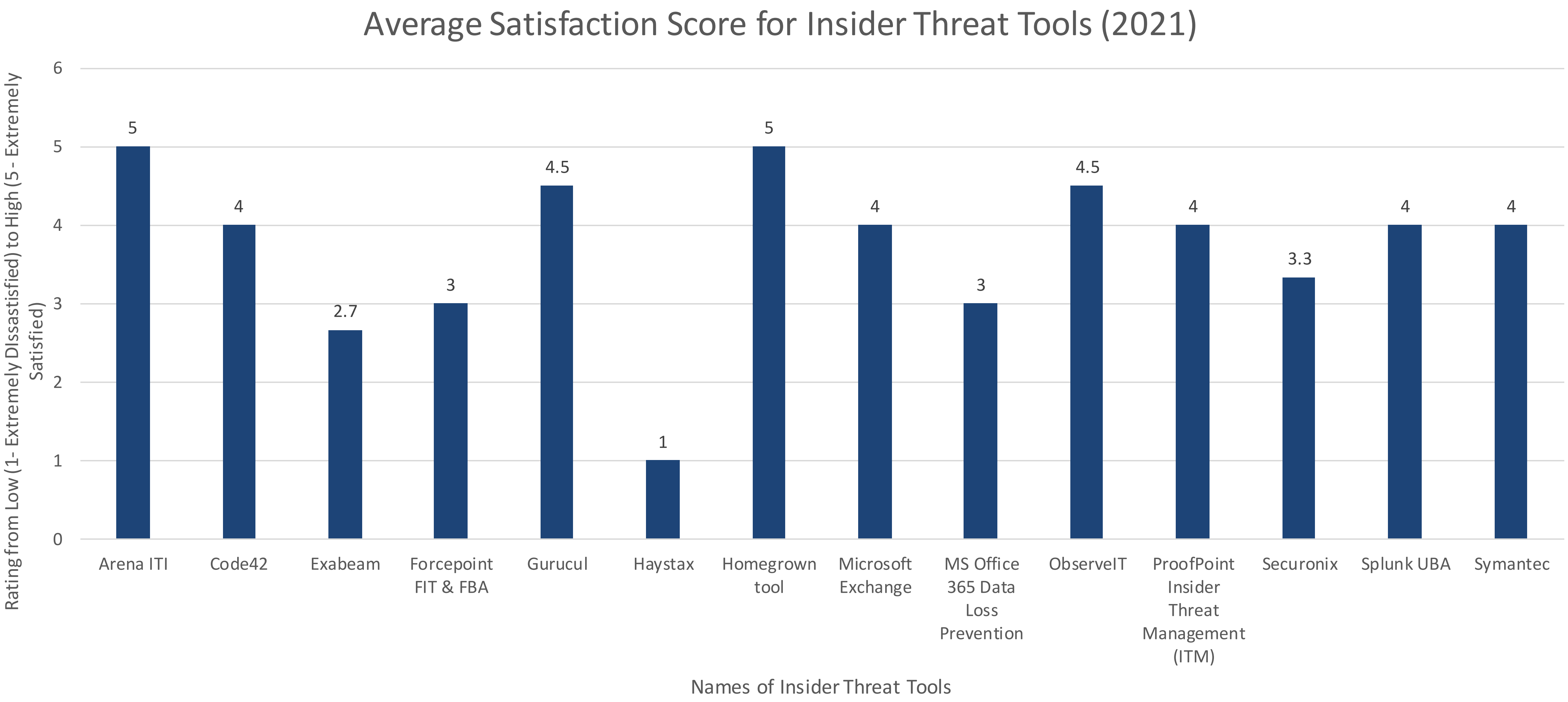
# Overall Average Tool Ratings Across 5 Metrics



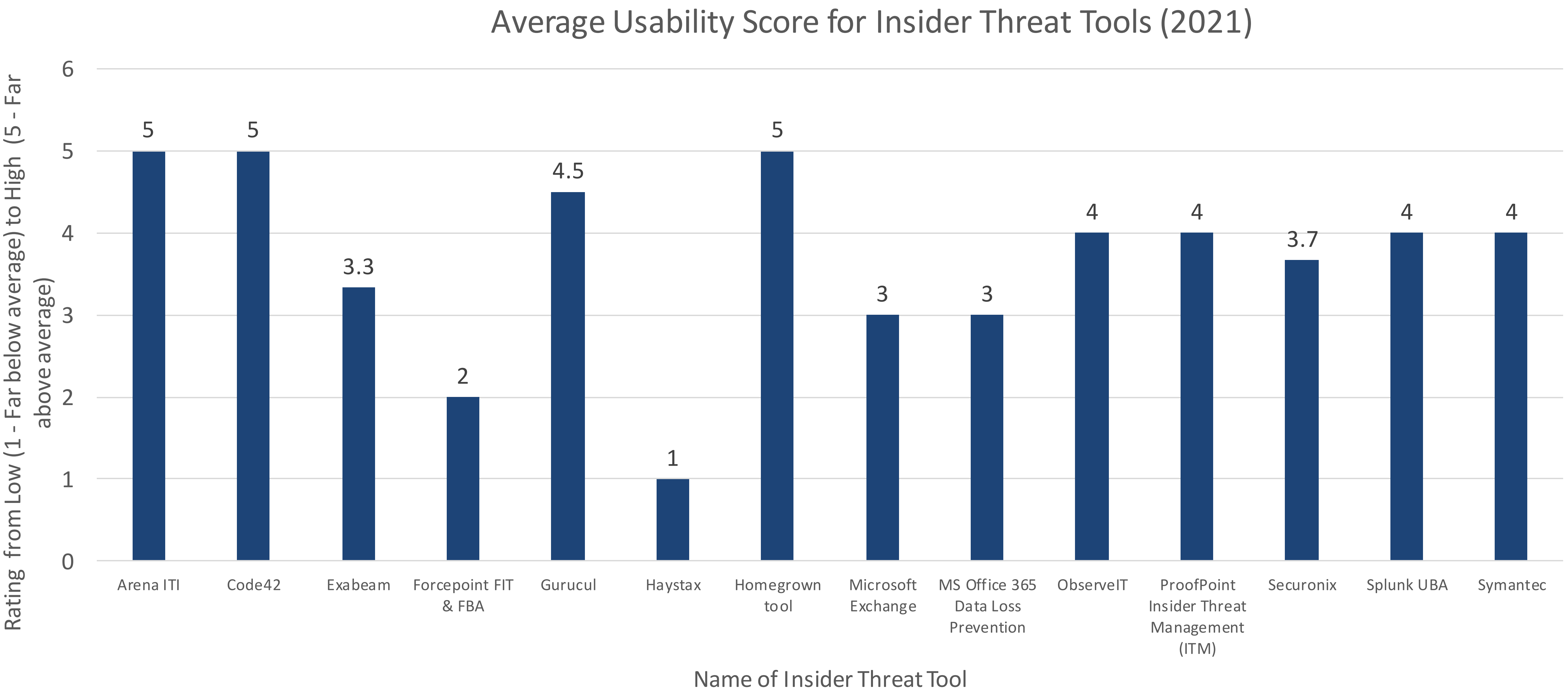
Average Tool Rating by Score of Satisfaction, Usability, Configuration, Fit, and Maintenance Requirements (2021)

