ANALYTICA42

DATASHEET

Full Lifecycle Security Services Overview

About Analytica42

We provide continuous risk evaluation programs and full lifecycle security solutions. Analytica42 was founded by an elite group of information technology and security professionals with more than two decades of background building technical solutions across a wide array of vendors, as well as leading professional services teams, including blue and red, threat research, and development teams. This deep combination of hands-on and leadership experience enables Analytica42 to deliver significant value in the most efficient manner—providing a high ROI on your security investments.

We take your difficult-to-address use cases or success criteria and translate them into practical, achievable results. It is our mission to not only help you with immediate security needs, but to empower you to address them going forward.

Services

Compromise Assessment

- Leverage existing/new tools to identify previously unknown anomalous activity and potential threats.
- Apply the results of the Compromise Assessment to tune and create content for your security solutions.

Threat Hunting and Analytics Training

Leverage your tools and real-world use cases of attacks and methodologies that illustrate how to conduct threat hunting and create analytics tied to threat hunting scenarios.

Threat Hunting On-the-Job (OTJ) Training

Often paired with the Compromise Assessment. Client team shoulder surfs and learns from Analytica42 staff while they are conducting the assessment or tuning/creating content.

> *Analytica42 not only built out a whole new class of alerts in our emerging SIEM platform but provided a script to automate the creation and maintenance of alerts based on external definitions. They took a deep dive approach simulating attacks to ensure the alerts covered real world scenarios.*

Head of Cybersecurity Engineering, Fortune 500 Media Company

Security Tools Content Creation

Often paired with the Compromise Assessment or SIEM Use Case Consulting. The service works with clients to create security content that will identify patterns/behaviors that may not be detected within existing security tool rules and signatures.

Security Information Event Manager (SIEM) Use Case Consulting

Coordinate with Analytica42 staff to determine SIEM use cases/success criteria and leverage SIEM tools to conduct use case analysis, including gaps in data. Deliver results of use case efforts to client staff, including any dashboards/ reports/queries.

Managed Detection & Response (MDR) Creation/Development

Leverage the experience of Analytica42 staff, who have built MDR Services organizations in the past, to help design and build an MDR solution for your organization. This includes people, processes, and technology.

Security Operations Center (SOC) Operations

- Work closely with seasoned security staff that have built SOCs at large organizations. Conduct gap analysis of SOC processes/ tools/staff.
- Receive recommendations for SOC optimization.

Data Analytics

- Work with Analytica42 staff to determine what analytics you need from your big data solutions.
- Analytica42 staff will define the appropriate data sets, tools, and queries necessary to help you find the information within your data and make it presentable to the right audience.

Application Development

- Analytica42 will work with you to determine your development requirements, both technical and procedural.
- Once requirements are determined and test environment is identified, Analytica42 will develop and test the solution, then work with you to deployit.

Workflow and Automation Development

- Analytica42 will work with you to assess your workflow requirements and available automation tools, e.g. Security Orchestration Automation Response (SOAR) and steps.
- The Analytica42 team will then update your existing SOAR tool or automation platform to enable the workflow or automation to address your use cases and deploy it in production.

Deployment Services

- Analytica42 will work with your staff to deploy various tools, including SIEM, SOAR products, Endpoint Detection Response (EDR).
- The team will work with your staff to determine a feasible deployment plan and then execute the plan based on specific success criteria.