

Breakthroughs for Defenders

XDR Kill Chain™ – Full visibility across the entire attack surface minimizing enterprise security risk

Stellar Cyber's XDR Kill Chain – delivering the promise of EVERYTHING detection and Response

The XDR Kill Chain is a fully MITRE ATT&CK compatible kill chain that is designed to characterize every aspect of modern attacks while remaining intuitive to understand.

All Stellar Cyber alert types are aligned to the XDR Kill Chain out of the box, so you can start detecting full attack progressions immediately.

Modern Attacks Need Modern Thinking

- ✓ First new kill chain invented in years – designed specifically for XDR detections, where threats can attack any point in the infrastructure.
- ✓ Loop interface prioritizes detections into five phases: initial attempts, persistent foothold, exploration, propagation, and exfiltration / impact – analysts can easily see attacks as they happen and respond to the most emergent needs first.
- ✓ Captures the progression of complex attacks – alerts appear in the context of the five-phase kill chain so analysts can easily prioritize them without getting lost in details.
- ✓ Incorporates commonly used MITRE ATT&CK framework for detailed analysis and adds new tactics and techniques beyond the MITRE ATT&CK framework.
- ✓ Clearly shows external vs. internal attacks – helps analysts know exactly where to look to stop attackers.



STELLAR CYBER XDR KILL CHAIN

Holistic security posture monitoring in one intuitive dashboard

XDR Kill Chain Stage	Initial Attempts	Persistent Foothold	Exploration	Propagation	Exfiltration & Impact
XDR Extended Detections	External XDR NBA, External UBA, XDR SBA	External XDR NBA, External UBA, XDR SBA	External XDR Malware, XDR Intel, XDR EBA	Internal XDR NBA	
MITRE Tactics	Reconnaissance, Resource Development, Initial Access, External Credential Access	Execution, Persistence, Defense Evasion, Command and Control	Discovery, Collection	Internal Credential Access, Privilege Escalation, Lateral Movement	Exfiltration, Impact



XDR Malware

Covers all malware-related detections

XDR Intel

Covers all threat intelligence-related detections

XDR User Behavior Analytics (UBA)

Covers user anomaly detections

XDR Network Behavior Analytics (NBA)

Covers network anomaly detections

XDR Endpoint Behavior Analytics (EBA)

Covers all host-based anomaly detections

XDR Sensor Behavior Analytics (SBA)

Covers injection anomaly detections on the operational side

WHY STELLAR CYBER'S XDR KILL CHAIN PROVIDES BETTER RISK REDUCTION

Lockheed Martin Cyber Kill Chain	XDR Kill Chain
Outdated, created 2011	Created 2021, up to date
Malware centric	General enough for all detections
Prior MITRE ATT&CK, not compatible with ATT&CK	MITRE ATT&CK native by design
Cannot differentiate between internal / external attacks	Built-in external versus internal / lateral attack distinction
Linear, did not capture complex attack progression	Better capture for complex multi-stage attacks with loop design
Lack of tagging, cannot categorize hot trends	Multi-tag-based categories, easier to capture hot trends such as ransomware