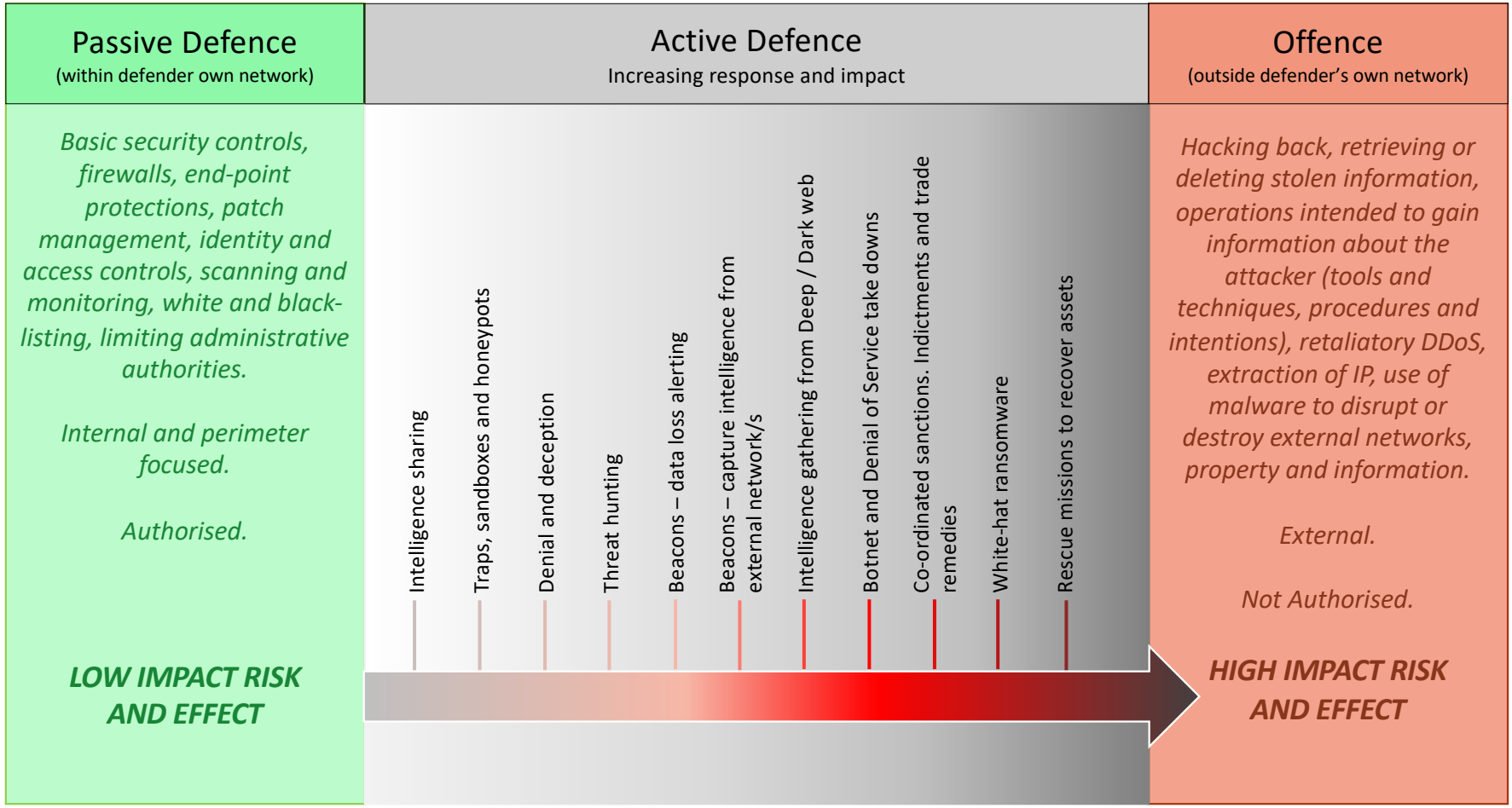
Passive Defence
(within defender own network)
Basic security controls, firewalls, end-point protections, patch management, identity and access controls, scanning and monitoring, white and black-listing, limiting administrative authorities.
Internal and perimeter focused.
Authorised.
LOW IMPACT RISK AND EFFECT
Active Defence
Increasing response and impact
Intelligence sharing
Traps, sandboxes and honeypots
Denial and deception
Threat hunting
Beacons – data loss alerting
Beacons – capture intelligence from external network/s
Intelligence gathering from Deep / Dark web
Botnet and Denial of Service take downs
Co-ordinated sanctions. Indictments and trade remedies
White-hat ransomware
Rescue missions to recover assets
Offence
(outside defender's own network)
Hacking back, retrieving or deleting stolen information, operations intended to gain information about the attacker (tools and techniques, procedures and intentions), retaliatory DDoS, extraction of IP, use of malware to disrupt or destroy external networks, property and information.
External.
Not Authorised.
HIGH IMPACT RISK AND EFFECT