BlackStratus™ SIEMStorm™

Rapidly identify and resolve threats... streamline compliance... and transform volumes of security data into understandable, ***actionable*** information – all with the power of BlackStratus SIEM Storm.

Your business depends largely on the management of information across your organization – from customer records to critical corporate financial data. And without sophisticated measures to protect all enterprise data from security threats, you can put your business processes, regulatory compliance efforts, and even financial security at risk. Yet company-wide security management has a reputation for being highly complex, not to mention costly, especially for companies with limited IT budgets and resources.

To be effective, security information management (SIM) solutions need to deliver the right return on your technology investment – a robust, streamlined, cost-effective method for centrally managing security strategies and security information. BlackStratus SIEM Storm puts the power of SIM technology within your reach. With BlackStratus SIEM Storm, you can counteract emerging threats and streamline your compliance processes – with an easy-to-use, affordable security solution that can be managed with minimal on-staff IT security personnel.

Through patented SIM software technology and a uniquely powerful architecture, BlackStratus SIEM Storm provides the sophisticated capabilities you need from a SIM solution, but without the complexity of deployment and resource demands of existing SIM solutions. Plus, BlackStratus SIEM Storm enables you to scale the solution easily, so you can expand your security management needs as your business grows. With an unprecedented level of automation, real-time monitoring, enterprise-wide visibility, and actionable intelligence, BlackStratus SIEM Storm empowers you to continually ensure the integrity and privacy of your critical data.

The only SIM solution to fully integrate with HP's uCMDB, BlackStratus SIEM Storm ensures seamless data integration with ITIL framework's Configuration Management process. Enterprises can now be assured that their security information management system is up-to-date and gain a real-time comprehensive view of their organizations security posture.

www.BlackStratus.com

Real-time Threat Identification Ensures a Rapid Response.

BlackStratus SIEM Storm uses real-time threat identification technology to rapidly sift through massive amounts of security data and extract the relevant information you need to protect your most valuable assets. By tying together diverse and disparate events across the network, BlackStratus SIEM Storm uncovers suspicious patterns and anomalies that would otherwise be missed. State-of-the-art visualization and reporting enables you to identify, track, and analyze incidents, and delivers actionable security information to the appropriate people before the threat becomes a costly attack. An integrated remediation workflow ensures an effective and consistent response.

Address Compliance Requirements Cost-effectively.

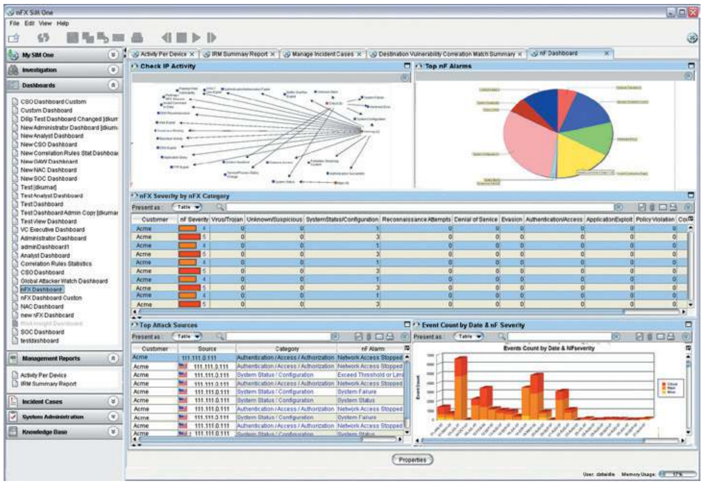
BlackStratus SIEM Storm addresses a multitude of regulations based on industry standards such as COBIT – so you can successfully and cost-effectively demonstrate a sound framework for the most important aspects of regulatory compliance. A comprehensive suite of monitoring, analysis, and reporting tools ensures that you can monitor the performance and effectiveness of your security controls. With comprehensive compliance reporting, you have the documentation you need to meet auditors' demands. Unlike other SIM solutions, BlackStratus SIEM Storm provides a clearly defined and repeatable process to ensure the quick and accurate handling of security incidents.

As your organization grows in size and complexity, you must have the ability to efficiently and cost-effectively extend your SIM solution. That's why we designed BlackStratus SIEM Storm to easily scale right along with your changing business requirements, dramatically reducing your total cost of ownership. Because your growing SIM infrastructure easily incorporates data from new devices, applications, and databases, you can also scale your comprehensive security visibility.

BlackStratus SIEM Storm makes scalability possible because it's the only SIM solution built on a multi-tiered, distributed architecture. The BlackStratus SIEM Storm architecture also delivers the full failover and redundancy required to ensure that analysts and operators are never down. This means you never miss events that might constitute policy or regulatory compliance violations – or events that can cause downtime and information loss.

Multiple Correlation Technologies Ensure that Threats are Identified Rapidly.