| | Arena ITI | Code42 | Exabeam | Forcepoint FIT & FBA | Gurucul | Haystax | Homegrown tool | Microsoft Exchange | MS Office 365 Data Loss Prevention | ObserveIT | ProofPoint Insider Threat Management (ITM) | Securonix | Splunk UBA | Symantec |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ■ Satisfaction (Average) | 5.00 | 4.00 | 2.67 | 3.00 | 4.50 | 1.00 | 5.00 | 4.00 | 3.00 | 4.50 | 4.00 | 3.33 | 4.00 | 4.00 |
| ■ Usability (Average) | 5.00 | 5.00 | 3.33 | 2.00 | 4.50 | 1.00 | 5.00 | 3.00 | 3.00 | 4.00 | 4.00 | 3.67 | 4.00 | 4.00 |
| ■ Configurability (Average) | 5.00 | 3.00 | 3.67 | 3.00 | 5.00 | 1.00 | 5.00 | 3.00 | 3.00 | 4.00 | 4.00 | 3.33 | 3.00 | 3.67 |
| ■ Fit (Average) | 5.00 | 4.00 | 3.00 | 3.00 | 4.50 | 2.00 | 5.00 | 4.00 | 3.00 | 4.00 | 4.00 | 3.33 | 4.00 | 3.50 |
| ■ Maintenance Req. (Average) | 5.00 | 4.00 | 3.00 | 4.00 | 3.00 | 2.00 | 5.00 | 3.00 | 3.00 | 3.50 | 5.00 | 3.00 | 3.00 | 3.50 |

