Introduction

SecureGate is an Italian cybersecurity company dedicated to enhancing the digital protection of organizations through innovative solutions and managed services. The company operates primarily through two specialized business units, **SGBox** and **CyberTrust 365,** and the new product **GroundSOC.**

SGBox is the business unit of SecureGate focused on developing and providing a next-generation SIEM (Security Information and Event Management) & SOAR (Security Orchestration, Automation, and Response) platform. This modular and scalable solution is designed to offer comprehensive control and management of IT security. The platform's architecture allows it to adapt to various business needs, providing functionalities such as log management, event correlation, incident management, and vulnerability assessment. SGBox is utilized globally, supported by a growing network of partners, to help organizations proactively monitor and mitigate cyber threats.

CyberTrust 365 serves as SecureGate's Managed Security Service Provider (MSSP) division, offering a suite of managed cybersecurity services. These services include 24/7 monitoring, proactive defense, and in-depth threat analysis, allowing businesses to focus on their core operations while ensuring robust protection against cyber threats. CyberTrust 365's offerings encompass External Attack Surface Management (EASM), Vulnerability Assessment and Penetration Testing (VA/PT), SOC as a Service, Security Advisory, Managed SIEM and Build Your Own SOC (BYOS) services. This customer-centric approach ensures tailored security strategies that align with specific organizational needs and compliance requirements.

GroundSOC is the new Platform of SecureGate designed to help Large Enterprises and MSSPs in the management of huge volume of logs, enabling unified visibility, scalable data collection, and advanced log compliance across IT and OT environments. It includes **all capabilities of SGBox**, enhanced with enterprise-scale features for corporate SOCs and MSSPs.

The strategic structuring of SecureGate into these two business units enables the company to deliver both advanced security products through SGBox and comprehensive managed services via CyberTrust 365, effectively addressing the diverse cybersecurity challenges faced by organizations today.

Multitenant SIEM&SOAR Platform

SGBox is a scalable, multi-tenant security platform that combines SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) into a unified solution. It is designed for MSSPs (Managed Security Service Providers), enterprises, and large organizations that need to manage security operations to prevent cyber threats and consequent data loss.
SGBox SIEM also helps organizations automate compliance monitoring, generate audit-ready reports, and detect violations in real time. It is particularly valuable for MSSPs, financial institutions, healthcare providers, and enterprises that must adhere to strict regulatory standards.

SGBox includes many security capabilities, aggregated in some license packages to meet the different requirements of every specific final user.

Log Management

SGBox Log Management is a core component of its SIEM & SOAR platform, offering centralized collection, intelligent parsing, long-term retention, and powerful analytics. It helps organizations improve security, meet compliance, and troubleshoot IT issues faster.

SGBox provides an enterprise-grade log management solution as part of its SIEM vfr & SOAR platform, enabling organizations to collect, normalize, store, analyze, and archive logs from diverse sources for security, compliance, and operational monitoring.

MS AD Auditor

SGBox's Microsoft Active Directory (AD) Auditor is a specialized security module designed to monitor, analyze, and audit AD environments for security risks, compliance violations, and insider threats. It provides deep visibility into user activities, permission changes, and authentication events, helping organizations secure their identity infrastructure.

SGBox AD Auditor enhances Active Directory security by providing real-time monitoring, threat detection, compliance reporting, and automated response—going beyond native Windows logging. It's essential for enterprises, MSSPs, and regulated industries (finance, healthcare) to protect their identity infrastructure.

System Monitor

SGBox System Monitor to provide real-time monitoring, performance tracking, and security analysis for servers, workstations, cloud instances, and network devices. It ensures operational stability, detects anomalies, and prevents outages while integrating with security workflows.

SGBox System Monitor bridges the gap between IT operations and security teams, offering unified visibility into performance & threats.

SGBox Correlation Engine: Intelligent Threat Detection & Analysis

SGBox's Correlation Engine is the core intelligence layer of its SIEM & SOAR platform, to detect complex threats by analyzing relationships between events across logs, networks, and endpoints. Unlike basic log searching, it uses rules and threat intelligence to identify attack patterns that would otherwise go unnoticed.

