🚨 The Problem

Right now, we don’t have centralized visibility into what’s happening in our environment.
That means if an account is compromised or a malicious actor is inside the network, we might not know until it's too late.

💼 The Risk

- Prolonged downtime due to slow detection and response
- Reputational damage from breaches or ransomware
- Legal and compliance issues due to missing audit trails
- High recovery costs after an incident

✅ The Solution

A SOC and SIEM solution helps us:

- Detect threats in real time
- Investigate incidents quickly and accurately
- Proactively defend our environment
- Build a defensible security posture with auditable logs

📈 The ROI

The cost of a breach (downtime, lost data, legal, reputation) vastly outweighs the cost of a SOC/SIEM.
Investing now is significantly cheaper than cleaning up later.

🧩 What I Propose

Let’s start with a manageable SOC/SIEM solution—possibly through a managed service (MSSP/MDR).
It scales with us, requires minimal internal overhead, and gives us the visibility and control we’re missing.

💡 Bonus: We Might Already Have It

Depending on our Microsoft 365 licensing, we might already have access to core capabilities:

- **Microsoft 365 Business Premium** includes Defender for Business—offering endpoint detection, reporting, and alerting features.
- **Microsoft 365 E5 or E5 Security** includes Defender XDR and Microsoft Sentinel—full-blown XDR and SIEM/SOAR platforms.
- These tools can tap into the logs we’re already generating—and turn them into security intelligence.

Before we spend more, let’s make sure we’re using what we’ve already paid for.

📌 Bottom Line

Without a SIEM, we’re flying blind.
With it, we gain real-time detection, forensic capability, and peace of mind.