

# Day 54

## Exploitation Analyst

### Patch/Update Deployment Analysis:

AI can greatly improve Patch/Update Deployment Analysis by automating risk assessment and decision-making. It can:

- Prioritize patches by analyzing severity, exploitability, and system criticality.
- Predict impact on performance, downtime, and compatibility using past deployment data.
- Recommend scheduling by learning normal system usage to minimize disruption.
- Detect anomalies after patching (e.g., unusual logs, failed services).
- Simulate outcomes in test environments using digital twins before applying to live systems.

Steps:

Visit the Microsoft update catalog:

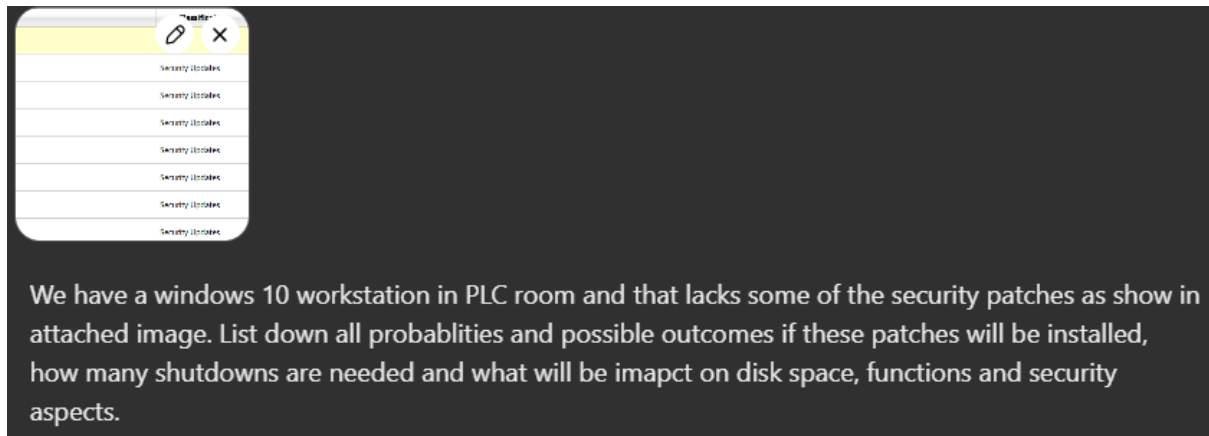


Search for any services, say SQL:

The screenshot shows the search results for "SQL" in the Microsoft Update Catalog. The results are displayed in a table with columns: Title, Products, Classification, Last Updated, Version, Size, and Download. The table lists 15 updates for various Microsoft SQL Server versions, including RTM Cumulative Updates, Security Updates, and Service Packs. Each update has a "Download" button next to it. The table is paginated, showing updates 1 to 25 of 534. Navigation links for "Previous" and "Next" are visible at the top right of the table.

Title	Products	Classification	Last Updated	Version	Size	Download
<a href="#">SQL Server 2022 RTM Cumulative Update (CU) 21 (KB5065865)</a>	Microsoft SQL Server 2022	Updates	9/11/2025	n/a	462.6 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2017 RTM GDR (KB5065224)</a>	Microsoft SQL Server 2017	Security Updates	9/9/2025	n/a	452.1 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2016 Service Pack 3 GDR (KB5065226)</a>	Microsoft SQL Server 2016	Security Updates	9/9/2025	n/a	510.8 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2017 RTM CU (KB5065225)</a>	Microsoft SQL Server 2017	Security Updates	9/9/2025	n/a	542.9 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2022 RTM CU (KB5065220)</a>	Microsoft SQL Server 2022	Security Updates	9/9/2025	n/a	462.5 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2022 RTM GDR (KB5065221)</a>	Microsoft SQL Server 2022	Security Updates	9/9/2025	n/a	340.7 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2016 Service Pack 3 GDR (KB5065227)</a>	Microsoft SQL Server 2016	Security Updates	9/9/2025	n/a	507.8 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2019 RTM GDR (KB5065223)</a>	Microsoft SQL Server 2019	Security Updates	9/9/2025	n/a	507.9 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2019 RTM CU (KB5065222)</a>	Microsoft SQL Server 2019	Security Updates	9/9/2025	n/a	888.7 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2019 RTM GDR (KB5063758)</a>	Microsoft SQL Server 2019	Security Updates	8/12/2025	n/a	506.5 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2016 Service Pack 3 GDR (KB5063762)</a>	Microsoft SQL Server 2016	Security Updates	8/12/2025	n/a	485.4 MB	<a href="#">Download</a>
<a href="#">Security Update for SQL Server 2016 Service Pack 3 CU (KB5063761)</a>	Microsoft SQL Server 2016	Security Updates	8/12/2025	n/a	482.5 MB	<a href="#">Download</a>

Take snap of a part of it and paste in the ChatGPT with prompt:



Prompt:

*We have a windows 10 workstation in PLC room and that lacks some of the security patches as show in attached image. List down all probablities and possible outcomes if these patches will be installed, how many shutdowns are needed and what will be imapct on disk space, functions and security aspects.*

Output:

I'll break this down for you in a structured way. The screenshot you shared shows pending **SQL Server security updates and cumulative updates**. Since this is a **Windows 10 workstation in a PLC (industrial control) room**, every change has to be carefully considered for availability, security, and disk impact.

---

### 1. Probabilities and possible outcomes of installing patches

**Positive outcomes (likely):**

- **Security hardening:**
  - Vulnerabilities in SQL Server (2016, 2017, 2019, 2022) will be closed.
  - Prevents exploits such as remote code execution (RCE) or privilege escalation.
  - Reduces the attack surface in a critical ICS environment.
- **Bug fixes and stability improvements:**
  - Cumulative updates often fix memory leaks, deadlocks, query processing issues, and driver bugs.
  - Better compatibility with modern Windows 10 components.

**Neutral / manageable outcomes:**

- **Disk space usage:**
  - Each patch is ~340 MB – 543 MB. Installing all may consume around 3–4 GB total after extraction + installation + backup of replaced files.
  - Windows keeps uninstall backups in `Windows\Downloaded` some space remains occupied until cleanup.
- **Performance impact:**

--The End--