SGBox's Correlation Engine transforms raw logs into actionable security insights by connecting dots between disparate events, reducing false positives and Accelerating response via SOAR automation.

SGBox User Behavior Analytics (UBA): Advanced Insider Threat Detection

SGBox UBA (User Behavior Analytics) detects anomalous user activities by analyzing behavioral patterns across systems. Unlike rule-based monitoring, it uses statistic algorhythms to establish baselines and flag deviations that indicate potential risks.

SGBox UBA provides proactive threat detection by profiling normal behavior to spot anomalies, reducing investigation time with risk-prioritized alerts and stopping insider threats before data is stolen.

SGBox Vulnerability Assessment (VA) Module: Proactive Threat Prevention

The SGBox Vulnerability Assessment (VA) Module is a core component of the SGBox SIEM & SOAR platform, designed to identify, prioritize, and remediate security weaknesses across IT infrastructure before attackers exploit them. It integrates automated scanning and risk scoring to reduce organizational exposure to cyber threats.

SGBox's Vulnerability Assessment Module goes beyond traditional scanners by linking vulnerabilities to active threats (via SIEM correlation), automating remediation (via SOAR) and simplifying compliance with pre-built reports.

SGBox Threat Intelligence Feed Integration: Enhanced Threat Detection & Response

The SGBox Threat Intelligence (TI) Feed Integration module enriches security monitoring by incorporating real-time threat data from external sources, enabling proactive identification of known malicious indicators (IPs, domains, hashes, etc.). It correlates this intelligence with internal logs to detect attacks earlier, reduce false positives, and automate responses.

SGBox Threat Intelligence Integration transforms raw IoCs into actionable security by boosting detection accuracy with real-time TI correlation, accelerating response via SOAR automation and enabling proactive hunting for hidden threats.

SGBox SOAR (Security Orchestration, Automation & Response)

SGBox SOAR is a module within the SGBox SIEM & SOAR platform, added to automate security operations, accelerate incident response, and reduce manual workloads for SOC teams. By integrating with SIEM, threat intelligence, and IT systems, it transforms alerts into actionable workflows with playbooks.

SGBox SOAR empowers SOC teams to respond faster with automation, reduce workload by eliminating repetitive tasks and meet compliance with detailed audit trails.

SGBox Incident Management: Unified Threat Response & Incident Handling

SGBox Incident Management is a core component of its SIEM & SOAR platform, designed to streamline the detection, investigation, and resolution of security incidents. It combines automated workflows and collaboration tools to help SOC teams respond faster and more effectively to cyber threats.

SGBox Incident Management transforms chaotic security operations by standardizing response with structured workflows and reducing resolution time via automation.

Managed Security Services

In today's evolving threat landscape, organizations face relentless cyberattacks—from ransomware and phishing to sophisticated nation-state intrusions. CyberTrust 365 Managed Security Services (MSS) provides enterprise-grade cybersecurity protection, combining 24/7 threat monitoring, advanced SIEM & SOAR, endpoint security, and expert incident response to defend businesses against modern cyber threats.

SGSoc - 24/7 Threat Monitoring & Response

CyberTrust 365 Security Operations Center (SOC) Service provides enterprise-grade, around-the-clock cybersecurity monitoring and incident response, ensuring organizations are protected against evolving threats. Combining AI-driven analytics, expert security analysts, and automated response workflows, the SOC acts as an extension of the final customer IT team to detect, investigate, and neutralize cyber threats in real time.

Benefits of CyberTrust 365 SGSoc

✓**Faster Threat Detection** – Combined detection and analysis tecniques reduce mean time to detect (MTTD) from days to minutes.
✓**Reduced Workload** – No need for an in-house SOC team; experts handle monitoring & response.
✓**Cost-Effective Security** – Predictable subscription pricing vs. hiring full-time analysts.
✓**Compliance Assurance** – Meets regulatory requirements with documented evidence.