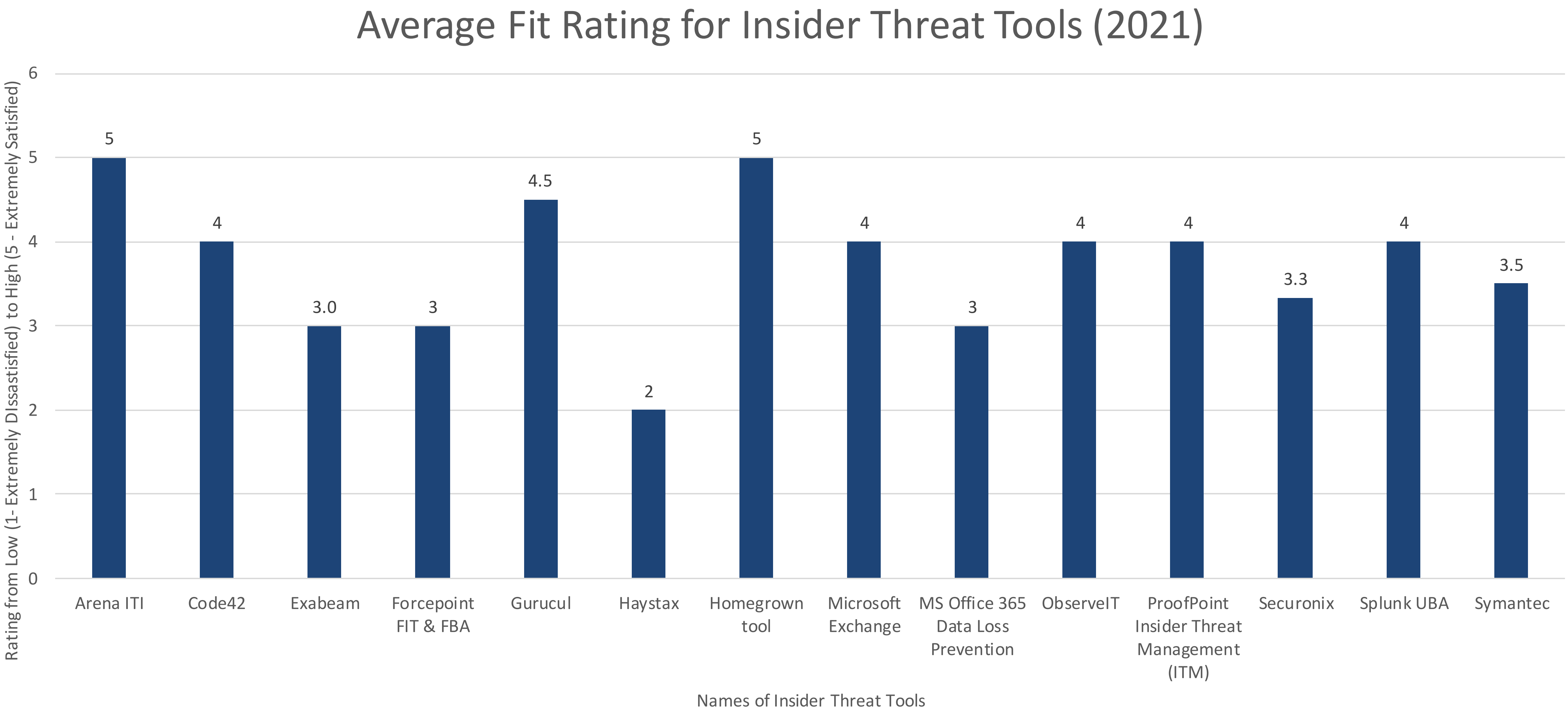
# Overall Average Rating - Satisfaction



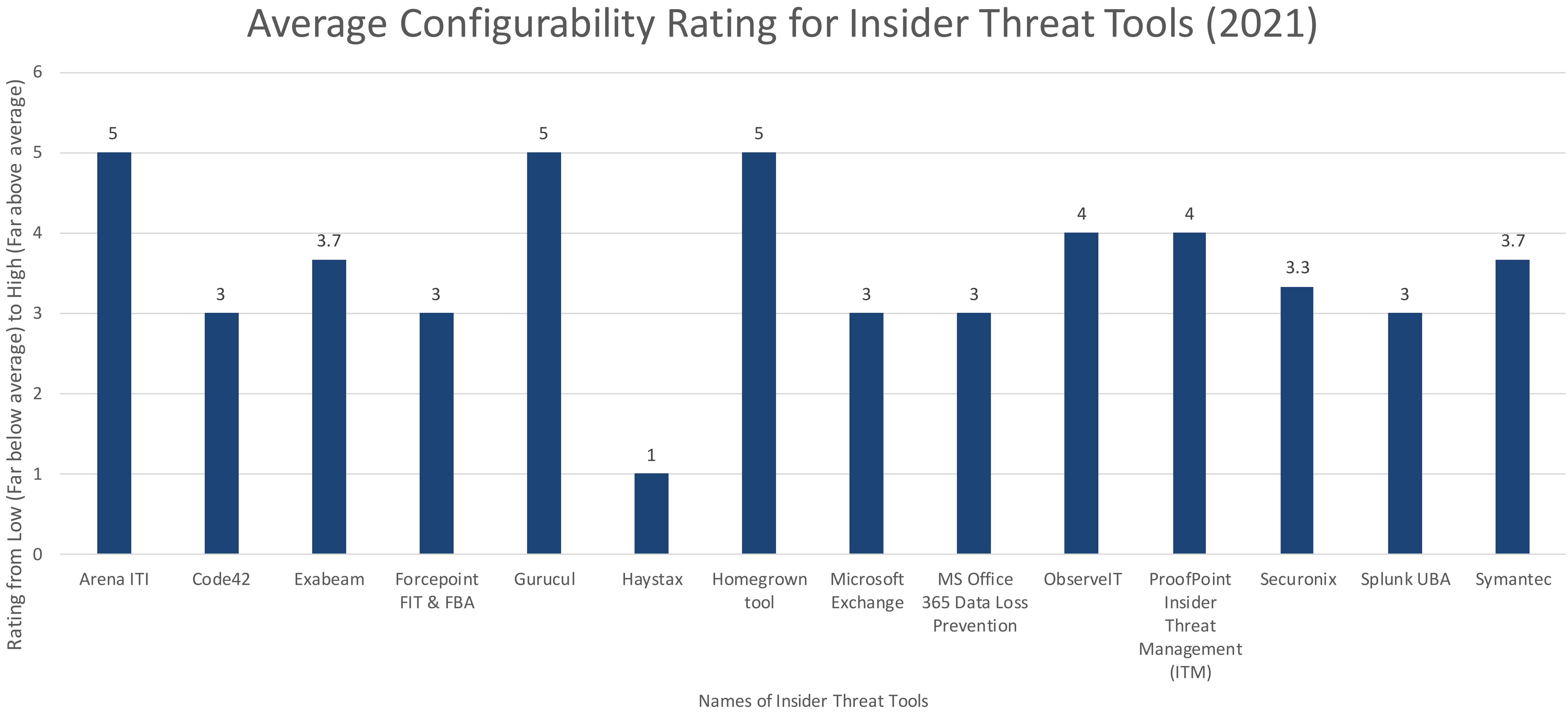
# Overall Average Rating - Usability



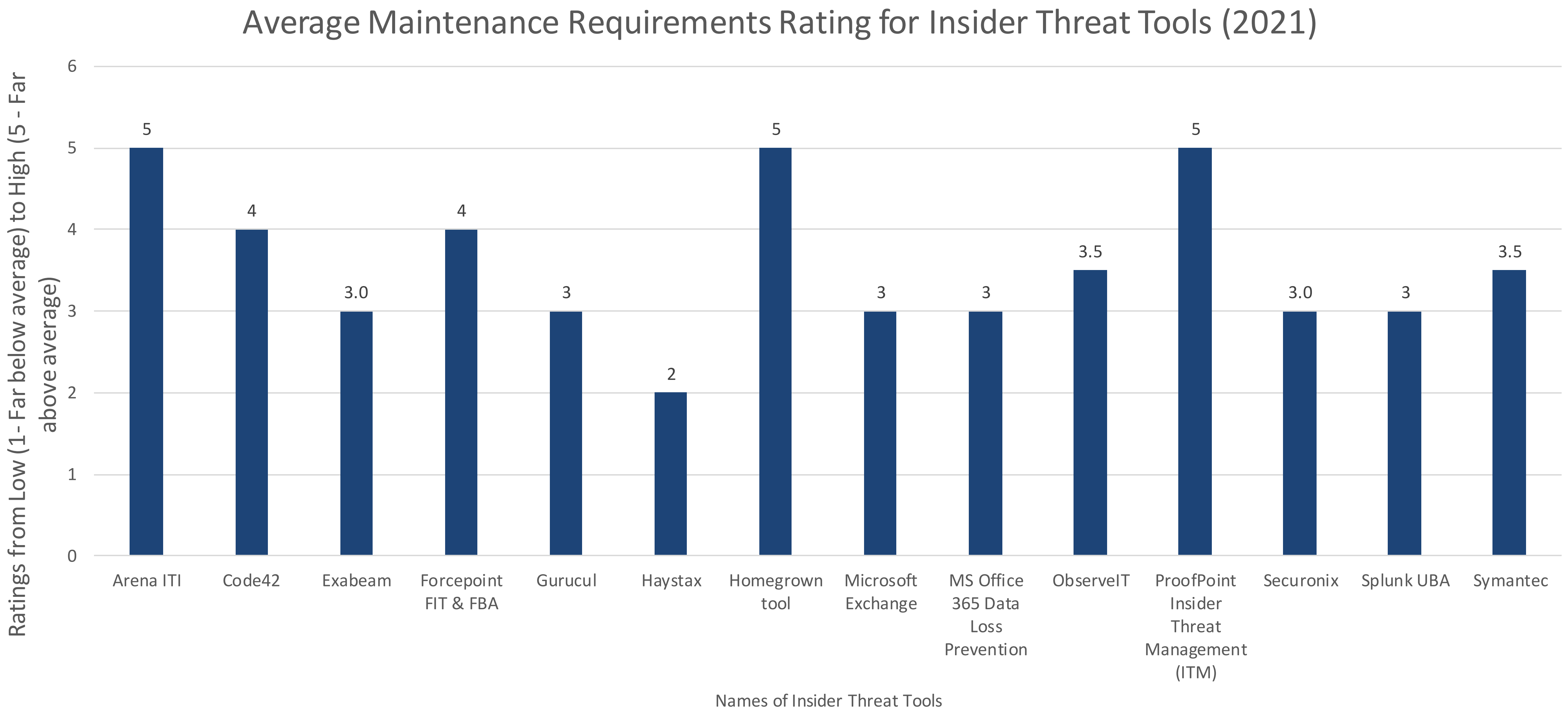
# Overall Average Rating - Fit



# Overall Average Rating - Configurability



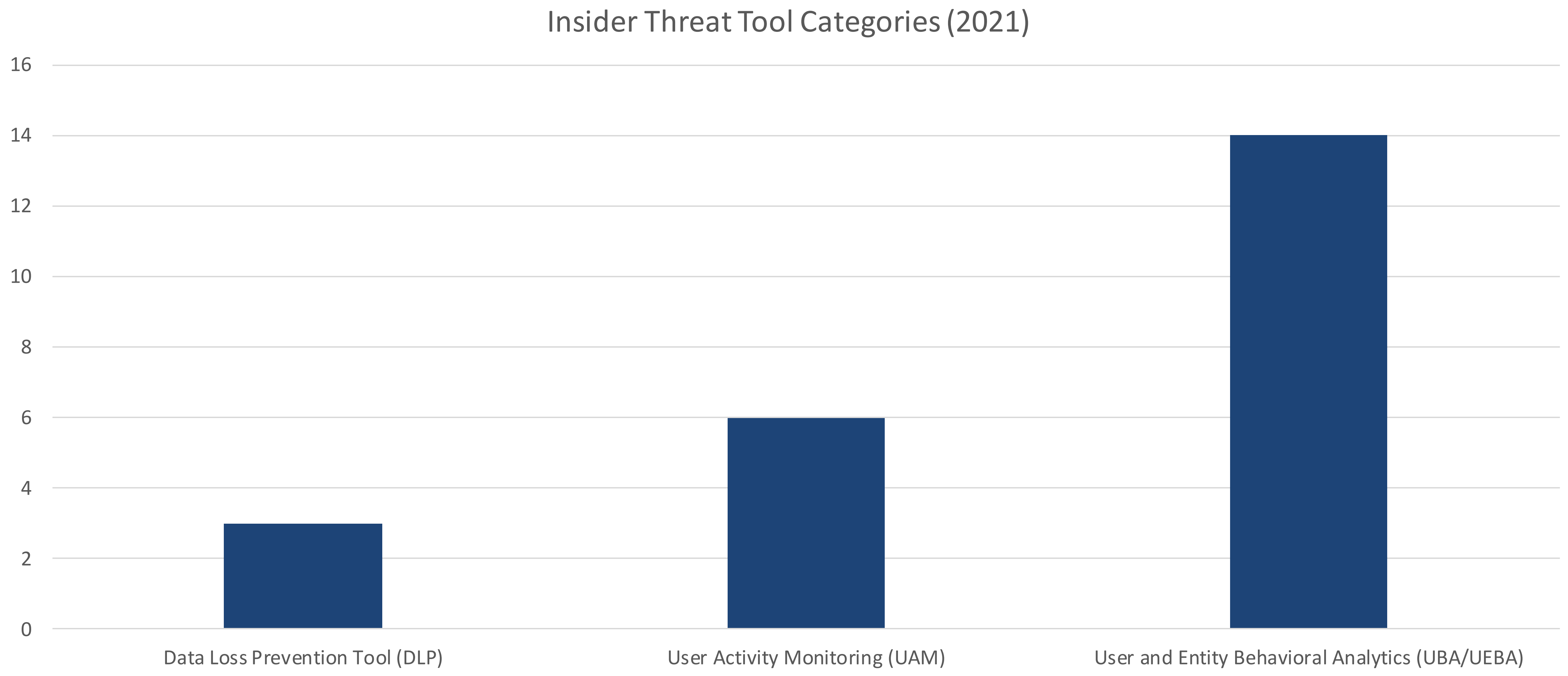
# Overall Average Rating – Maintenance Requirements



Insider Threat Tool Survey Results 2021

# 2021 Tool Reviews by Member-Assigned Category

# Tool Categories



# UBA/UEBA Tool Reviews

| User and Entity Behavioral Analytics (UBA/UEBA) | 14 |
|---|---|
