

## Cyber-Informed Defense Models

dvantages

Proactive, anticipates threats

Threat intelligence, adversary behavior

High context, includes adversary TTPs

Enhanced incident response, informed by likely threats

Targeted coverage, based on threat data

Potentially resource-intensive, covers all possible opssions

High complexity, requires specialized skills and tools

Qualitative metrics, based on threat intel

Quantitative metrics, based on vulnerability data

Vulnerability identification and remediation

Moderate complexity, relies on established frameworks and tools

Efficient, based on vunerability criticality

Low context, focuses on technical flaws

Basic incident response, focused on remediation efforts

Broad coverage, addresses all known vulnerabilities

Reactive, addresses known vulnerabilities

Disadvantage