Secure your Estate:
Understand & Mitigate Patching Risks

Starting Soon

Housekeeping

Speakers

Brian See| Director Cyber Defense

Jonathan Trayers | Director MSS

Slides & Recording

Slide deck and recording will be shared with everyone after this session

Polls & Questions

We'd love your input in our polls and encourage questions throughout the webinar. Keep an eye on the chat box and type your questions in there

Ekco is one of Europe's leading security-first cloud providers.

What makes us different

We're the **proactive specialists** that help you **push boundaries**, who feel like part of your team, that **transform your security** for good.

We've built **close, transformative partnerships** with hundreds of customers across Europe, through friendly, personalised support and hands-on management.

We act as an extension of your team; we **believe in transparency and collaboration** to jointly achieve objectives.

800+
Customers

860+
Employees

300+
Security Employees

HQ – Ireland
- Dublin
- Waterford
- Kildare
- Cork

UK
- London
- Milton Keynes
- Reading
- Birmingham
- Bournemouth

Netherlands
- Alkmaar
- Rotterdam
- Groningen
- Veenendaal

New Locations
- Malaysia
- Slovakia
- Spain
- Boston
- Cape Town

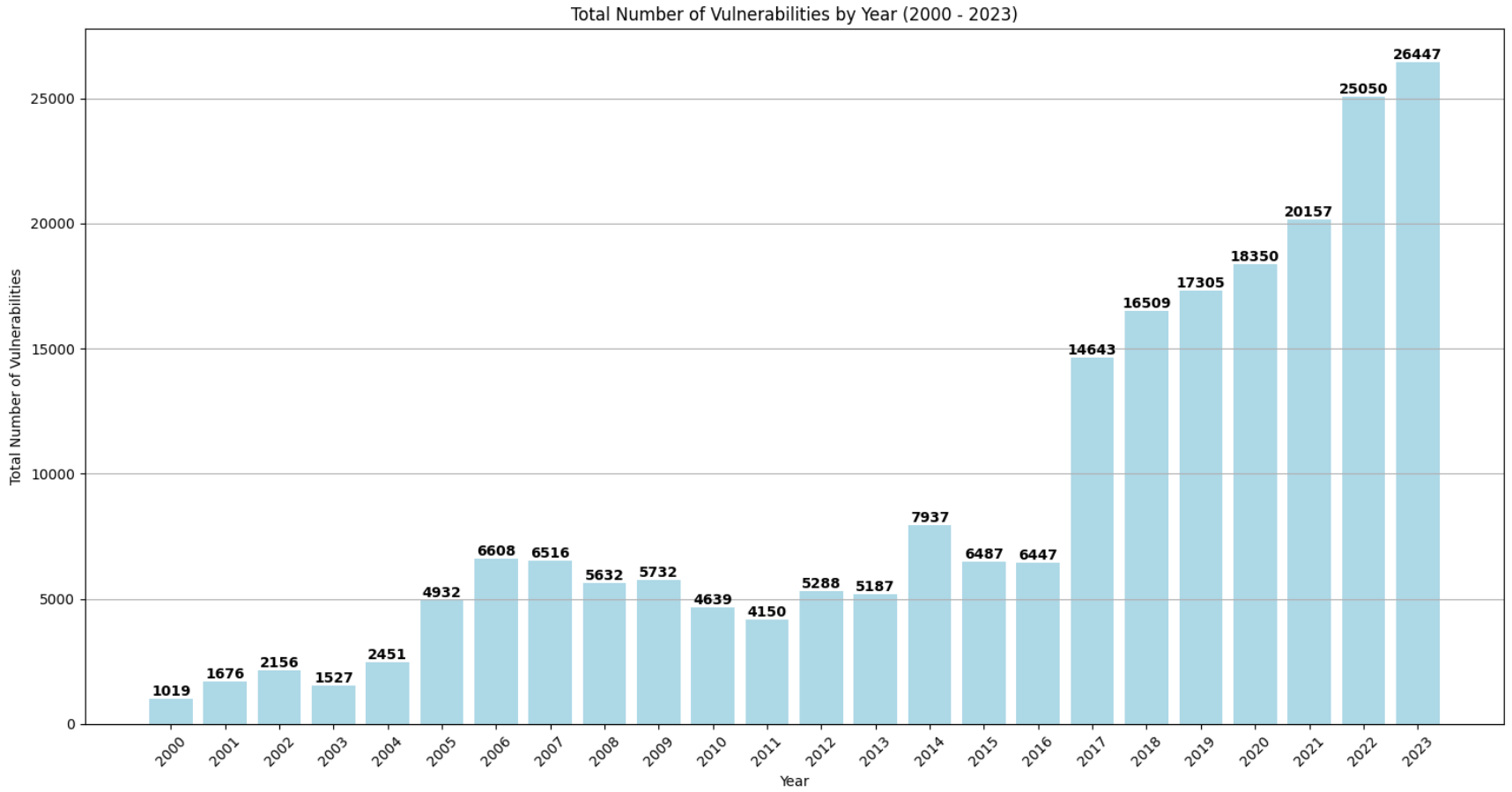
How big is the Challenge

26,447

Number of CVEs published in 2023

97

97 high-risk vulnerabilities



The scale of the Vulnerabilities today

Vulnerabilities by Impact Types

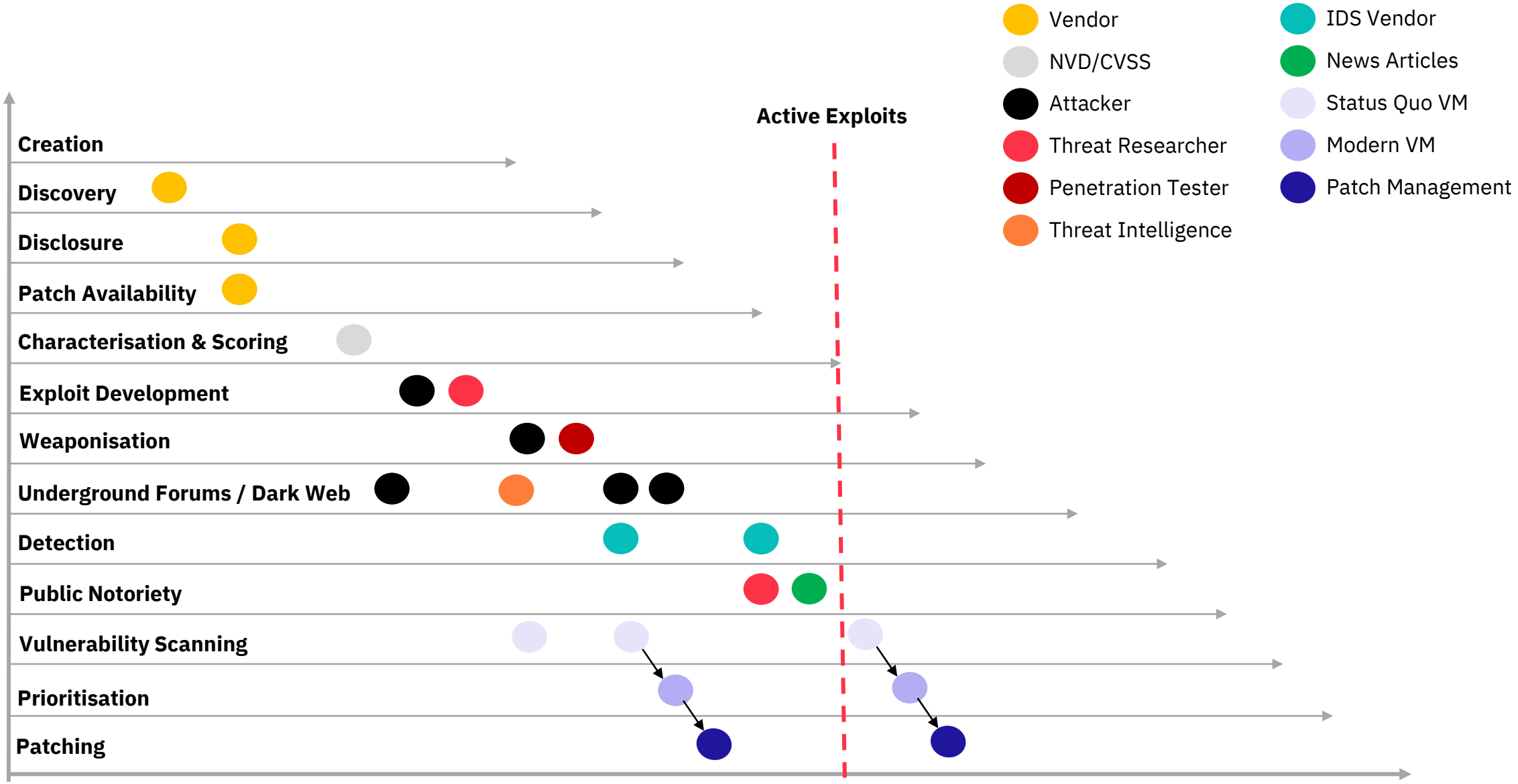
Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	1041	165	186	1597	356
2015	1430	177	255	1793	602
2016	1239	469	608	2050	704
2017	1870	857	1027	3372	1394
2018	1728	666	850	2207	1418
2019	1534	670	916	1699	1326
2020	1691	817	1387	1677	1094
2021	2087	806	1121	2297	926
2022	2067	944	1527	2437	1145
2023	2581	1059	1525	2559	1545
2024	527	262	294	535	245
Total	17795	6892	9696	22223	10755