| Arena ITI | 1 |
| Exabeam | 2 |
| Forcepoint FIT & FBA | 1 |
| Gurucul | 2 |
| Haystax | 1 |
| Securonix | 3 |
| Splunk UBA | 1 |
| Symantec | 3 |

# User Activity Monitoring (UAM) Reviews

| User Activity Monitoring (UAM) | 6 |
|---|---|
| Code42 | 1 |
| Exabeam | 1 |
| Homegrown tool | 1 |
| ObserveIT | 2 |
| ProofPoint Insider Threat Management (ITM) | 1 |

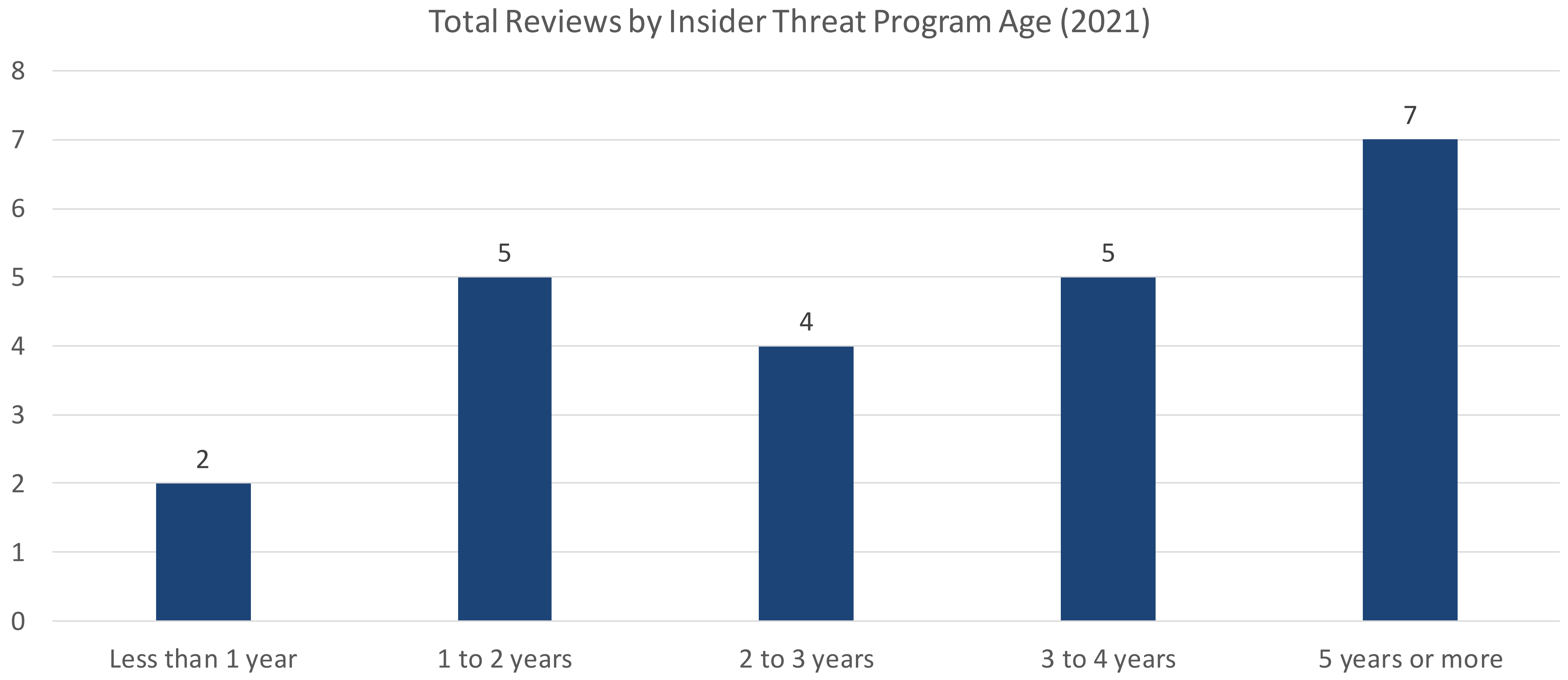
# Data Loss Prevention Reviews

| Data Loss Prevention Tool (DLP) | 3 |
|---|---|
| Microsoft Exchange | 1 |
| MS Office 365 Data Loss Prevention | 1 |
| Symantec | 1 |