BlackStratus SIEM Storm identifies suspicious patterns that would otherwise go unnoticed. Multi-dimensional correlation delivers unprecedented security visibility by tying together diverse security activities across the network. BlackStratus SIEM Storm is designed to efficiently process the high volume of data that comes from security and network devices, core applications, and databases. Only BlackStratus SIEM Storm provides this powerful, all-in-one correlation capability for addressing historical, real-time, and potential threats.



BlackStratus SIEM Storm provides a complete view of enterprise security posture and rapidly identifies suspicious patterns of activity that would otherwise go unnoticed. Multiple views of actionable security information are tightly integrated with reporting and analytics to intuitively pinpoint threats in real-time.

Rules-Based Correlation

The BlackStratus SIEM Storm rules-based correlation engine can perform 100 million state checks per second, so you can handle massive amounts of data when effectively monitoring applications, databases, and perimeter devices in real time. Importantly, BlackStratus SIEM Storm allows users to apply conditional logic to identify likely attack scenarios. BlackStratus SIEM Storm is the only SIM solution to implement multi-state rules that require meeting a series of conditions within a specified time period prior to an alert being issued. This protocol reduces the number of rules security analysts must write and maintain – since rules for a particular vulnerability can be nested – and also reduces the number of false positives.

Vulnerability Correlation

BlackStratus SIEM Storm is one of the only SIM solutions that supports vulnerability correlation without writing rules. Security teams can immediately reap the benefits of vulnerability correlation, identifying potential threats to high-value assets by correlating scanner and IDS data. Security personnel can also prioritize patching efforts to reduce risk without losing time writing and maintaining rules.

Statistical Correlation

BlackStratus SIEM Storm applies statistical algorithms out-of-the-box to automatically determine incident severity, assigning a threat score based on asset value. Statistical correlation analyzes network behavior and identifies threats based on the presence and severity of anomalous event patterns.

Historical Correlation

With historical correlation, security analysts can identify repeating patterns of attacks, as well as automated and slow attacks that may be veiled within millions of raw security events. Historical correlation allows for quick detection of previously unrecognized malicious events, adding another level of defense to your security program. With the ability to review past events, analysts are better positioned for real-time detection of future zero-day attacks.

BlackStratus SIEM Storm Provides Real-time Monitoring and Threat Identification with State-of-the-Art Security Visualization and a 'Seamless' Workflow.

A revolutionary new usability and workflow design makes BlackStratus SIEM Storm the most easy-to-use interface available today, enabling users to quickly and easily identify and respond to security issues. The powerful new suite of visual tools makes it easier than ever to access all security information faster through high-level views of overall security health. Analysts can quickly differentiate false positives from real threats, understand the exact nature and scope of a threat, and make sure that vulnerabilities are mitigated before a threat can proliferate.

Intuitive Graphical User Interface

BlackStratus SIEM Storm features an all-new graphical user interface (GUI) that is powerful yet easy-to-use. Users can quickly access the information they need – with fewer clicks to actionable intelligence. From the GUI, operators and analysts can easily open, investigate, assign, edit, and close security incidents. They are guided through the steps necessary to create and resolve virtually any security incident. BlackStratus SIEM Storm puts the most important information at the analysts' fingertips and ensures a seamless security event workflow.

Risk Insight Dashboards

With Risk Insight Dashboards, you gain access to real-time snapshots of your organization's overall security health based on security-related data from across the enterprise. You can measure deviations from the risk baseline and get instant, visually intuitive access to the metrics, reporting, baseline, and investigative information needed to manage risk and ensure that security standards are met.

Link Maps

This invaluable tool allows you to visualize relationships among different assets under attack, and identify the target, type, and method of the attack. Users can clearly see the course of an attack as it propagates across a network, and drill down on a specific asset at any time to get more detailed information.

Geo Map

The geo map monitors events by country and city, flags suspicious traffic from specific countries, and pinpoints suspicious sources down to a specific longitude and latitude.

Device Status View

Easy-to-view and analyze, agent count charts provide you with real-time visibility into the status of collectors across the network. These tools also allow you to configure remote collectors from the security operations center.

Global Threat Dashboard

At a glance, you can view correlated attacker information through an easy-to-understand dashboard and determine if your organization is under attack from one of the top 10 emerging attack sources.

The Most Powerful SIM Reporting Available Today. Bar None.

BlackStratus SIEM Storm delivers a wide and rich range of security and compliance reports based on comprehensive data from devices, applications, and databases. BlackStratus SIEM Storm integrates industry-leading Business Objects (Crystal Reports) reporting to ensure that users have the most powerful and full-featured SIM reporting suite available today. A multitude of reports provide a real-time picture of security posture and ensure that compliance requirements are being fulfilled. Simply collecting raw log data isn't enough – your power comes from how the data is leveraged for compliance, security, or operational business reporting.

