ArcSight Intelligence and MITRE ATT&CK

Micro Focus ArcSight Intelligence covers 75% of ATT&CK tactics and techniques.

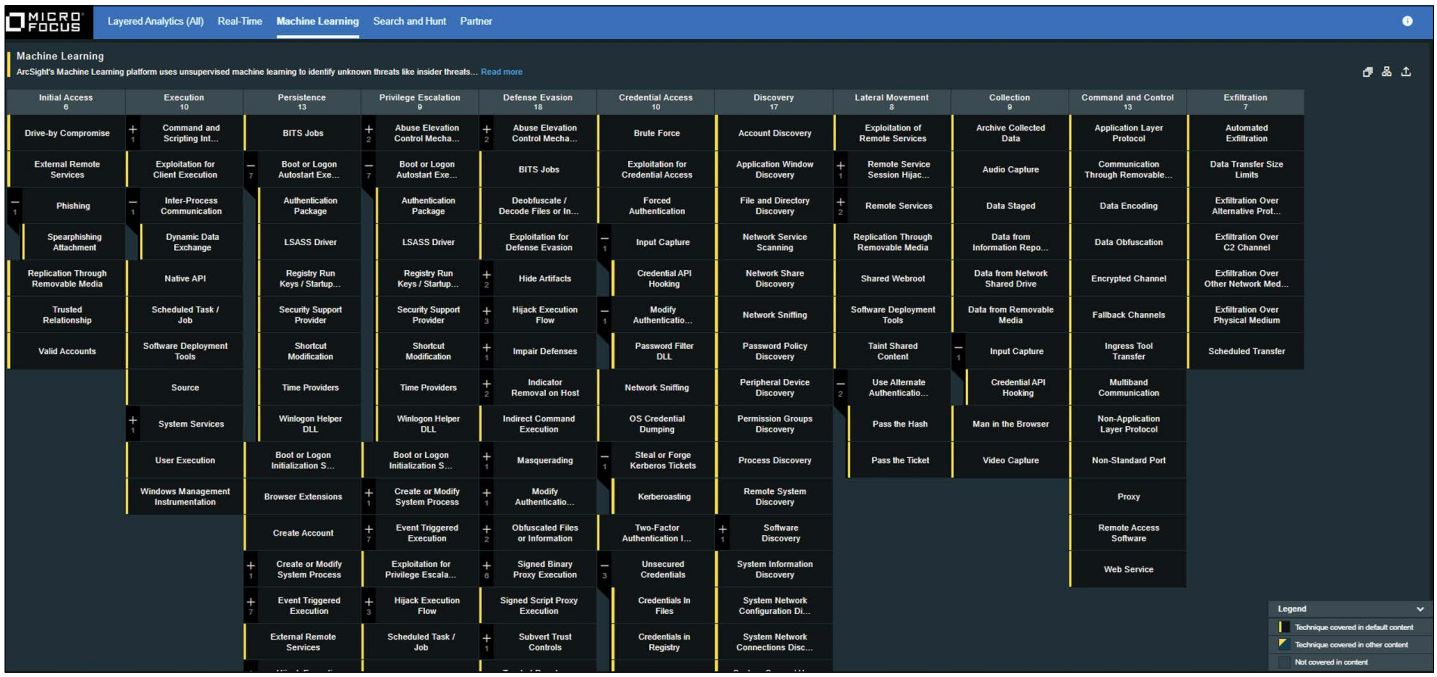

Figure 1. Heatmap

MITRE's ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a living knowledge base of threat tactics and techniques observed in real-world attacks on enterprise networks, and it plays a pivotal role in ArcSight Intelligence's behavioral analytics.

Detect the Unknowns with ArcSight Intelligence and ATT&CK

With detailed information on data sources, mitigation, examples, and detection for many tactics and techniques, ATT&CK is a one-stop-shop for security researchers, practitioners, or vendors to better understand how to effectively protect organizations from real attacks. Today, ArcSight Intelligence covers 75% of the ATT&CK framework that has been seen in the wild, and our coverage will continue to grow.

ArcSight Intelligence leverages more than 450 machine learning models to baseline the behavior of every user and entity within an organization and evaluate deviations from those baselines as potentially risky behaviors. Our machine learning models are carefully mapped to ATT&CK's 219 techniques to better understand:

- Which attack techniques our customers face most often
- Where ArcSight Intelligence provides coverage most effectively
- How we can leverage our anomaly models to protect businesses against real threats.

ArcSight Intelligence's behavioral analytics covers 75% of the techniques in MITRE's ATT&CK framework*, providing effective coverage against a range of threats that can facilitate exfiltration of high-value information, fraud, and more.

*The heatmap above does not represent the full MITRE ATT&CK framework. Visit **mitre.microfocus.com** for more information.