VulnSentry: Crowdstrike Vulnerability Management

Presentation by:
Christian Somoya

https://github.com/Csomoya/sql-project

Who:

- Our customers and the cyber products they use.

What:

- Vulnerability Management. Helping customers stay informed about staying up to date with the latest advisories.

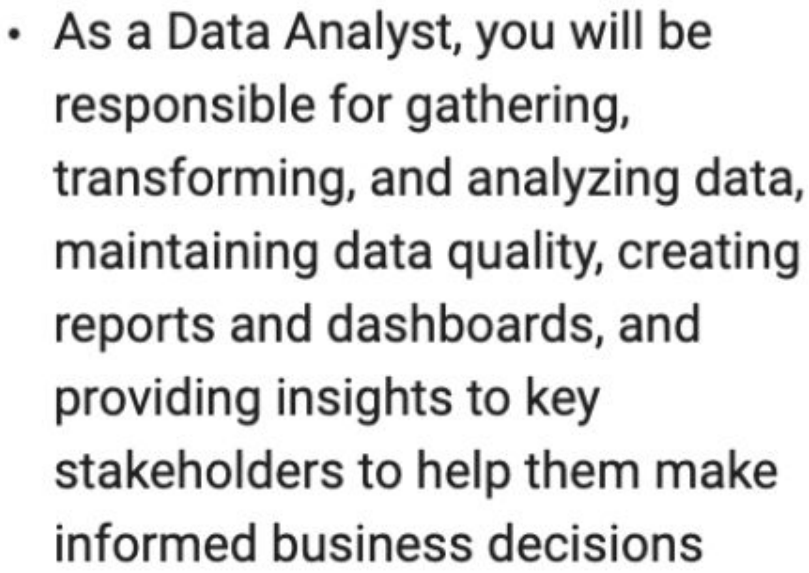
How:

- Comprehensive Analytics designed to inform and alert customers about vulnerabilities and past threats.

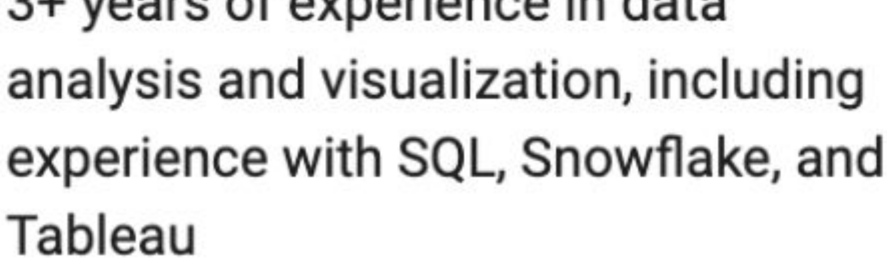
Job Description

CROWDSTRIKE

Data Analyst (REMOTE)

