The BMC Approach to SIEM:

Cross-platform event log management and correlation
# Table of Contents

1. YOUR ORGANIZATION’S POTENTIAL FOR A MAINFRAME BREACH .............................................. 1

2. OUR ABILITY TO DO THREE THINGS VERY WELL SEPARATES THE BMC SIEM EXPERIENCE FROM MANY OF OUR COMPETITORS IN A CROWDED MARKETPLACE ............................................. 2

3. DISTRIBUTED APPROACH TO LOG MANAGEMENT AND CORRELATION ................................................. 2

4. THE BMC SIEM ARCHITECTURE ........................................................................................ 2
   - Web Server Apps, IDS, Anti-virus
   - Linux & UNIX Servers
   - Routers/Firewalls
   - Windows Active Directory
   - SAP Activity
   - SQL Databases/Log Files
   - IBM z/OS Mainframe
   - Virtual Log Management & Correlation
   - Features

5. INSTALLATION REQUIREMENTS .................................................................................. 4
   - Features
Your organization’s potential for a mainframe breach

The BMC SIEM Server provides a standards-based method of collecting all the system log messages of your network using industry standard syslog protocol and SNMP traps. These messages are then correlated into understandable threats, alerts, and actions using sophisticated, easily configured rules, which are then reduced to actionable “tickets” that are sent to administrators as a trigger for remediation of incidents.

BMC SIEM accepts any standard syslog (RFC 3164 or 5424) data generated by UNIX platforms, routers and various enterprise applications. Additionally, BMC provides software agents that can convert non-standard proprietary message logs to syslog format from Microsoft Windows, IBM® z/OS, Linux, Linux on z, and Macintosh operating systems, including an agent for SAP®.

BMC SIEM system runs as a Windows service, with a standard web browser UI, and consumes minimal system resources. The entire BMC SIEM package can be downloaded in about 30 seconds on a modest 10 Mbps Internet connection. With its ability to collect and reformat disparate log data to industry-standard syslog protocol for SIEM, BMC provides system-wide interoperability unmatched by rival, competing SIEM vendors.

For regulatory compliance, BMC SIEM was architected to facilitate standards set forth by PCI DSS, HIPAA, SOX, GLBA, FISMA, and many other industry requirements and provides out of the box compliance scorecards. BMC SIEM’s archival and storage functionality provides up to 5,000 days of storage and uses encrypted checksums for file integrity. With no additional software required, BMC SIEM employs authentication and AES 256 encryption between agent programs and the BMC SIEM. Any BMC site requiring U.S. Government compliance will be secure through a FIPS 140-2 certified cryptographic module that provides secure transactions between all deployed agents and the main BMC SIEM.

BMC SIEM also ships with many packaged reports templates designed with auditors in mind. These reports can be easily customized to fit users’ requirements and BMC SIEM can be set up to send reports to any e-mail address at any scheduled interval.
OUR ABILITY TO DO THREE THINGS VERY WELL SEPARATES THE BMC SIEM EXPERIENCE FROM MANY OF OUR COMPETITORS IN A CROWDED MARKETPLACE:

1. **We deliver best-in-class event log monitoring and correlation**: BMC SIEM correlates syslog messages employing automated event management and self-learning algorithms to uncover user behavior indicative of threat. When an alert is generated, BMC SIEM creates an actionable ticket, which can be reflected in a help-desk, or used in e-mail or other notifications. The BMC correlation engine consumes minimal resources yet is capable of receiving burst traffic of up to 20,000 messages per second.

2. **We expand SIEM capabilities with agent technology for virtually every platform**: BMC can aggregate syslog messages into a single security system in real-time from a myriad of diverse systems including Windows, UNIX, Linux, Linux on z Systems, IBM z/OS, Macintosh and SAP, plus log-generating devices such as routers and firewalls. The security console that receives the log data can be the BMC SIEM or other SIEM product.

3. **We provide simple installation and implementation**: The BMC SIEM package takes about 30 seconds to download on a 10 Mbps connection. Within just a few minutes the BMC SIEM console is receiving user/system log data, correlating event logs for any sign of potential threat, ready to alert.

**DISTRIBUTED APPROACH TO LOG MANAGEMENT AND CORRELATION**

At the heart of the BMC SIEM Correlation engine is a distributed management approach to message transmission that reduces large amounts of random, aggregate log data into smaller amounts of pertinent and actionable data. One or more instances of BMC SIEM continuously gathers log data from devices and agents in real-time. This log data is stored, filtered through an advanced correlation engine and monitored for anomalous threat patterns.

When a threat is detected, the system creates an internal ticket, viewable to BMC users which can trigger specific actions ranging from simple e-mail notifications to sending a message to the help desk warning of the threat. Consequently a ticket can be created in your help-desk, or can be sent to a higher level SIEM system, BMC or other. BMC SIEM can operate in an “unattended mode,” operate as a correlation component in a larger log management strategy, or operate as the central security console of your enterprise.

The result is a highly scalable and flexible architecture that supports log aggregation, filtering, correlation, real-time notification, a trigger for remediation, as well as a full suite of forensic tools and reporting functions — all in one easy-to-use package.

