ANLYZ®

ANLYZ SOAR - SPORACT

PRODUCT SHEET

A holistic solution for Incident Management, Automation and Response.

Anlyz SOAR's analytical capabilities enable security operations teams to track, analyze and terminate threats. Data insights equip the team to comprehend the current landscape of cyber security arena by threat categories. Contextual insights arm them with diverse combat methods. Overall, Anlyz SOAR enables CISOs and leadership teams to develop better strategy around people, process and technology for comprehensive security incident response management.

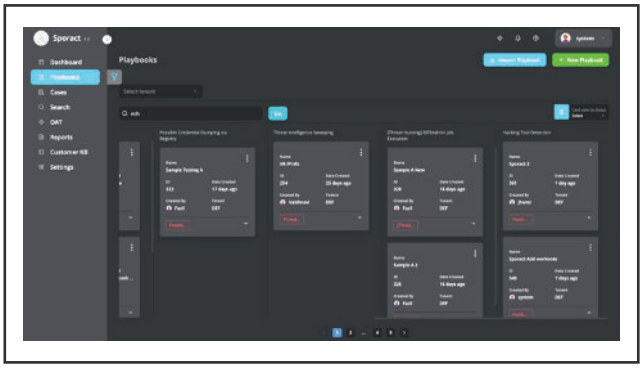
KEY BUSINESS CHALLENGES

- **ALERT OVERLOAD-** 150K + Alerts/Week
- **HUMAN INTERVENTION-** Manual Responses
- **TALENT SHORTAGE-** Limited Skilled Resources
- **WORK FROM ANYWHERE-** Perimeter Is Long Gone
- **INVESTIGATION-** Average Root Cause Analysis(RCA) Takes 4 Days
- **SECURITY IN SILOS-** Alert In Each Dashboard

KEY FEATURES

Versatile Playbooks with decision based playbook chaining

To create an autonotmous SOC, constantly developing Playbooks are imperative in order to save analyst's time and ensure a better experience. Leverage 150+ qualitative playbooks, customized for the modern SOC: Enrichment playbooks to provide meaningful data; Investigation playbooks designed to look for more evidence; Response playbooks built to handle standardised actions for known alerts & Logic-based chained playbooks that combine multiple playbooks optimally, to provide a swift outcome with the least number of actions required. These specially designed no code playbooks combine the best of people, process and technology to automate SOC operations.

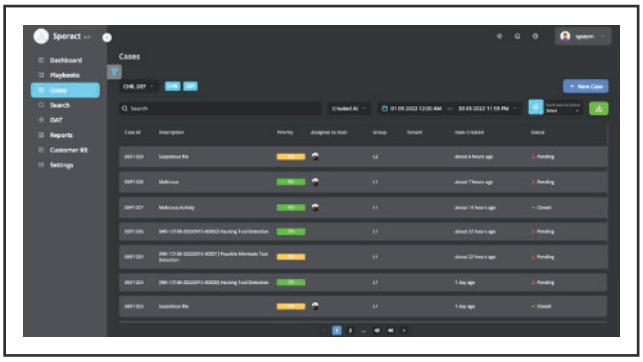


Role-based visualization

Role based dashboards allow alerts to be managed in effectively to ensure analyst focuses on the relevant details. These role based dashboards help SOC teams to track incidents effectively and also measure SOC operations performs using quantifiable metrics.

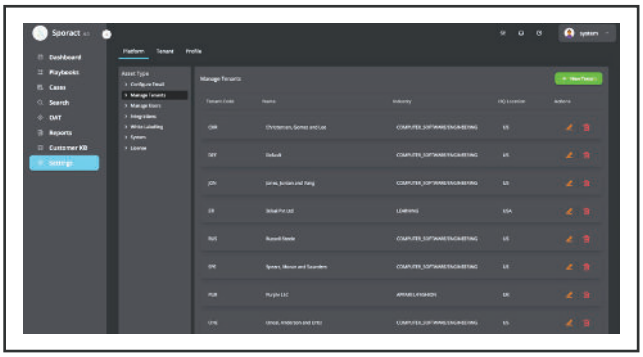
Case management

Manual or automated response in the built-in Case Management tool provides canned resolution to defined activities, thus speeding up incident tracking & investigation, making it easier for analysts to close security alerts. This functionality is the most impactful operationally as it applies to the most complex of use cases and can significantly improve analyst effectiveness.