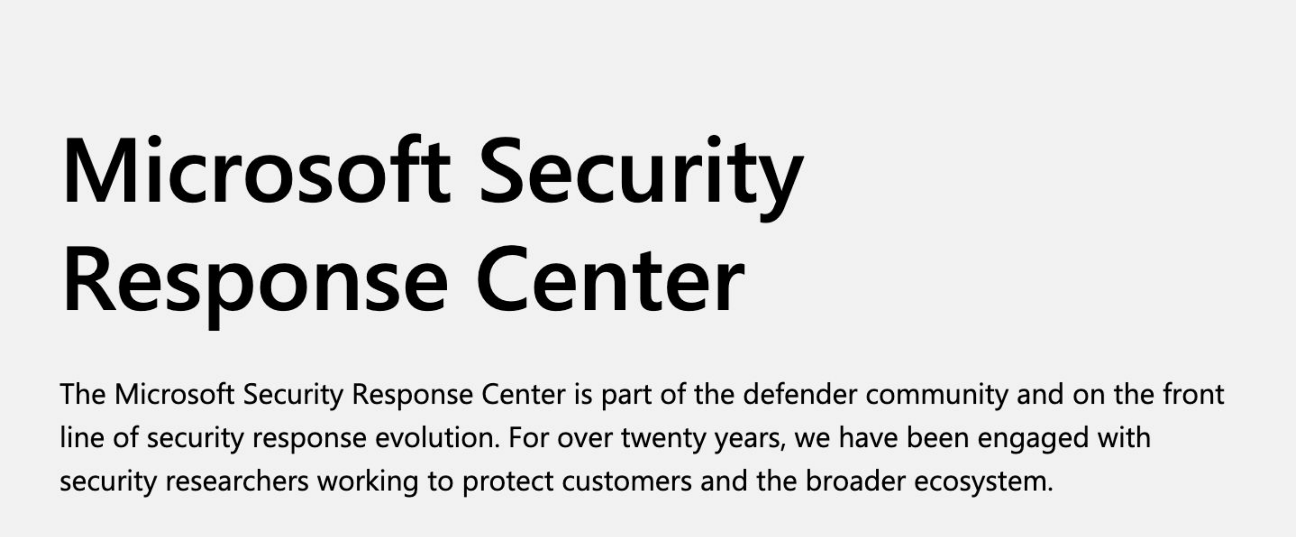


- As a Data Analyst, you will be responsible for gathering, transforming, and analyzing data, maintaining data quality, creating reports and dashboards, and providing insights to key stakeholders to help them make informed business decisions



3+ years of experience in data analysis and visualization, including experience with SQL, Snowflake, and Tableau

API DATA SOURCE



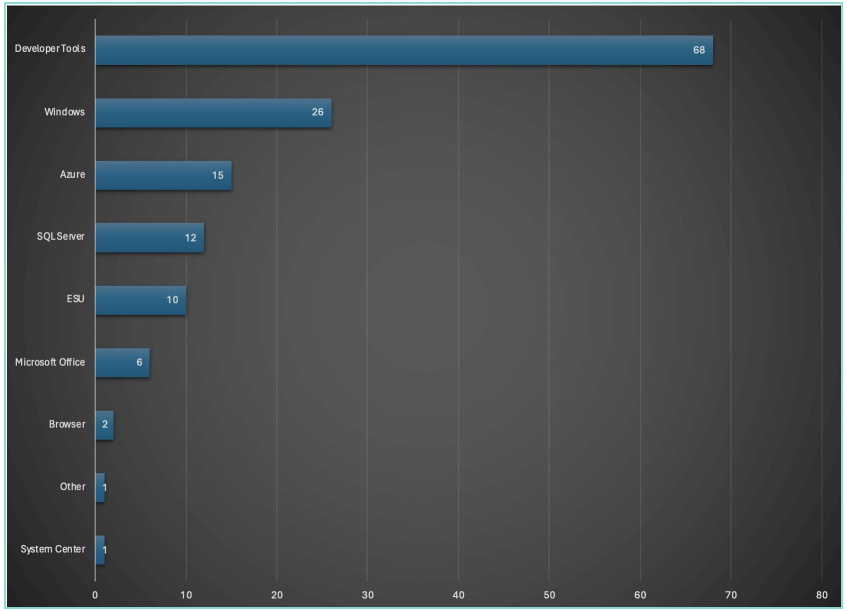
Microsoft Security Response Center

The Microsoft Security Response Center is part of the defender community and on the front line of security response evolution. For over twenty years, we have been engaged with security researchers working to protect customers and the broader ecosystem.

https://msrc.microsoft.com/update-guide

Which Microsoft products should our customers be most aware of?

- Advisories for Developer Tools takes the far lead.
- Raise awareness levels for new Dev patches. Recommend alerts when new versions are released.
- Lower likelihood of compromise through Dev Tools.

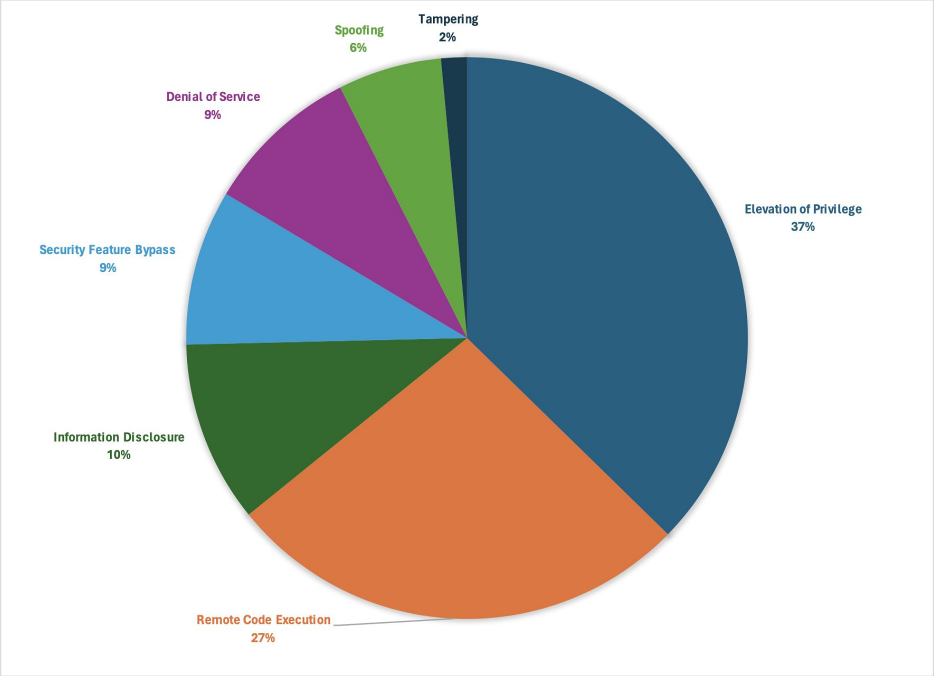


What is the threat landscape for Microsoft products?