Richer, More Flexible Reporting

BlackStratus SIEM Storm's rich reporting environment allows security teams to generate reports that incorporate real-time and historical data. Reports are seamlessly integrated with analytics and data visualization to provide a comprehensive understanding of an organization's security picture at any point in time. Reports measure everything from risk exposure to compliance, and custom reports allow users to get tailored information. Role-based dashboards meet specific information needs of analysts, operators, and executives. BlackStratus SIEM Storm excels at enabling the rapid and accurate analysis of real-time security event data, giving users the tools and capabilities they need to analyze and report on security, log, and application data for security policy and compliance monitoring.

Regulatory Compliance Reporting

BlackStratus SIEM Storm includes a standard suite of operational and executive reports that address key compliance regulations such as Sarbanes-Oxley, HIPAA, FISMA, GLBA, and PCI. Operational reports create a prioritized view of threats against compliance asset groups. Executive reports and dashboards show overall security posture, vulnerability, and incident management trends.

Role-based Reporting

An array of pre-packaged report templates for analysts, operators, and executives enables the rapid and granular assessment and mitigation of all possible risks.

Policy Compliance Monitoring

When implemented as part of an integrated policy compliance directive, such as Cisco's Network Admission Control initiative, real-time security policy compliance monitoring denies vulnerable machines access to the network until appropriate patches and updates have taken place.

Powerful Analytics with Integrated Charting

Next-generation analytics allow users to slice and dice security data and view it intuitively using multiple dimensions of data in a familiar pivot table format. Data mining also allows analysis of events based on specific criteria to identify anomalous incidents. As a result, analysts can now pinpoint previously undetectable raw event details in a comprehensive, console-style view.

Detailed MSSP Views and Reporting

For managed security service providers (MSSPs), BlackStratus SIEM Storm provides important capabilities that ensure the maintenance of secure and compliant operations. MSSPs can do more than just monitor an organization's security infrastructure; now they can also manage security risks, with comprehensive views of risk exposure and policy compliance posture. MSSPs gain an independent perspective on the security posture of each customer's organization or across multiple organizations with IP overlap and true private IP address support.

A Fully Integrated Incident Resolution Workflow Based on Industry Best Practices.

By integrating the SANS Six-Step Incident Response process, BlackStratus SIEM Storm guides teams through a proven process to fully eradicate threats. Users are assured that each incident is handled with a rigorous, defined, documented, and complete process. Preconfigured incident templates and customizable resolution procedures simplify the incident resolution process.

Policy Compliance and Remediation

BlackStratus SIEM Storm takes information related to policy violations and closes the loop by triggering a workflow that allows teams to contain and remedy violations. BlackStratus SIEM Storm simultaneously ensures that vulnerable systems apply appropriate updates and definitions.

Evidence Retention

Virtually any document, image, report, chart, or other relevant data can be attached to an incident case. Other files, such as scanned images, audio interview records, and traffic captures may also be added to cases and are cryptographically check-summed upon insertion to ensure the integrity of the evidence.

Role-Based Access and Incident Collaboration

Incident cases may be assigned to different users and shared among a group. Granular access controls can be applied to case data so that several analysts may collaborate on a case while maintaining important "need to know" authorization structures. Additionally, all actions performed by system users are recorded in audit logs.

Help Desk Integration

BlackStratus SIEM Storm's incident resolution management process integrates with help desk products including HP Service Desk, Remedy, and Peregrine to facilitate communication with the network operations and change management groups that own the patching process.

Embedded Security Knowledge Base: More Knowledge. More Secure and Compliant Operations.

To be effective, your team must understand the characteristics of attacks and take proper and timely containment and remediation steps. The embedded security Knowledge Base provides valuable guidance by eliminating the need to perform hours of research from a variety of external sources on vulnerabilities and threats.

Integrated with all of the functional areas of BlackStratus SIEM Storm, the Knowledge Base ensures that vulnerability information, compliance guidelines, and remediation procedures are never more than a click away. Operators and analysts get a continual flow of relevant and actionable information to pinpoint attacks – enabling them to provide containment and remediation steps to network and configuration managers.

Teams get even more specific response information in the event of a recurrence because the Knowledge Base can be updated with organization-specific data, such as information about a previous incident. BlackStratus' dedicated team of experts publishes bimonthly advisories to the Knowledge Base on the latest security threats.

About BlackStratus

BlackStratus delivers security compliance solutions that help stop the ever-increasing attacks that threaten organizations. Through its patented BlackStratus technology, BlackStratus not only solves security compliance challenges, but provides the proof needed to address the myriad of regulatory and internal governance requirements. The BlackStratus' suite of solutions enables governments and organizations to address external and internal threats, mitigation, log management and reporting. Governments and companies of all sizes around the world rely on BlackStratus to gain unparalleled security visibility, prevent costly downtime, and achieve and maintain compliant operations.

For more information on BlackStratus SIEM Storm – and the suite of BlackStratus security and compliance solutions – please call 732-393-6000 or e-mail info@blackstratus.com

BlackStratus™