**THE BMC SIEM ARCHITECTURE**

**Web Server Apps, IDS, Anti-virus**
BMC SIEM monitors a variety of applications, including third-party anti-virus systems, IDS systems, HTTP servers, mail servers, and other infrastructure assets in your enterprise. BMC also includes a simple SDK that lets you extend the range of what you want to monitor.

**Linux & UNIX Servers**
BMC SIEM monitors Linux and UNIX syslog data via standard agentless syslog, or via special BMC agents. This provides the ability to flag suspicious messages such as unauthorized access attempts, and track user access to these systems.

**Routers/Firewalls**
BMC accepts real-time syslog data from routers and firewalls, looking for anomalous data and failed access attempts. BMC SIEM includes a “geo database” of IP addresses, to track the location of all access attempts to specific countries.

**Windows Active Directory**
BMC SIEM monitors AD for user and account changes, as well as tracks user logons, logoffs, lockouts, failed logons, and other user activity.

**SAP Activity**
BMC SIEM provides an agent that is specific to SAP, which monitors a variety of SAP messages and events, including user logons, logoffs, and other access items.
SQL Databases/Log Files
BMC SIEM provides techniques and adapters that permit special visibility to SQL databases through ODBC connections and log file monitoring.

IBM z/OS Mainframe
BMC SIEM provides a software agent for z/OS that intercepts, in real time, RACF, ACF2, Top Secret, DB2 accesses, CICS, IMS, TCP, FTP, TSO plus other events and reformats the mainframe messages to syslog protocol for the BMC SIEM or a number of other SIEM systems.

BMC’s SIEM Agent has certified integrations with IBM® Security QRadar®, HP ArcSight, and a strategic partnership with McAfee. SIEM Agent has field integrations with many other leading SIEM solutions including Splunk® and LogRhythm.

Virtual Log Management & Correlation
The BMC SIEM can receive VMWare vCenter and vSphere syslog files in the BMC SIEM correlation engine and monitor security threats as if monitoring a physical server. Because vCenter is a centralized cloud platform and generates a syslog format native to SIEM, BMC SIEM is capable of receiving and correlating virtual Windows, Linux and UNIX event logs from the VMWare platform.

Features
• Pure software browser-based solution: Deploys across a small footprint and consumes minimal system resources. The complete system downloads in less than 30 seconds on a 10 Mbps connection. It is a pure software solution viewable on any web browser.
• High-speed search and correlation: Uses an advanced correlation engine, which performs semantic analysis of your messages in real-time.
• High-speed message reception: Can process more than 10,000 messages per second and can handle burst traffic of more than 20,000 messages per second.
• Automatic response for fast remediation: Incorporates a simple, extensible “actions” capability that allows targeting specific messages based upon device, keyword, facility, severity and/or time of day. The solution can run programs on that data including updating relational ODBC databases, relaying syslog messages, send SNMP traps, and then send e-mail alerts, or create helpdesk notifications and other actions.
• Flexible reporting: Delivers a host of bundled reports for threat detection and cyber-forensics right out of the box. These reports facilitate compliance requirements set forth by PCI DSS, HIPAA, SOX, FISMA, GLBA and many other standards. These reports can be easily customized to fit management requirements.
**INSTALLATION REQUIREMENTS**

The BMC SIEM Correlation Server requires Windows Vista, Windows 7, Windows 8, and Windows 20xx workstation or server platforms. There are no hard limits on CPU, disk space, or memory resources. The BMC SIEM download package incorporates the Apache HTTP server, easy Windows-based installation setup, a ready-to-run configuration, and a comprehensive user manual.

The system also includes a copy of the BMC Syslog Windows Tool Set with a user manual so users can easily add Syslog capability to an existing Windows platform, making the BMC Security Server fully enterprise-capable.

Additional information on installation requirements for all BMC products may be found at [BMC.com/support.html](http://BMC.com/support.html).

**Features**

- **Data aggregation and archiving**: Can collect in excess of 50 Gigabytes of data each day at a single site, and save this data online for up to 500 days (given enough storage.) The system can compress and archive data for a period of more than 10 years (5000 days).

- **Input filtering**: Filters input data by device, facility, severity, message keyword, time of day, or any combination thereof. Filtered data can be discarded, or put into a separate repository (and possibly permanently archived) for further analyses or forensics.

- **Improved syslog categorization**: Syslog protocol “facility” codes, which define the data sources for syslog messages, are limited to 24 predefined categories. BMC SIEM removes this restriction, permitting users to define their own facilities, such as “applications,” and “devmsgs,” so that data can be better categorized and managed. Also expands syslog message categorization and correlation, not otherwise available using the standard specification.

- **High-speed search**: Uses a proprietary data extraction program that employs high-speed, real-time indexing. Users can search a terabyte of data for a particular keyword in less than one second.

- **Taxonomy, ontology, and cataloging**: Automatically catalogs information by IP address, username, facility, and severity. Users can further create catalogs of information based upon simple or complex match patterns bringing flexibility in managing and grouping message data, while maintaining high data throughputs.

---

**FOR MORE INFORMATION**

To learn more about BMC AMI for Security, please visit [bmc.com/ami-security](http://bmc.com/ami-security)