Top Vendors Most Vulnerabilities
Last 10 Years

TOP VENDORS MOST VULNERABILITIES	TOTAL
Microsoft	11,350
Google	11,036
Oracle	9,422
IBM	6,958
Cisco	6,066
Apple	5,344
Redhat	5,326
Adobe	5,340

Source: CVEDETAILS.COM

Lifecycle of Vulnerability Exploitation



Threat & Vulnerability Management Model

Increased Risk *(Low Maturity)*

Decreased Risk *(High Maturity)*

NON-EXISTENT	SCANNING	ANALYSIS & PRIORITISATION	ASSESSMENT & COMPLIANCE	ATTACK MANAGEMENT	BUSINESS RISK MANAGEMENT
No Vulnerability Scanning	Vulnerability assessment solution in place	Driven by Regulatory Framework	Risk assessed	Attacker and threat focused	Threat and risk aligned with business goals
Manual Vulnerability Assessments	Ad-hoc vulnerability scanning	Scheduled vulnerability scanning	Scan data prioritised	Multiple threat-vectors scanned and prioritised	All threat vectors scanned and prioritised
Adhoc Patching	**Rudimentary patching**	**Scan to Patch lifecycle**	**Patching, data driven by priority**	**Patching based on risk to critical assets**	**Continuous patching**
No Process Exists	Basic process	Emerging Processes	Measurable processes	Efficient, metrics-based processes	Unified business and IT processes
No Metrics	Basic metrics	Little measurable metrics	Emerging metrics and trends	Threat-driven metrics and trends	Measurement integrated to entries risk management