- Privilege Escalation is over ⅓ of the chart.

- Recommend stricter IAM policies and least privilege principle.

- Proportion of privilege escalation threats will go down



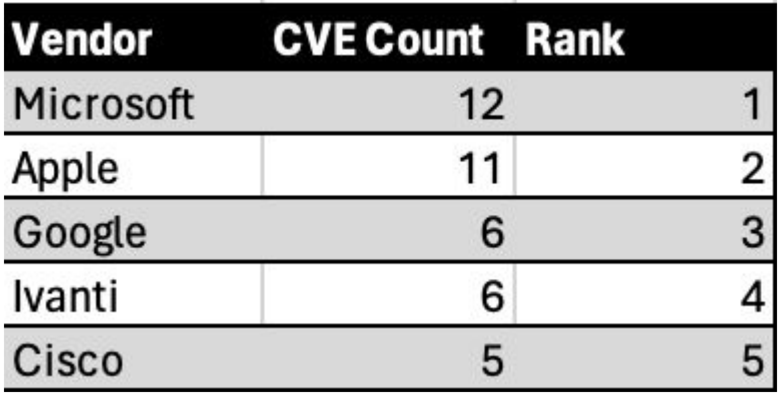
Web Scrape Data Source

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

What vendors have the most reported vulnerabilities?

- Ivanti CVE’s not proportional to market share.
- Recommend customers proceed with Ivanti cautiously.
- Ivanti will take security controls more seriously so customers stay safe.



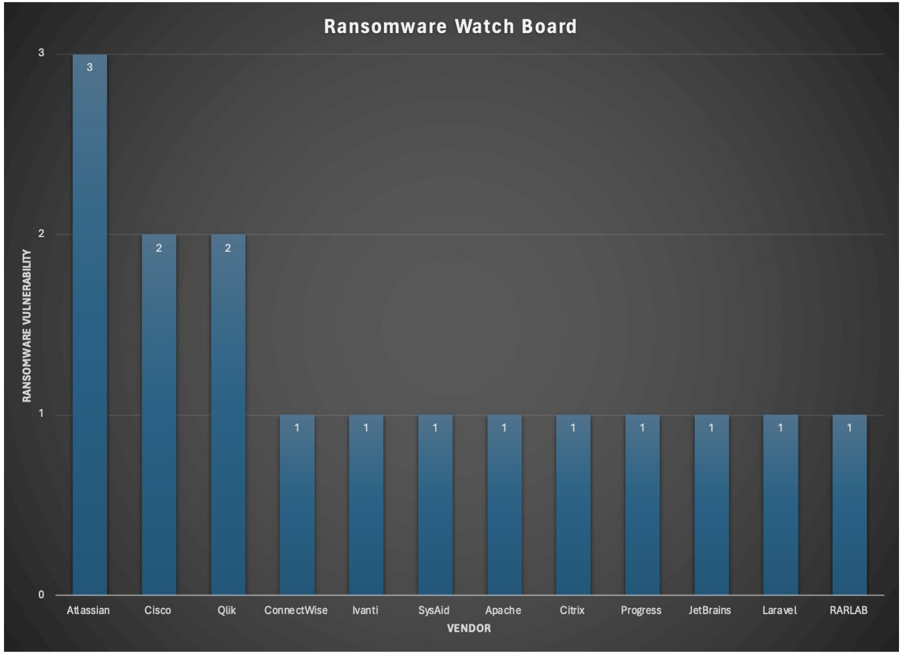
Vendor	CVE Count	Rank
Microsoft	12	1
Apple	11	2
Google	6	3
Ivanti	6	4
Cisco	5	5

Which vendors have had the most vulnerabilities involving ransomware?

- Atlassian has the most, Being on this list is already enough

- Put vendors on a seperate advisory list. Create alerts for said list for new patches.

- Companies on watch list will meet security objectives in order to get off.



The cyber landscape is ever-changing, our customers need an informed and actionable approach to prepare for tomorrow's challenges.