CyberTrust 365 EASM (Cyber Risk Prevention)

Cybertrust 365 ACRM is an automated cyber risk monitoring and AI-driven remediation platform that offers organizations comprehensive visibility into their cybersecurity posture. By leveraging extensive databases of leaked passwords, dark web content, and advanced attack surface management tools, Cybertrust 365 ACRM provides a suite of solutions designed to proactively identify and mitigate cyber threats.

Services included into Cybertrust 365 ACRM:

✓**Leaked Credentials Monitoring -** Utilizes AI and human analysts to proactively search for and analyze compromised or exposed login credentials on the dark and public web, helping businesses prevent unauthorized access.
✓**Attack Surface Management -** Provides a web-based interface to visualize and monitor an organization's external internet-facing assets, including domains, IP addresses, and open ports, ensuring a comprehensive understanding of potential entry points for attackers.
✓**Vulnerability Scanning** - Continuously tests public assets and platforms for vulnerabilities using templates that minimize false positives, enabling fast and accurate scanning across numerous hosts.
✓**Cyber Risk Scoring -** Compiles risk ratings from multiple data points, such as leaked corporate emails, dark web exposure, attack surface size, and infrastructure vulnerabilities, providing organizations with an overall cyber risk score.
✓**AI-Powered Recommendations -** Offers personalized cybersecurity recommendations and easy-to-understand remediation plans to help organizations implement best practices and reduce risk exposure.

WAPT (Web Application Penetration Testing) Service

WAPT is a security evaluation process that simulates real-world attacks on web applications to identify and address vulnerabilities.
helpful to identify vulnerabilities in web applications, APIs, and mobile backends before attackers exploit them. Using manual and automated techniques, our certified ethical hackers simulate real-world attacks to uncover weaknesses that could lead to data breaches, financial loss, or compliance violations.

Vulnerability Assessment Service: Proactive Risk Identification & Mitigation

Our Vulnerability Assessment Service provides a systematic approach to identifying, classifying, and prioritizing security weaknesses across the IT infrastructure. Using automated scanning tools combined with expert analysis, we deliver actionable insights to strengthen your security posture before attackers can exploit vulnerabilities.

✓**Risk Reduction:** Prevent breaches by closing security gaps
✓**Cost Savings:** Avoid expensive incident response and downtime
✓**Compliance:** Meet regulatory requirements for vulnerability management
✓**Informed Decision-Making:** Allows IT teams to prioritize remediation based on real risks.
✓**Continuous Improvement**: if done regularly, it enables ongoing security posture enhancement
✓**Security Awareness:** Increases visibility into your threat landscape.

Security Audit Services: Comprehensive Protection Assessment
The **Cybertrust 365** security audit is a systematic evaluation of an organization's information systems, policies, and procedures to identify vulnerabilities, assess compliance, and ensure alignment with security best practices. Our audits combine automated tools with expert manual review to provide a 360° view of the cybersecurity posture and provide the clarity and direction needed to make informed decisions about the cybersecurity strategy.

The Visibility Fabric for Modern SOC

GroundSOC offers a hybrid and resilient architecture that ensures continuous visibility, empowering security teams with unlimited data ingestion and total control over operational costs.

Acting as a visibility and data-pipeline layer, it enhances any existing SIEM intelligently collecting, filtering, enriching, and forwarding logs with complete transparency and control.

Thanks to the Cluster-native architecture, Data management is optimized through sophisticated NoSQL storage techniques, which dramatically reduce occupied space while maintaining log integrity for legal purposes.

The flexibility of the software allows its use both in single business contexts and in multi-tenant mode.

Key Highlights:
- Smart log collection, filtering, and enrichment
- Multi-destination forwarding to SIEM/SOAR tools
- Built-in dashboards and Threat-Hunting
- Compliance-ready architecture for NIS2, GDPR & SAMA Cybersecurity Framework.
- Scalable, container-based deployment