Early Maturity

PEAK DATA OVERLOAD

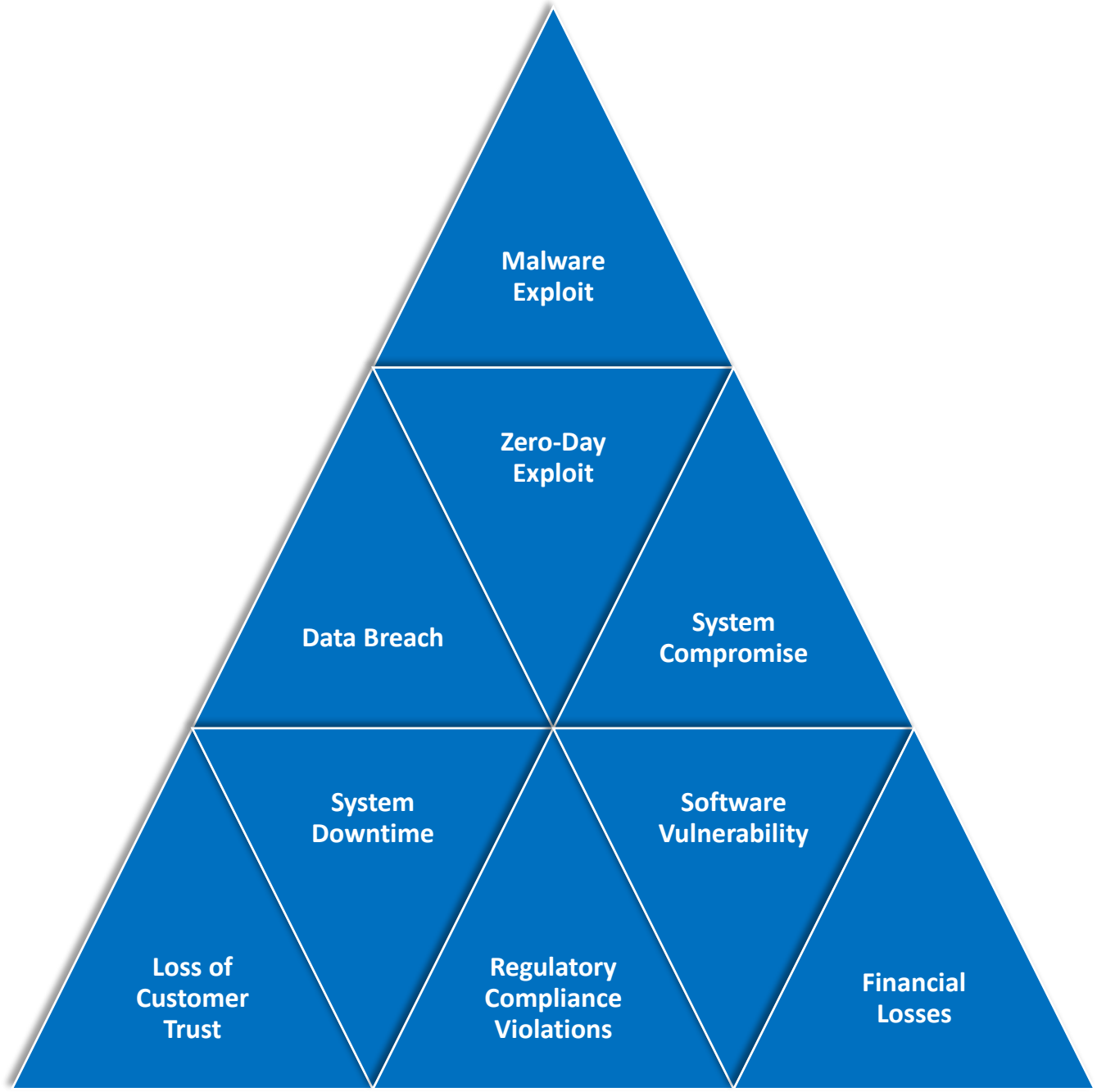
Data Driven

EFFECTIVE PRIORITISATION

Business Risk & Context

Common issues addressed by security patch management

- Patch management is essential for addressing known vulnerabilities in software and operating systems.
- Failure to patch leaves systems exposed to exploitation by cyber attackers, leading to data breaches, financial losses, and reputational damage.
- Proactive patch management reduces the window of opportunity for attackers and enhances overall security posture



Breakdown of Patch Types

Hardware	
Firewall	1
Router	1
Network Switch	2
Intrusion System / IPS	2
Web Gateway Proxy	2
Email Gateway Appl.	2
Network Access Control	2
Printers	4
IP Phones	4
Mobile Device / Phones	3
Internet of Things / IoT	3
Operational Technology / OT	3

Operating System	
Windows	1
MacOS	2
Linux	2
Android	3
Apple iOS	3
OS for IoT and OT	3

Software	
Office Suites	1
Database	1
Email & Web Server	1
Third-party Software	2
Bespoke Software	2
Utilities and Tools	2

Server & Computer	
Desktops	3
Laptops	3
Servers	3

Realistic Expectations

1. **Perfection is unrealistic (zero vulnerabilities)** - Will the banks ever eliminate credit card fraud?
2. **Near all organisations have limited resources to address issues**
3. **Factor in the business impact costs + remediation costs**
   - If the risk outweighs the cost – eliminate or mitigate the vulnerability.
4. **Apply the Pareto Principle – the 80/20 Rule**
   - Focus on the vital few not the trivial many.
   - 80% of your risk can be eliminated by addressing 20% of the issues.
5. **Patch or Mitigate**
   - Impact on availability from a bad patch vs the risk of not patching.
   - Recommendations: Determine how wide-spread of the problems / Implement defence in depth.

Effective Patch Management Practices

1 #

Regular Assessment

- Conduct regular assessments to identify vulnerabilities in software and systems.
- Utilize vulnerability scanning tools to detect weaknesses and prioritize patches based on severity.

2 #

Patch Prioritisation

- Prioritize patches based on severity, potential impact, and relevance to your organization's infrastructure.
- Develop a risk-based approach to prioritize critical patches that address high-impact vulnerabilities.

3 #

Testing Procedures

- Implement a robust testing process to evaluate patches before deployment.
- Test patches in a controlled environment to ensure compatibility and prevent unintended system disruptions.

4 #

Scheduled Patching Cycles

- Establish scheduled patching cycles to ensure timely deployment of updates.
- Balance the need for quick patch deployment with the requirement for thorough testing to minimize downtime and risks.

5 #

Automated Patch Management Tools

- Leverage automated patch management tools to streamline the patching process.
- Automate patch deployment, monitoring, and reporting to enhance efficiency and consistency.

6 #

Change Management Integration

- Integrate patch management with change management processes to maintain transparency and accountability.
- Document patching activities and ensure alignment with organizational policies and compliance requirements.