Insider Threat Tool Survey Results 2021

# 2021 Tool Reviews by Age of Program

# Tool Reviews by Age of Program



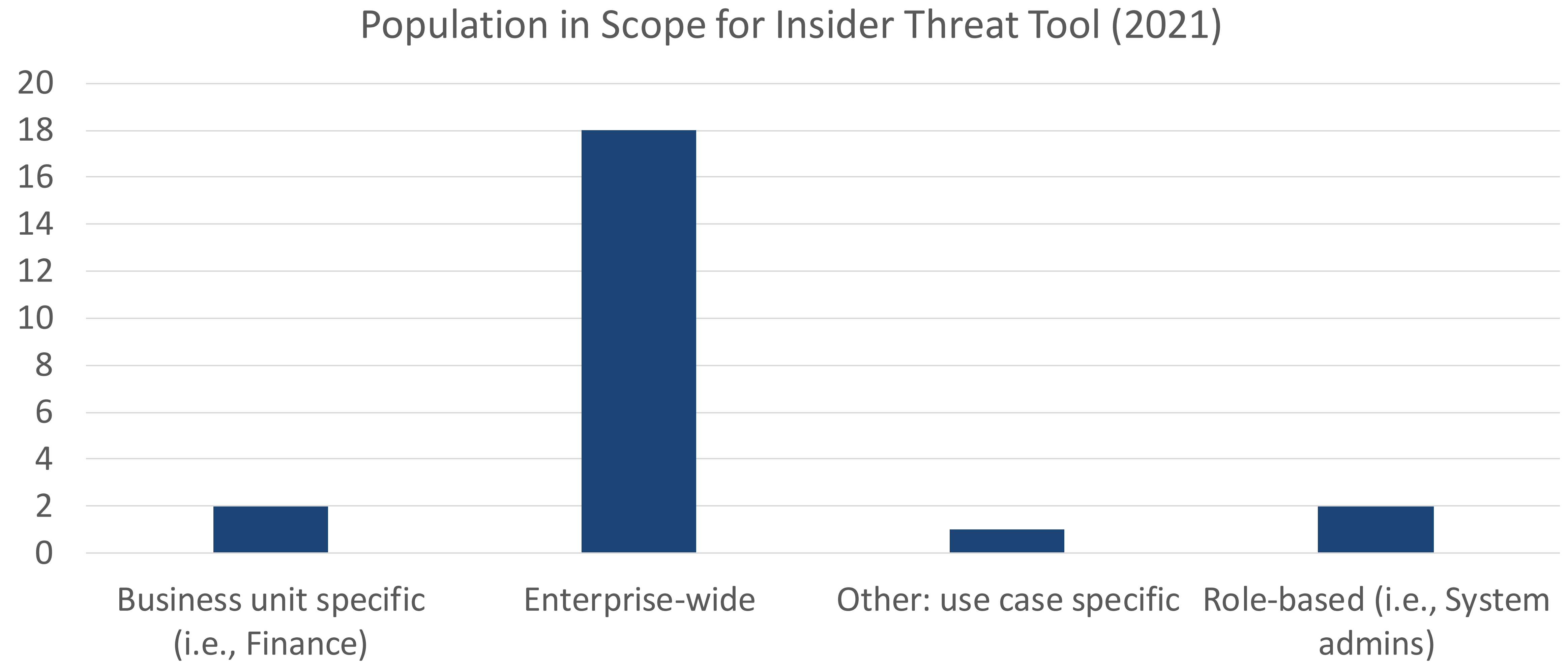
# Tool Reviews by Insider Threat Program Age

| | Less than 1 year | 1 to 2 years | 2 to 3 years | 3 to 4 years | 5 years or more | Grand Total |
|---|---|---|---|---|---|---|
| Arena ITI | | | | | 1 | 1 |
| Code42 | | | | 1 | | 1 |
| Exabeam | | 1 | 1 | 1 | | 3 |
| Forcepoint FIT & FBA | | | | | 1 | 1 |
| Gurucul | | 2 | | | | 2 |
| Haystax | | | | 1 | | 1 |
| Homegrown tool | | | | | 1 | 1 |
| Microsoft Exchange | 1 | | | | | 1 |
| MS Office 365 Data Loss Prevention | 1 | | | | | 1 |
| ObserveIT | | 1 | | 1 | | 2 |
| ProofPoint Insider Threat Management (ITM) | | | | | 1 | 1 |
| Securonix | | | | | 3 | 3 |
| Splunk UBA | | | 1 | | | 1 |
| Symantec | | 1 | 2 | 1 | | 4 |
| **Grand Total** | **2** | **5** | **4** | **5** | **7** | **23** |

