Integrated Defense with
ATAR®, ArcSight and Interset UEBA

ATAR® | **ArcSight** | **INTERSET**

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 Micro Focus 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.

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®, Interset UEBA, ArcSight

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 Micro Focus ArcSight and Interset UEBA to help with the prioritization and investigation of alerts as well as the remediation of incidents.

ArcSight Alert Prioritization

Ingest Incident
ArcSight Alerts & Events → Create Incident Ticket on ATAR® → Get Risk Score From Interset → **ATAR®**

Risk < 20

Prioritize Alert
Decrease Incident Severity
Increase Incident Severity

Risk > 70

Take Action
Run Playbook → Close Ticket
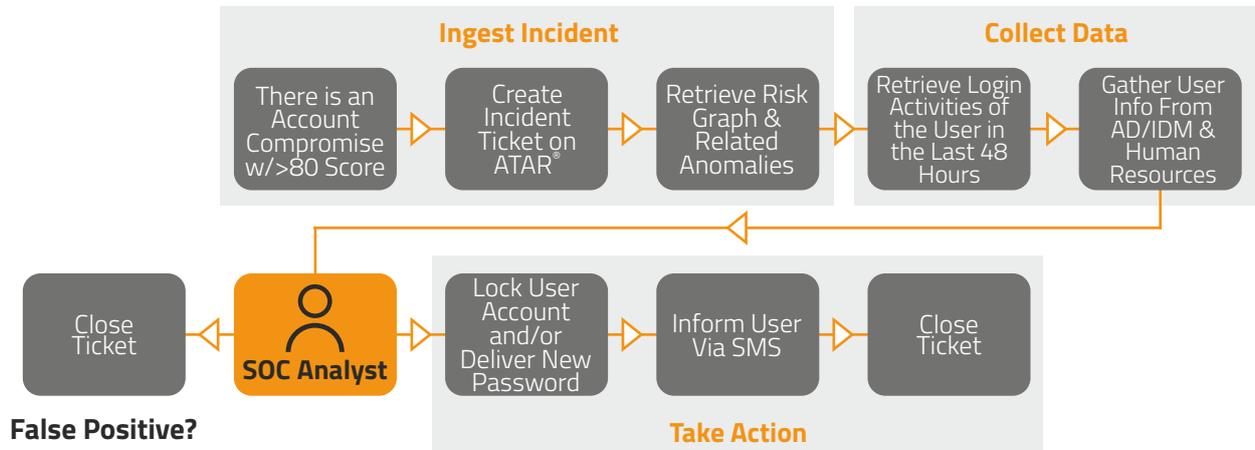
USE CASE #2   Account Compromise

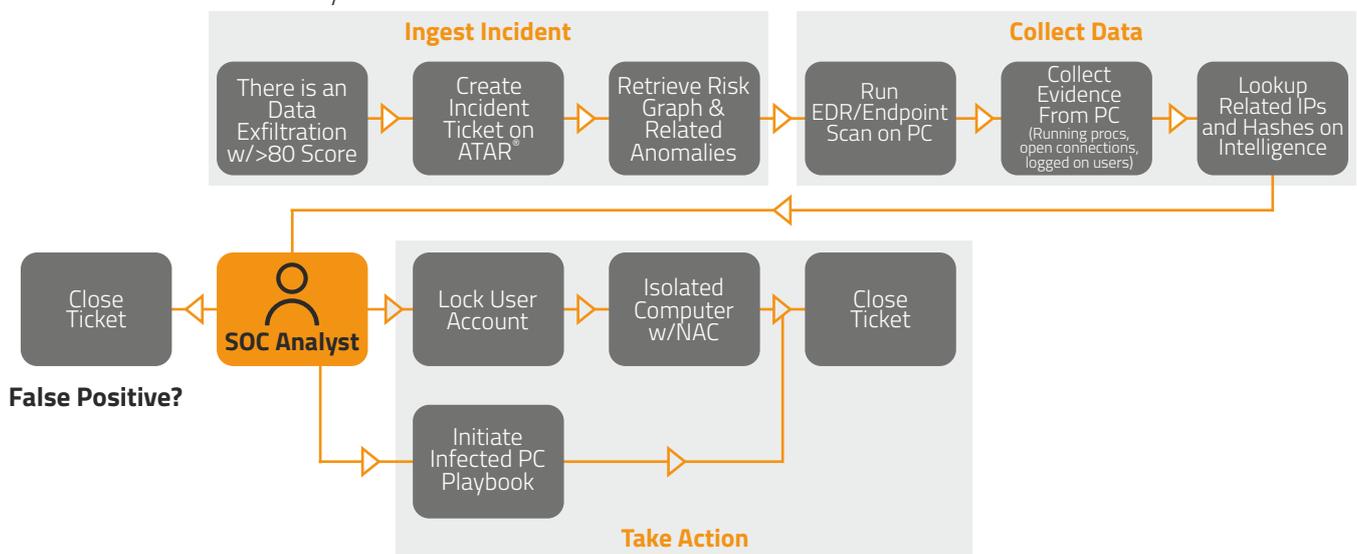**Challenge:** It's crucial to detect an account compromise, investigate the case, and respond promptly.

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.

Ingest Incident

There is an Account Compromise w/>80 Score → Create Incident Ticket on ATAR® → Retrieve Risk Graph & Related Anomalies

Collect Data

Retrieve Login Activities of the User in the Last 48 Hours → Gather User Info From AD/IDM & Human Resources

Close Ticket ← **SOC Analyst** → Lock User Account and/or Deliver New Password → Inform User Via SMS → Close Ticket

False Positive?

Take Action

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.

Ingest Incident

There is an Data Exfiltration w/>80 Score → Create Incident Ticket on ATAR® → Retrieve Risk Graph & Related Anomalies

Collect Data

Run EDR/Endpoint Scan on PC → Collect Evidence From PC (Running procs, open connections, logged on users) → Lookup Related IPs and Hashes on Intelligence

Close Ticket ← **SOC Analyst** → Lock User Account → Isolated Computer w/NAC → Close Ticket

Initiate Infected PC Playbook →

False Positive?

Take Action

About MicroFocus

Micro Focus helps organizations run and transform their business. Driven by customer-centric innovation, our software provides the critical tools they need to build, operate, secure, and analyze the enterprise. By design, these tools bridge the gap between existing and emerging technologies—enabling faster innovation, with less risk, in the race to digital transformation. To learn more about **Micro Focus, visit www.microfocus.com.**

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**