Designing a Ransomware Resilience Strategy in Azure & Microsoft 365

“Mitigation starts with preparation, not reaction.”

Microsoft CERTIFIED EXPERT

#MicrosoftSecurity #SC100 #DefenderXDR #AzureBackup #ZeroTrust #PerparimLabs

What Is Ransomware?

- Encrypts files and holds data hostage for money
- Spreads via email, web, USB, chat apps (Trojan-style)
- WannaCry, Petya, etc. = major global attacks

🧠 *Victim behavior + admin mistakes = root cause*

Why It Succeeds

⚠️ Common vulnerabilities:

- Local admin rights to end users
- Lack of employee training
- No backup/restore plan
- Delayed threat detection

PerparimLabs

#MicrosoftSecurity #SC100 #DefenderXDR #AzureBackup
#ZeroTrust #PerparimLabs

Step 1 – Control Privileged Access

✅ Implement **Least Privilege**
✅ Use **PIM** (Privileged Identity Management)
✅ Disable local admin rights by default
✅ Monitor role assignments in Azure & M365

🧠 “If they can't install it, it can’t encrypt.”

#MicrosoftSecurity #SC100 #DefenderXDR #AzureBackup #ZeroTrust #PerparimLabs

PerparimLabs

Step 2 – Daily Backup & Restore

🔄 Backup = Best Insurance
Real-world scenario:

- Client hit with ransomware
- All files encrypted on shared server
- Daily backup saved the day → restore to previous version

💾 Use Azure Backup + Backup Vault
💡 Optional: Site-to-site backup for hybrid recovery

#MicrosoftSecurity #SC100 #DefenderXDR #AzureBackup #ZeroTrust #PerparimLabs

PerparimLabs

Step 3 – Mitigation Strategy

Adopt a **Cybersecurity Framework**

✅ Implement Microsoft Defender for Cloud

✅ Prioritize risk mitigation (not just detection)

✅ Enable Microsoft Defender XDR (extended detection and response)

#MicrosoftSecurity #SC100 #DefenderXDR #AzureBackup #ZeroTrust #PerparimLabs

PerparimLabs

Step 4 – Monitor Across Cloud & Devices

Tools that stop ransomware before it spreads:

- **Defender for Cloud** → Azure VMs + Hybrid Infra
- **Defender XDR** → Files, emails, apps, identities
- **Sentinel (SIEM/SOAR)** → Unified incident correlation + response

🎯 Each layer = visibility + control

#MicrosoftSecurity #SC100 #DefenderXDR #AzureBackup #ZeroTrust #PerparimLabs

PerparimLabs

Real-World Case Study

🎨 Graphics Company: All server files encrypted

✅ Daily backups restored full environment

❌ No Defender/privileged access → initial infection still unknown

📘 Lesson: Backup alone ≠ prevention — use layered defense

#MicrosoftSecurity #SC100 #DefenderXDR #AzureBackup #ZeroTrust #PerparimLabs

PerparimLabs

CTA – Let's Talk Resilience

PerparimLabs

💬 What's your organization's ransomware mitigation plan?
👇 Would love to hear your backup + privileged access strategies.

#MicrosoftSecurity #SC100 #DefenderXDR #AzureBackup
#ZeroTrust #PerparimLabs

Tool Summary

Capability	Microsoft Solution
Privileged Access Control	Microsoft Entra PIM
Backup & Restore	Azure Backup, Backup Vault
Ransomware Detection	Microsoft Defender XDR
VM Monitoring	Defender for Cloud
SIEM/SOAR	Microsoft Sentinel

PerparimLabs

#MicrosoftSecurity #SC100 #DefenderXDR #AzureBackup
#ZeroTrust #PerparimLabs