Insider Threat Tool Survey Results 2021

# 2021 Tool Reviews by Population Scope

# What is the population in scope for this insider threat tool?



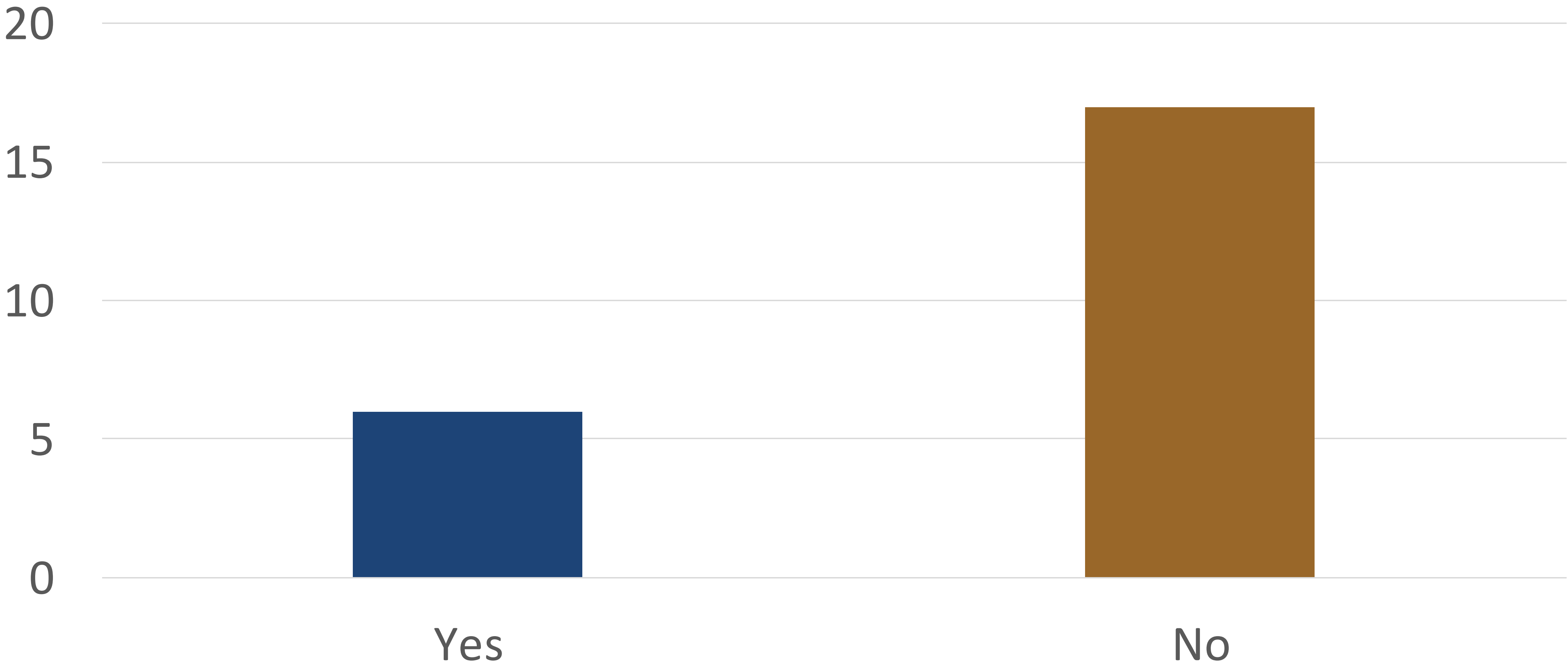
# Tools by Population Scope

| | Business unit specific (i.e., Finance) | Enterprise-wide | Other: use case specific | Role-based (i.e., System admins) | Grand Total |
|---|---|---|---|---|---|
| Arena ITI | | 1 | | | 1 |
| Code42 | | 1 | | | 1 |
| Exabeam | | 2 | 1 | | 3 |
| Forcepoint FIT & FBA | | 1 | | | 1 |
| Gurucul | | 2 | | | 2 |
| Haystax | | 1 | | | 1 |
| Homegrown tool | | 1 | | | 1 |
| Microsoft Exchange | | 1 | | | 1 |
| MS Office 365 Data Loss Prevention | | 1 | | | 1 |
| ObserveIT | | 1 | | 1 | 2 |
| ProofPoint Insider Threat Management (ITM) | | 1 | | | 1 |
| Securonix | | 3 | | | 3 |
| Splunk UBA | 1 | | | | 1 |
| Symantec | 1 | 2 | | 1 | 4 |
| **Grand Total** | **2** | **18** | **1** | **2** | **23** |

Insider Threat Tool Survey Results
2021

# 2021 Tools Reviewed in Previous Years

# Have you evaluated this tool before?



# If yes, how has your opinion of the tool changed since?

| Response | Number of Responses |
|---|---|
| No. | 3 |
| No it has not. | 1 |
| Previous survey was completed with an older version of the tool. | 1 |
| The tool improves with subsequent releases and the vendor uses customer feedback for enhancements. | 1 |

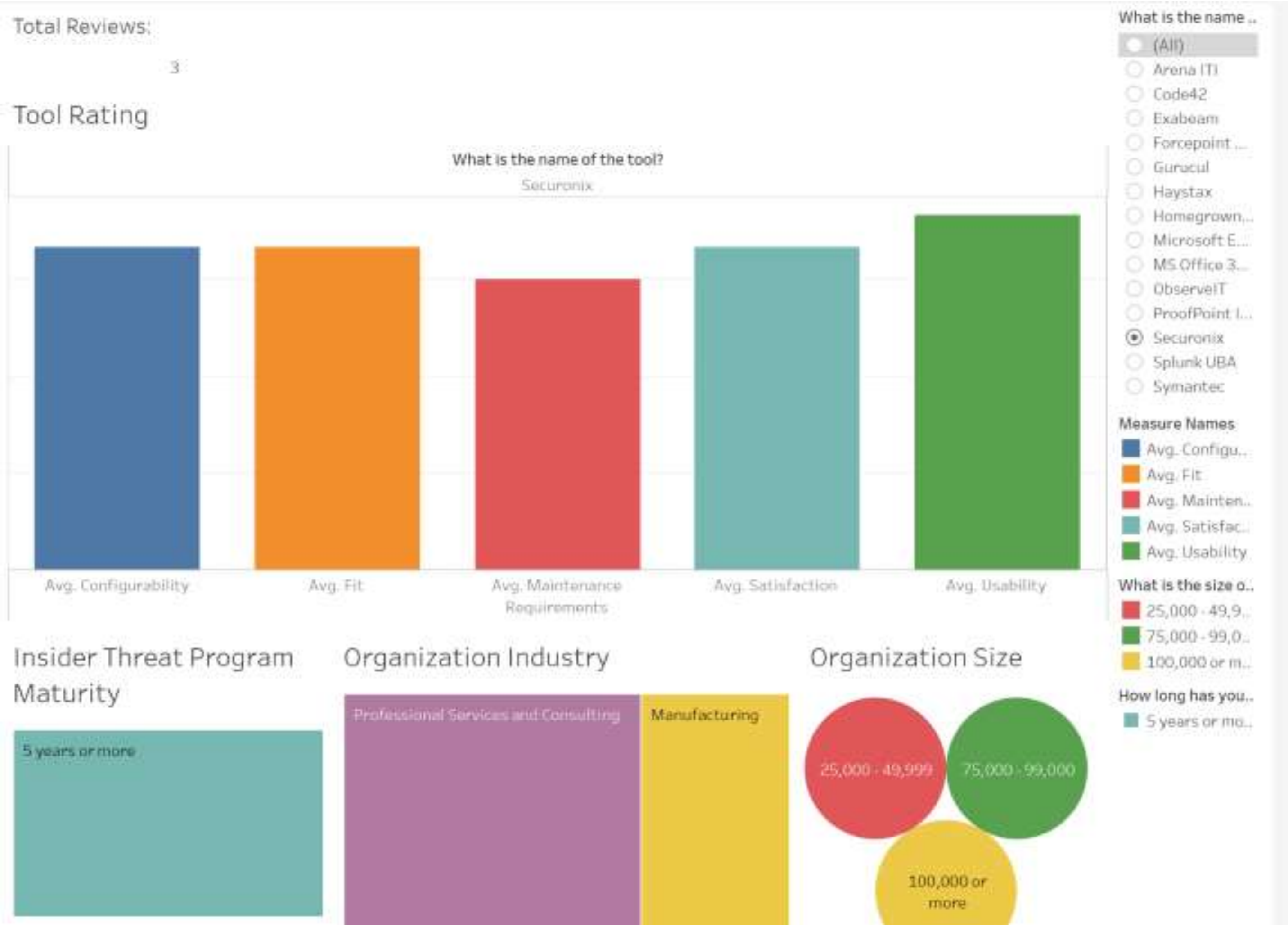
# Tools that have been reviewed in previous years.

| Tool Name | Number of Responses |
|---|---|
| Arena ITI | 1 |
| ProofPoint Insider Threat Management (ITM) | 1 |
| Securonix | 3 |
| Symantec | 1 |

Insider Threat Tool Survey Results
2021

# Summary by Tool and Category Type (Tableau Dashboards)

# Summary by Tool, Arena ITI



Total Reviews:

3

Tool Rating

What is the name of the tool?

