opentext™ | Cybersecurity

atarlabs

Partner Flyer

Integrated Defense with ATAR, ArcSight and Interset UEBA

To improve operational and security efficiencies, the modern SOC should leverage layered analytics by integrating the capabilities of SIEM, user and entity behavior analytics (UEBA), and SOAR.

Integrated Defense with ATAR, ArcSight and Interset UEBA at a Glance

Key Benefits

- A unified security operation through ATAR automation and orchestration capabilities.
- No more missed incidents and unresolved gaps in your security posture.
- Unite the knowledge on separate systems to defeat adversaries.

Products

- ATAR
- ArcSight
- Interset

Implementing/Introducing End-to-End Security Operations

Currently, enterprises are hard-pressed to keep up with adversaries, struggling to get ahead. The problem is clear, but the solution seems out of reach for most. The increasing complexity of attacks and growing need for more talent in the security operations center (SOC) make the solution a fleeting one. Even when the necessary technology stack is available, disjointed technologies make it hard to see the big picture and act on it.

ATAR, integrated with ArcSight and Interset User and Entity Behavioral Analytics (UEBA), creates a fast-acting environment against threats with top-of-the-line capabilities distributed across an enterprise at your fingertips.

ArcSight's powerful correlation engine uses rules and threat intelligence to identify and alert you to threats across the enterprise in real time. It can send those alerts to ATAR for evaluation, and after prioritization and investigation, appropriate action can be taken to further eliminate your adversaries. User behavior and anomaly data from Interset UEBA can be brought into ATAR to be used for enhancing incident detection and investigation capabilities. ArcSight's real-time event correlation and Interset's machine-learning-driven anomaly detection gives ATAR customers the ability to respond to attacks faster than humanly possible.

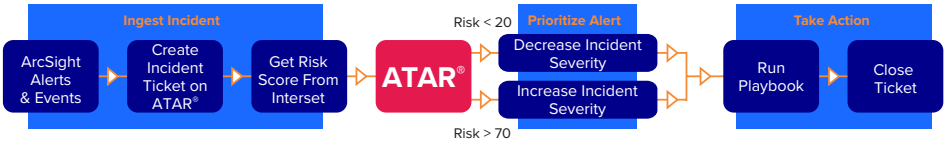
Customers can easily enjoy the benefits of the out-of-the-box joint integration without any additional investment.

Use Case #1: Reducing SIEM Alert Tsunami

Challenge: Enterprises get hundreds of security alerts every day, and SOC teams drown in the tsunami of alerts while trying to evaluate and prioritize those alerts.

Solution: ATAR is integrated with ArcSight and Interset UEBA to help with the prioritization and investigation of alerts as well as the remediation of incidents.

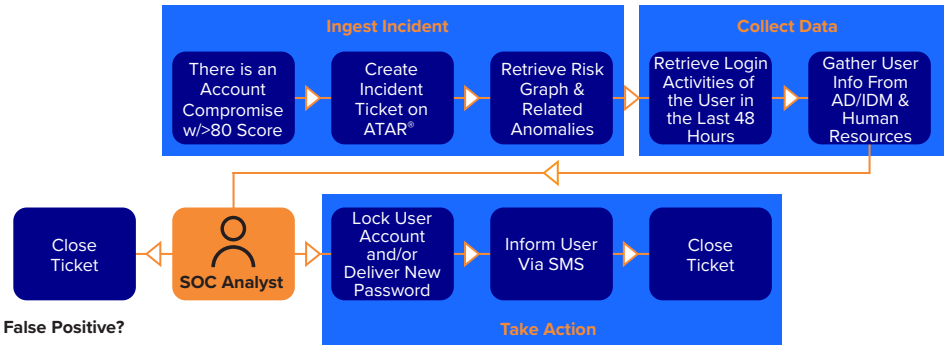
ArcSight Alert Prioritization



Use Case #2: Account Compromise

Challenge: It's crucial to detect an account compromise, investigate the case, and respond promptly.

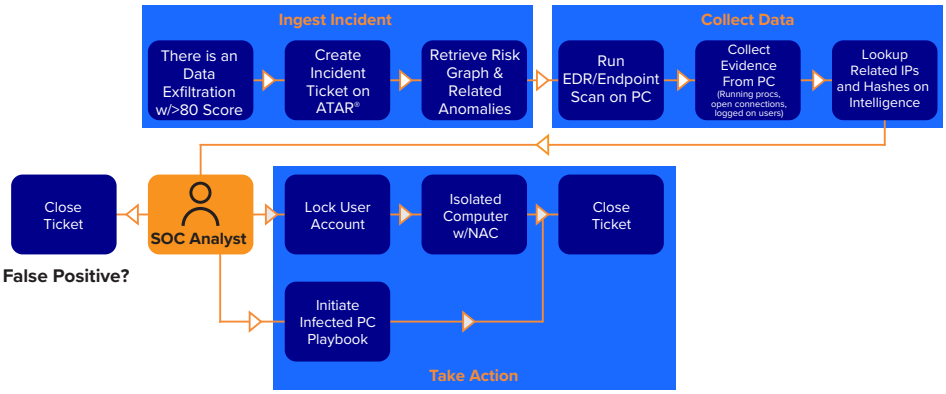
Solution: ATAR can ingest anomaly data from Interset and create an incident ticket on its own Incident Management Service Desk. With its broad integration portfolio, orchestration, and automation capabilities, ATAR investigates, ascertains the case, and takes necessary actions to prevent the compromise.



Use Case #3: Data Exfiltration

Challenge: Detecting and differentiating anomalous data flow from normal traffic transmitting network boundaries is challenging.

Solution: Using unsupervised machine learning, Interset detects unusual behaviors that signal an attempt at data exfiltration, and then informs ATAR. Then ATAR connects suspicious PCs to collect evidence, lock the user accounts, and isolate the PCs from the network automatically.



About Atar Labs

ATAR Labs launches SOAR platform ATAR to support organizations that find catching up with the speed and volume of cyber-attacks challenging. ATAR defense robot automatically runs the pre-programmed attack reflexes and frequently runs repetitive operations in a security operations center without the need of a human expert. By this means, while 30–40% of the total alarm handling the load is covered by the platform, incident investigation and response capabilities provided by ATAR allow operation center experts to analyze and resolve incidents 15 to 20 times faster. To get more information about ATAR Labs visit: **www.atarlabs.io**

Connect with Us

www.opentext.com

opentext™ | Cybersecurity | atarlabs

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

761-000127-001 | O | 10/23 | © 2023 Open Text