Cybersecurity Program Building Blocks

We Design XDR programs for MSPs and Direct Customers

1. Identity Management + Conditional Access:

Why First? This is the foundation. You must know *who* has access to *what* . Conditional access builds upon this by enforcing rules based on context (location, device, time, etc.). If you don't control identities and access, all other security measures are weakened.

Think of it as securing the front gate. If someone gets past the gate, they have access to everything else.

2. Device Management:

Why Second? Once you know who's accessing, you need to know *what* they're accessing from. Device management ensures that devices meet your security standards (patched, encrypted, etc.).

Compromised devices are a major entry point for attackers. By managing devices you can reduce the number of vulnerable entry points.

3. Endpoint Protection:

Why Third? Now that you've secured identities and devices, you need to protect the endpoints themselves from malware, exploits, and other threats. Endpoint protection provides real-time defense.

This is your first line of active defense against malware and other threats that may get past your gate and device security.

4. Email and Messaging Security:

Why Fourth? Email remains a primary vector for phishing and malware. Securing email and messaging is critical to preventing attackers from gaining initial access or spreading within your network.
Because so much malicious activity is delivered via email, it is critical to secure this vector.

5. Information Protection:

Why Fifth? This focuses on protecting the data itself, regardless of where it resides. This includes encryption, data loss prevention (DLP), and access controls.
Once an attacker is inside, information protection limits the damage they can do by restricting access to sensitive data and preventing exfiltration.

6. Ransomware Protection:

Why Sixth? While ransomware protection is interwoven with many of the above (endpoint protection, backups, etc.), it deserves specific attention. This step emphasizes proactive measures like regular backups, incident response planning, and user education to minimize the impact of a ransomware attack.
Ransomware is so devastating that it needs its own specific focus. This step is about making sure that if all other defenses fail, you can still recover your data.

All building blocks should be fully intergated and monitored 24x7 to be effective