7 #

Continuous Monitoring and Feedback

- Implement continuous monitoring mechanisms to track patch effectiveness and system health.
- Solicit feedback from stakeholders and end-users to identify any issues or improvements in the patch management process.

Patch management schedule

Structured approach to ensure that patches are - Identified, Prioritised, Tested, Deployed and Monitored is systematic manner

Monthly - Patch Management Plan

Week-1	
Date	**Task & Description**
Monday	**Vulnerability Assessment** ▪ Conduct a comprehensive scan of systems and software to identify vulnerabilities
Week-2	
Date	**Task & Description**
Monday	**Patch Identification** ▪ Review the results of the vulnerability assessment and identify required patches.
Tuesday	**Patch Prioritisation** ▪ Prioritize patches based on severity, impact, and criticality to the organization
Wednesday	**Testing** ▪ Test patches in a controlled environment to ensure compatibility and stability
Thursday	**Change Management** ▪ Integrate patch deployment plans with change management processes for approval
Week-3	
Date	**Task & Description**
Monday	**Patch Deployment** ▪ Deploy approved patches to production systems during scheduled maintenance windows.
Tuesday	**Verification** ▪ Verify successful patch deployment and monitor systems for any issues or anomalies
Wednesday	**Reporting & Documentation** ▪ Generate reports detailing patch deployment status, including any issues encountered.
Week-4	
Date	**Task & Description**
Monday	**Review & Adjust** ▪ Conduct a review of the patch management process and make adjustments as necessary.
Monthly	
Date	**Task & Description**
Monthly	**Ongoing Monitoring**

Critical Severity Patch Response

Date	Task & Description
Day 1	**Vulnerability Identification** ▪ Receive notification or advisory regarding the critical vulnerability.
Day 2	**Risk Assessment** ▪ Assess the potential impact of the vulnerability on the organization's systems and data.
Day 3	**Patch Identification** ▪ Research and identify available patches or mitigations for the vulnerability.
Day 4	**Patch Testing** ▪ Test patches in a controlled environment to ensure compatibility and stability.
Day 5	**Change Management** ▪ Integrate patch deployment plans with change management processes for approval
Day 6	**Patch Deployment** ▪ Deploy approved patches to production systems during scheduled maintenance windows
Day 7	**Verification** ▪ Verify successful patch deployment and monitor systems for any issues or anomalies.
Day 8	**Reporting and Documentation** ▪ Generate reports detailing patch deployment status, including any issues encountered
Day 9	**Post-Deployment Monitoring** ▪ Continuously monitor systems for new vulnerabilities or signs of exploitation
Day 10	**Review and Adjust** ▪ Conduct a review of the patch management process and make adjustments as necessary

Ekco patch management solution comparison matrix

	Patch Management Solutions		
Feature	**Microsoft Intune**	**Qualys**	**Ivanti**
Supported Platforms	Windows, MacOS, Android, iOS	Windows, Linux, MacOS, Unix	Windows, Linux, MacOS
Operating System Support	Yes	Yes	Yes
Third-Party Application Updates	Limited Support	Extensive Support	Extensive Support
Security Updates	Yes	Yes	Yes
Non-Security Updates	Limited Support	Yes	Yes
Feature Updates	Yes	No	Yes
Patch Rollback	Limited Support	Yes	Yes
Custom Patch Creation	No	Limited Support	Yes
Patch Compliance Reporting	Limited Reporting	Comprehensive Reporting	Comprehensive Reporting
Automated Patch Deployment	Yes	Yes	Yes
Cloud-Based Patch Management	Yes	Yes	Yes
Risk Assessment	No	Limited Support	Yes
Policy Deployment and Enforcement	No	No	Yes
Deployment Method	Cloud-based	Cloud-based	On-Premise and Cloud-based

Patch Management Service by Ekco

	Patch Management Service	
Service Feature	**Essential**	**Premium**
Vulnerability Assessment, Patch Prioritisation and Deployment	✓	✓
Testing and Validation	✓	✓
Patching Policy & Enforcement	✓	✓
Compliance Reporting	✓	✓
Risk Assessment	✓	✓
Cloud-Based Patch Management	✓	✓
Patch Rollback via Rapid Restoration		✓
Advanced risk assessment – threat modelling, risk scoring, and mitigation strategies		✓
24/7 Monitoring and Support		✓
Advanced vulnerability scanning		✓
Centralised management and real-time visibility		✓
Enhanced SLA and Priority Support		✓

Contact us to learn more

Cyber Security Patch Management Service