Multitenancy

Navigating between multiple customer environments can be a challenge for even the most skilled of security analysts. With Anlyz SOAR, focus on what is more critical to efficiently manage security incidents in the least possible time without violating compliance. MSSP providers will benefit most from this capability due to minimal deployment costs, option to scale and flexibility to distribute architecture.



Curated Threat intel

Anlyz SOAR empowers SOC with actionable insights from its curated Threat Intelligence platform (TIP). The Indicators of Compromise (IOCs) are collected from deep web, open sources & credible paid sources, followed by elimination of false positives to create a verified pool of malicious threat actors.This helps Auto Enrich IOCs with an aggregated verified database.

Easy Integrations

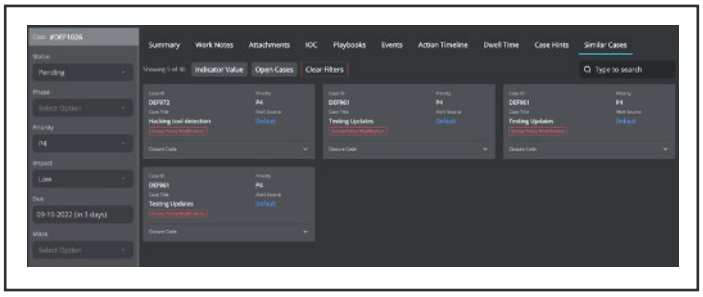
Anlyz SOAR's integrations provide comprehensive visibility and control across the enterprise solution stack including endpoint security, network security, email security, cloud platforms, IDP, Application security, edge security & business operations. Anlyz SOAR seamlessly integrates with homegrown business critical tools with robust APIs as well.

Reporting and Metrics

Advanced analytics and granular reporting widens visibility into the attack surface. Analyst load, along with key metrics like dwell time, MTTD & MTTR are tracked, empowering SOC teams to measure and track performance minutely. Anlyz SOAR also delivers automated industry-standard reports on time without any human intervention.

Powered by AI-ML

AI-Ml based algorithms provide meaningful insights and qualitative indicators to SOC analysts, helping them leverage data from past incidents, take more accurate decisions and reduce overall turn around time.



KEY BENEFITS

1. Increased SOC Efficacy

Orchestration & Automation of security incidents enables analysts to handle upto 10x more alerts daily. Anlyz SOAR empowers SOC operations with fast response time. With minimal to zero false positives, SOC analysts can focus on cases which truly need human intervention.

2. Resolve Incidents in Minutes

Minimise your MTTD and MTTR to threats using our customized out-of-the-box no code playbooks. Automate security tasks across a variety of tools, with confidence.

3. Say No to Alert Fatigue

Managing security incidents is simpler then ever with customized playbooks powered by curated threat intel and customer discovery, enabling modern SOC to handle alerts from hours to minutes. Thus, leading to a focused approach on high priority alerts in real time, rather than delayed actions leading to SLA breaches because of alert queue build-ups.

4. Designed to Minimise the Learning Curve

SOCs need not operate in complex environments with disparate tools. Anlyz SOAR's easy-to-understand interface and no code playbooks ensures that SOC analysts can quickly get started. This inturn leads to faster time to value.

5. Deployment Made Easy

Anlyz SOAR's inherently scalable architecture can expand across ever-growing organisations without any impact on the resources needed for deployment and management. Can easily be deployed on-premises, on a private cloud or as a fully-hosted solution.

MAXIMIZE PRODUCT EFFICACY WITH ANLYZ SOAR

Rapid Containment
All tickets will have playbooks triggered to immediately contain the incident, without waiting for an Analyst

High Fidelity Alert
On an average 100,000 alerts are generated and SIEM aggregates and corelates these alerts. This helps to zero in on the actual issue.

Compliance
A SIEM is the basic requirement for any compliance, having a SOAR as well directly enables you for SOC-2 compliance enabling you to onboard more clients.

Shortened RCA Span
It takes 4 days to conduct an RCA, with Anlyz that reduces to less than 5 Hours

Case Management
SOAR comes with inbuilt ticketing tool so additional investment on said tools will be avoided.

Automated Response
85% of alerts will be dealt with an automated response action to mitigate the threats.

ANLYZ®

Contact us at

contact@anlyz.co

www.anlyz.co