Securonix

Insider Threat Program Maturity

Organization Industry

Organization Size

What is the name ..

- ○ (All)
- ○ Arena ITI
- ○ Code42
- ○ Exabeam
- ○ Forcepoint ...
- ○ Gurucul
- ○ Haystax
- ○ Homegrown,..
- ○ Microsoft E...
- ○ MS Office 3...
- ○ ObserveIT
- ○ ProofPoint I...
- ● Securonix
- ○ Splunk UBA
- ○ Symantec

Measure Names

- 🟦 Avg. Configu..
- 🟧 Avg. Fit
- 🟥 Avg. Mainten..
- 🟦 Avg. Satisfac..
- 🟩 Avg. Usability

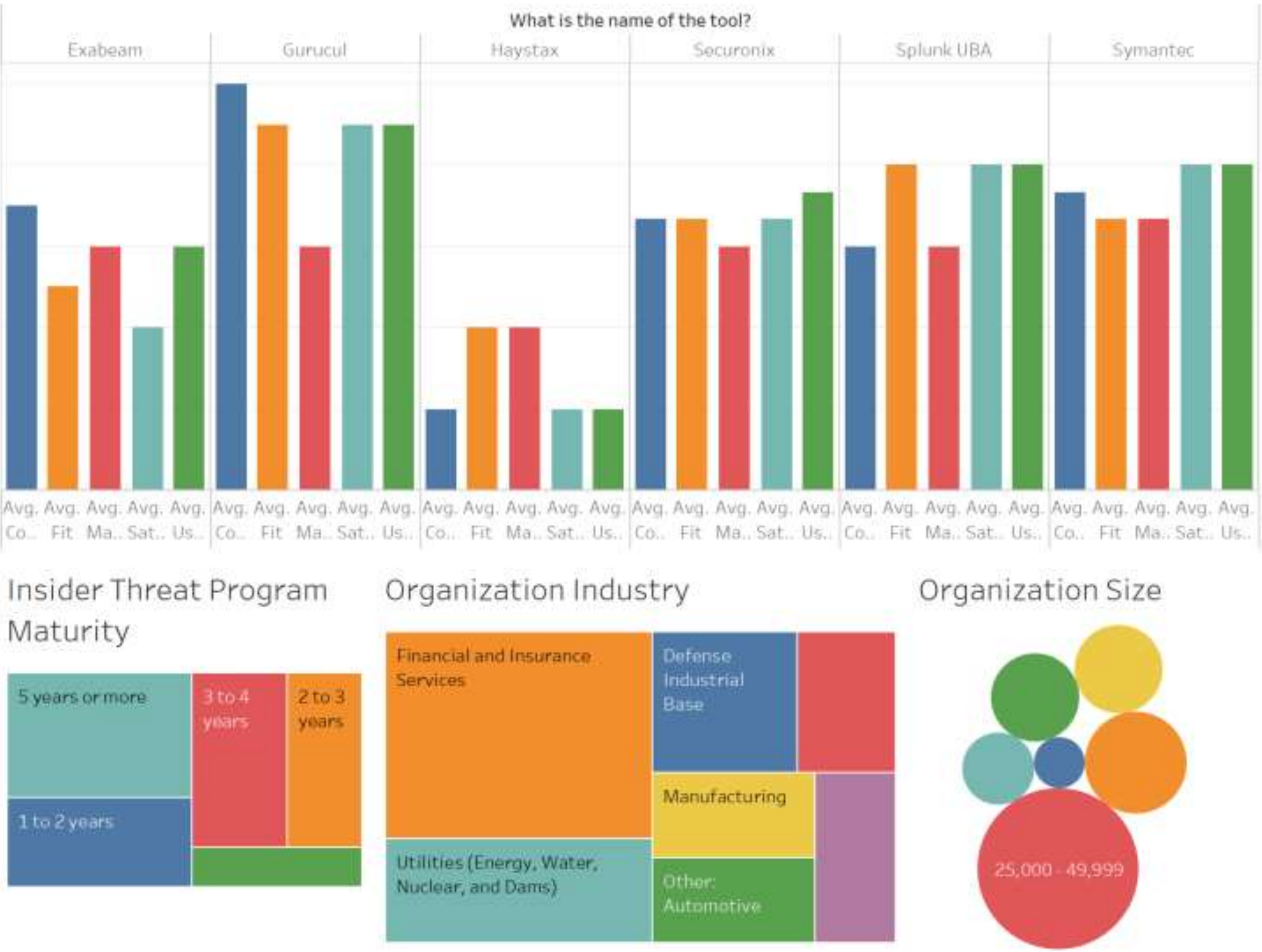
What is the size o..

- 🟥 25,000 - 49,9..
- 🟩 75,000 - 99,0..
- 🟨 100,000 or m..

How long has you..

- 🟦 5 years or mo..

# Summary by Category Type



Insider Threat Tool Survey Results 2021

# 2021 Comments

# Comments by Tool -1

**Arena ITI**

"Arena ITI is a proactive data analytics tool that **ingests technical and behavioral indicators** for risk scoring against user configured threat models."

**Exabeam**

"**Inability to set up role-based access for masking data/identity** makes this tool difficult to use in a holistic manner."

"Tech support tends to not be timely, so our team has taken on most of the parser development work."

**Microsoft Office 365 Data Loss Prevention**

"Understanding how other organizations have moved off Symantec DLP to MS O365 DLP successfully as well as the trials and tribulations they went through in order to achieve a mature state."

# Comments by Tool -2

**ObserveIT**

“Very useful tool for alerting on and capturing known risks.”

**Securonix**

“Good tool. **Sophisticated in capability but very complex.** Like driving a formula one car. Requires alot of time and commitment.”

# Comments by Tool -3

## Symantec - 1

“Features we like:

1.) Analyzer View (Analytics): The **ability to query multiple interconnected data sources on the fly using objects with drag-and-drop techniques for analysis**

2.) **Dashboarding: Prioritized view of custom queries** displayed on the homepage for daily monitoring

3.) Risk Modelling: **Pre-built scenarios work great with other Symantec tools – like DLP, SEP & Bluecoat** proxy which we fortunately have. We can also build **custom risk models** using a collection of other data sources in a kill chain sequence.

4.) Case Manager: We **classify** and mitigate **incidents**. **ML algorithms** help improve classification efforts over time.

5.) Data masking: Available, but not often used. We don’t share the application outside of our team but only when demonstrating to stakeholders.

