OrusGroup
The Science of Information Technology

SOC-as-a-Service White Paper

Even before the advent of the "Internet of Things" (IoT), the proliferation of mobile devices, and remote workers hackers had the upper hand. Today the problem is worse. The ever expending digital footprint of most IT organizations has ballooned to include support for telework, collaboration, and mobile applications. This increase corresponds with an increase in the attack surface and threat profile for Enterprise IT shops.

In recent years there has been an escalation of sophisticated and targeted ransomware exploits. Industries including state and local government and healthcare organizations have been heavily targeted. Attackers are spending more time to gather intelligence on their victims, achieving maximum disruption and scaled-up ransoms.

Security incidents can happen without warning and they often go undetected for long periods of time. Organizations struggle to identify incidents because they often work in silos or because the number of alerts is overwhelming. Collecting, correlating, and identifying threats among a large volume of security information is a key challenge. False alerts plague security teams in charge of dealing with these threats and cause an overhead of security information that increases the burden placed on security operations. All of this slows and impacts an organization’s effectiveness with incident response.

Although preventive measures remain an essential part of a CISO's overall strategy for diminishing security incidents, it is impossible to stop every attack. In fact, organizations must assume a network will be compromised at some point. What can become more important than preventing a breach is minimizing the resulting damage by detecting, containing, and controlling the incidents.

The threat actors targeting your data and your critical resources leverage numerous tools in conjunction with the scalability of virtualization and the Cloud to overwhelm your defenses. This is especially true if the focus of your security efforts is over reliant on documentation and compliance. The agility of your security program and its ability to adapt to the rapidly evolving attack surface and threat profile for your organization is what is necessary for the success of the program. Security program agility requires the following key capabilities:

- Aggregation of large volumes of information
- Efficient correlation and classification of data pertinent to your security posture
- An ongoing cipher of detection validation/investigation, and response
- Threat intelligence, cyber hunt, and feedback mechanisms to ensure the detection of intrusions and incidents can evolve with the threat profile

To effectively realize these capabilities today’s security programs need to incorporate automation and machine learning to deliver the situational awareness necessary to take proactive measures and mitigate the risks facing the organization. Security leadership will require a dashboard view that continuously evaluates security posture in order to guide informed decision making.

SOC-as-a-Service White Paper

The solution is to implement a Security Operations Center (SOC) with a threat intelligence capability. This type of advanced robust security infrastructure and expertise is beyond the reach of many IT organizations due to budget and resource constraints. The **OrusGroup has partnered with AgileBlue** to address these challenges with a best in breed effective and affordable SOC-as-a-Service solution for our customers.

The OrusGroup SOC-as-a-Service Difference

Risk based scoring allows for quick at a glance view of your organization's security posture.

OrusGroup SOC-as-a-Service Risk Score is based on 13 critical security factors and MITRE developed Indicators of Attack (IoA).

US based SOC staffed with US Citizens monitoring 24x7x365

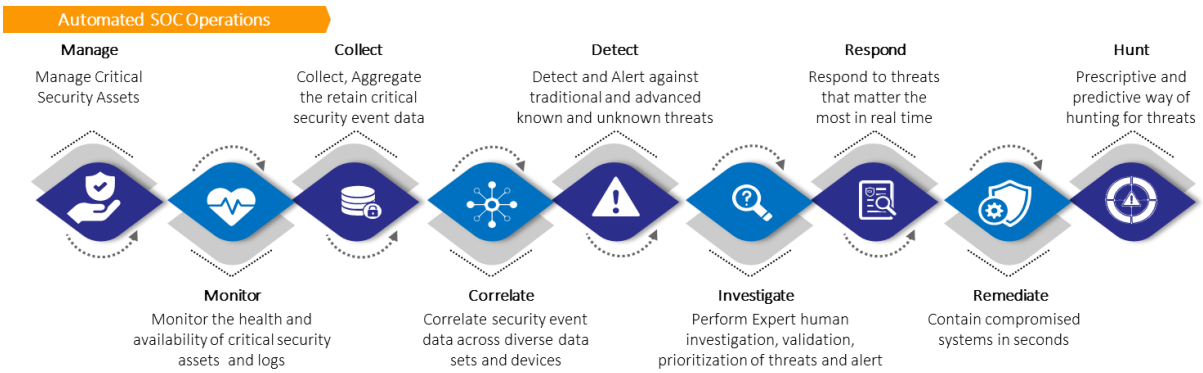
Our technology is innovative, efficient, and proven to be successful at significantly increasing the security posture of our clients. Our differentiators demonstrate why we are effective at improving our client's security programs. Our differentiators include the following:

- We use data science to create intelligent incidents not just alerts which are rampant with false positives because of old rules
- Our machine learning, user behavior analytics and cyber automation predict threats to your digital footprint
- We don't just read logs and create alerts. We track anomalous behavior across people, data, applications, Cloud and all digital entities
- Our proprietary Silencer technology enforces 90% true positives and correlates anomalous behavior
- Our Predictive Analytics & Risk Scoring shows real time remediation impact on risk profile

Our approach is based on three phases

1. Data Aggregation - Manage, Monitor, and Collect
2. Cyber Data Analysis – Correlate, Detect, Investigate
3. Response – Respond, Remediate, Hunt

These phases are shown below in our SOC Operational view based on AGILE BLUE SOC technology.



SIEM + 24/7 Monitoring

Our turnkey service includes an advanced SIEM, complete with setup, tuning, maintenance, monitoring, and staffing. Pulling local and cloud data and leveraging big data and machine learning, we get real-time insight, unlimited policy customization, logging, alerts, and dedicated personnel to fend off false-positives and provide critical Incident Detection. When detected, incidents are addressed immediately, day or night.

Managed Detection

A traditional SIEM deployed onsite (i.e., Splunk, LogRhythm, AlientVault, etc.) requires significant upfront and ongoing expense, staffing, and training. This makes it possible to detect a breach but difficult to respond in a relevant timeframe. Personnel must also sort through a sea of false positives. Our SOC automates this, allowing AgileBlue and our security partners to intervene in real time, stopping the breach and resolving it before it turns into something big.

Logging

With the depth of event monitoring and logging of a SIEM combined with next-generation cloud integrations with Office 365, Microsoft Azure, Amazon Web Services, GCP, and others, we can monitor all of your critical services allowing for end-to-end protection. This service provides (1) year log retention (additional years available at extra cost).

24x7 Staffing

Our SOC solution is staffed and monitoring log data and alerts 24x7x365. If an alert is validated as not being a false-positive, we step in immediately to shut down the affected systems and begin cleaning the affected equipment and software. Your subscription includes a Concierge Security Team dedicated to around-the-clock monitoring, alert review, and incident response. It also includes a Success Team who are dedicated to getting the service off on the right foot and ensuring continued service success. This team provide quarterly security reviews, project planning support, and features and roadmap discussion.

Analysis & Reporting

Our AgileBlue SOC solution provides clear visibility into the physical and virtual risks inherent in your environment. We'll provide you with weekly, monthly, and quarterly reports, and we can build almost any report you need. Our report writing capabilities are augmented with those of our security partner meaning we can deliver just about any report you would like.

Real-time Analytics Dashboard

We empower your entire team with data insights in real-time paired with cloud-based dashboards so your data is never stale.

OrusGroup SOC-as-a-Service provides the optimal features and service to secure your environment at a price point that fits within your budget.

- Fixed monthly fee based on devices
- 24/7 Security Ops Team
- Managed cloud-based SIEM
- Threat hunting
- Threat intelligence (3rd party)
- Real-time notifications and guided alerts
- Online analytics / reporting dashboard
- Integration with industry leading response tools
- Monthly review and recommendations
- Regulatory compliance

We invite you to contact us for your free SOC needs assessment

AGILEBLUE