ICA is has some downsides;

1.) **Batch processing takes a day (T+1) to complete**. The more data we feed it, the longer it takes. We have an on prem solution and we thinking to move processing to the cloud

2.) Interface: the interface is ok, not intuitive as others and there are a lot of screens to click through and sometimes the session breaks which is frustrating for the analysts. [Its a bug]

4.) ICA graphing is substandard. We export data into Power BI for stakeholder MI.

5.) There are other fiddly bits with the software and we have logged a few incidents in the past for patching. It’s an evolving product as most UBAs and the next version promises to be better than the last.”

# Comments by Tool -4

## Symantec - 2

“The tool is designed, like many others of it's kind, **to focus on data leakage prevention**, network activity and access. What it **struggles** to do is **to ingest** disparate **data** to provide an **holistic view** of a person. These data sets include **HR** information on misconduct, financial distress information, previous investigations etc. The moment one brings this in the tool becomes rather difficult to manage. Also I felt that the tool is much more **designed to fit** into a **SOC** as it is designed to work on alerts and actioning those events rather than providing just a holistic view of the person from an insider threat perspective.”

Insider Threat Tool Survey Results
2021

# 2021 Reviews for Tools with Known Versions

# Known Tool Versions - 1

| | |
|---|---|
| **Arena ITI** | 1 |
| 3.4 | 1 |
| **Exabeam** | 3 |
| 4.0.53 | 1 |
| I55.5 | 1 |
| SaaS platform | 1 |
| **Forcepoint FIT & FBA** | 1 |
| current | 1 |
| **Gurucul** | 1 |
| 8.0 R6 | 1 |
| **MS Office 365 Data Loss Prevention** | 1 |
| current | 1 |
| **ObserveIT** | 1 |
| 7.11.1.180 | 1 |

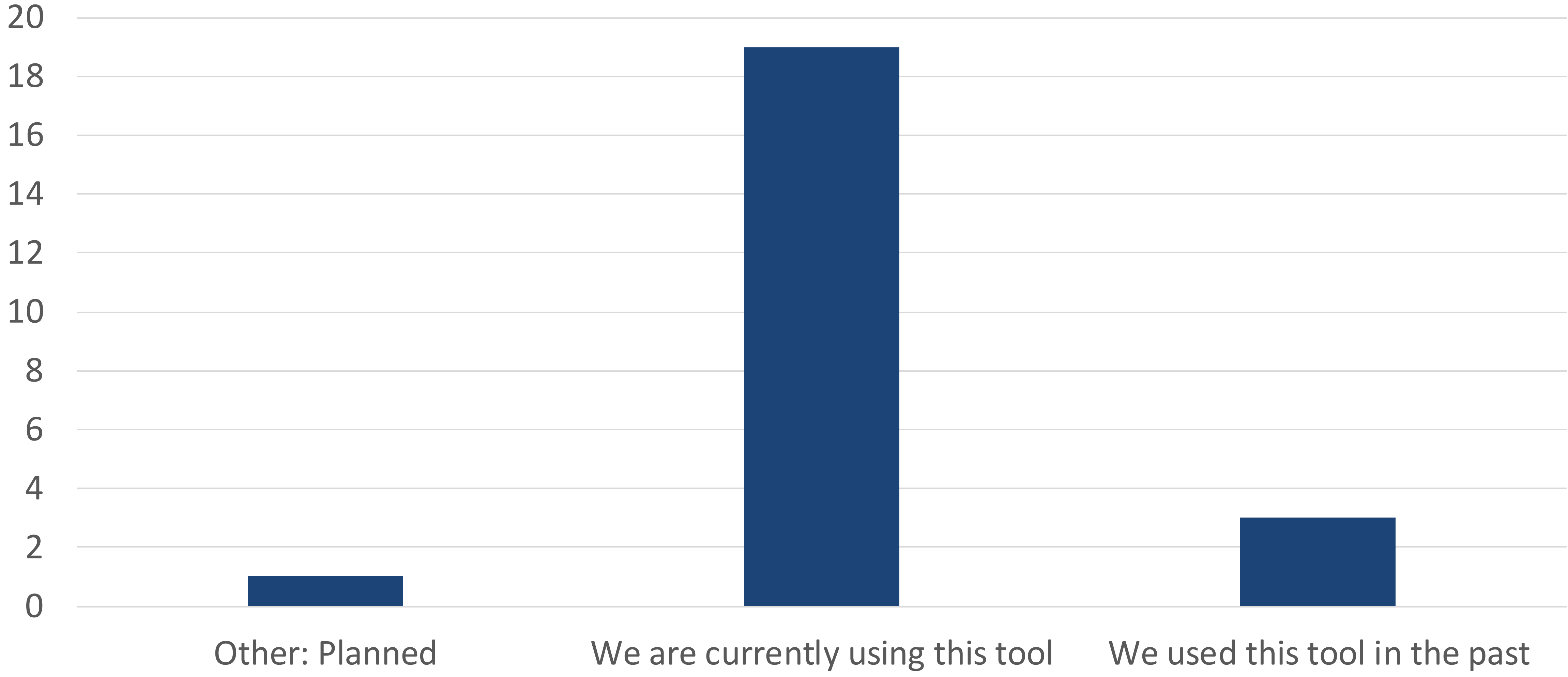
# Known Tool Versions - 2

| | |
|---|---|
| **ProofPoint Insider Threat Management (ITM)** | 1 |
| 7.11 | 1 |
| **Securonix** | 3 |
| 6 | 1 |
| 6.3 | 1 |
| Jupiter - V6.4 | 1 |
| **Splunk UBA** | 1 |
| 5.0.4.1 | 1 |
| **Symantec** | 2 |
| 6.5.4 | 2 |

Insider Threat Tool Survey Results
2021

# 2021 Tool Reviews by Organization Use

# When did your organization use this tool?



# Tools by Program’s Planned Usage, Past or Present

| | Other: Planned | We are currently using this tool | We used this tool in the past | Grand Total |
|---|---|---|---|---|
| Arena ITI | | 1 | | 1 |
| Code42 | | | 1 | 1 |
| Exabeam | | 3 | | 3 |
| Forcepoint FIT & FBA | | 1 | | 1 |
| Gurucul | | 2 | | 2 |
| Haystax | | | 1 | 1 |
| Homegrown tool | | 1 | | 1 |
| Microsoft Exchange | | 1 | | 1 |
| MS Office 365 Data Loss Prevention | 1 | | | 1 |
| ObserveIT | | 2 | | 2 |
| ProofPoint Insider Threat Management (ITM) | | 1 | | 1 |
| Securonix | | 2 | 1 | 3 |
| Splunk UBA | | 1 | | 1 |
| Symantec | | 4 | | 4 |
| **Grand Total** | **1** | **19** | **3** | **23** |

Insider Threat Tool Survey Results
2018 - 2021

# Additional Information

# Contact Information

Sonia Reed

Email: sreed@cert.org

Carrie Gardner

Email: cgardner@cert.org

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890

**Open Source Insider Threat Information Sharing Group (OSIT)**

Email: osit-forum-support@cert.org

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.