CARETOWER'S SIEM MANAGED SECURITY SERVICES

ENTERPRISE SECURITY MANAGER MSS -TRUE 24/7 SERVICE

CARETOWER
An Integrity360 Company

CHALLENGES & SOLUTION

Challenges

During recent times, organisations all over the globe are facing many challenges irrelevant of size or vertical when it comes to Security Information and Event Management (SIEM) solutions.

ADVANCED PERSISTENT THREATS

Many organisations have implemented a defence in depth strategy around their critical assets using APT, firewalls and IDS/IPS at the perimeter, two-factor authentication, internal firewalls, network segmentation, HIDS, AV and as well as other technologies. All of these devices generate a huge amount of data, which is difficult to monitor. A security team cannot realistically have all these dashboards open and correlate events among several components fast enough to keep up with the packets traversing the network.

COMPLIANCE

Almost every business is bound by some sort of industry regulation such as PCI-DSS, GPG13, ISO27001/2, HIPAA, SOX. Attaining and maintaining these regulations is a daunting task. Virtually every regulatory mandate requires some form of log management to maintain an audit trail of activity.

ZERO-DAY THREAT DETECTION

New attack vectors and vulnerabilities are discovered every day. Firewalls, IDS/IPS and AV solutions all look for malicious activity at various points within the IT infrastructure, from the perimeter to endpoints. However, many of these solutions are not equipped to detect zero-day attacks.

OPERATION SUPPORT

The size and complexity of today's enterprises is growing exponentially, along with the number of IT personnel to support them. Operations are often split among different groups such as the Network Operations Centre (NOC), the Security Operations Centre (SOC), the server team, desktop team, network team etc.

Each with their own tools to monitor and respond to events. This makes information sharing and collaboration difficult when problems occur.

FORENSICS

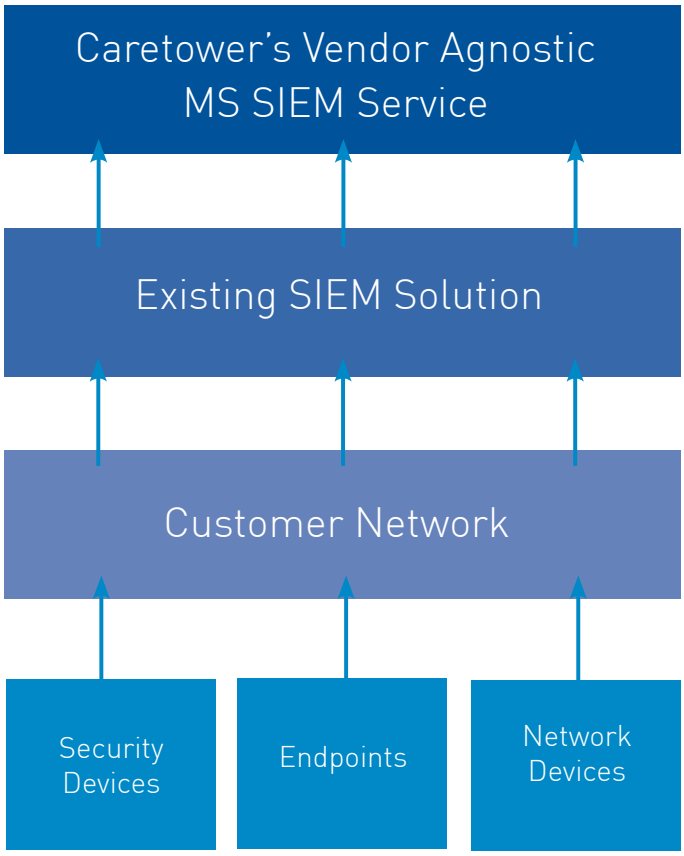
Not only must a forensics analyst interpret log data to determine what actually happened, the analyst must preserve the data in a way that makes it admissible in a court of law. Since log data represents the digital fingerprints of all activity that occurs across IT infrastructures, it can be mined to detect security, operations and regulatory compliance problems.

Whether it is the challenges of managing many disparate devices across different locations or having to face a cyber attack in the ever growing threat landscape, systems are compromised and affected with data being taken, along with the complexity of adhering to and maintaining industry driven compliances. These factors are major concerns for businesses as they are difficult to combat which need to be addressed and overcome in an effective and timely manner.

Solution

Caretower's Security Information and Event Management (SIEM) service collects, analyses and stores logs from networks, hosts and various applications. SIEM allows clients to:

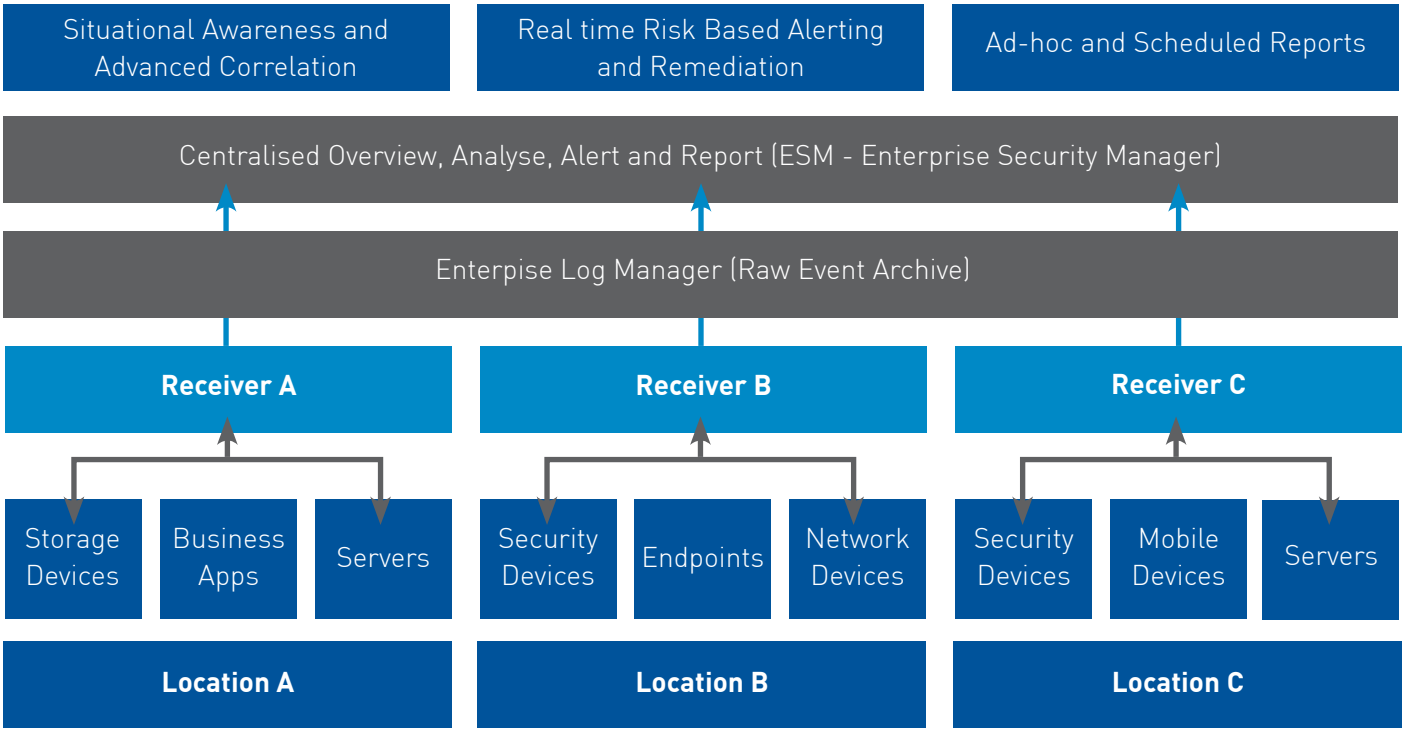
- **Collect logs from multiple locations into a central system:** This enables numerous receivers to feed into one central system for monitoring and reporting.
- **Summarise key incidents:** Critical events and alarms are reported to the client, in turn decreasing the period and resource.
- **Correlate critical events:** A pro-active holistic approach that ensures threats are identified where individual devices alone may not detect them.
- **Report on incidents:** A full reporting engine and dashboard is built into the Caretower's MSS SIEM service, providing clients with a real-time visibility and historic reporting activity.
- **Take immediate and suitable remediation activities:** This minimises the implication of threats on our client's network and allows our Incident Response Team to take immediate action.



SIEM MANAGED SECURITY SERVICES

SIEM MANAGED SECURITY SERVICES ARCHITECTURE

In the architecture diagram below, multiple receivers from multiple locations collect logs from various devices and ELM (Enterprise Log Manager) and ESM (Enterprise Security Manager) fetch these logs from the receiver periodically. ELM Stores the RAW logs mainly for compliance purposes and ESM uses normalised logs for reporting, correlation and alerting.



SIEM MANAGED SECURITY SERVICE

We can host the solution or the solution can reside within our customer's network. We wrap our services around either option which offers flexibility of architecture and management. We monitor security events 24/7 and provide in-depth security expertise. We also provide reports on spot-patterns across a number of customers to provide advanced warning on new threats.

- Proactive management
- Run by dedicated and industry leading certified security engineers (GIAC Certified Forensic Analyst) – GCFA
- SOC Engineer's vendor certified
- Escalation from tier 1 to tier 3 engineers
- 24/7 x 365 SOC cover
- Fully ISO27001 accredited SOC

- Service based on ITIL3 framework
- Customer oriented, process driven and service driven
- Transition, incident, problem and change management
- Portal access for incident and change management
- Multiple logins available for customer staff
- Change requests initiated by SOC or by the customer
- Incident tickets raised in management system automatically or manually via web portal
- Email notification of tickets raised and updated
- Bi-weekly/monthly reports generated for customers
- SLA - Measurable Escalations – industry leading SLAs
- Incident Response - SANS (SysAdmin, Audit, Networking, and Security)

INCIDENT RESPONSE

- Receive alerts in real-time
- Perform investigation using SIEM, based on log information
- Provide security reports with expert advice within SLAs
- SLAs depend on the business impact for the inbound alerts.
- Different SLAs are implemented for traditional support (change requests, patching, upgrading, etc.) and incident response (advice on alerts) and work through a remediation
- Remediation plan and infrastructure recommendations
- Change requests
- Fully logged and reports for audit trail

MINIMISE OPERATIONAL EXPENDITURE

- Improve productivity/effectiveness of the solution
- Maximise your investments
- Help achieve compliance
- Traditional monitoring and support
- Maintenance of rules and reports
- Offer agility and flexibility
- Reduce Internal Resource and Training Costs
- Gives you peace of mind that your security is safely managed by a team of experts 24 hours a day

VALUE TO CUSTOMERS

- Improve your security posture within your environment
- Threat Awareness
- Real-Time Trending
- Proactive Maintenance and Monitoring
- Risk Mitigation

RECOMMENDATIONS TO CUSTOMERS

- Deploy Base-Line configuration based on NIST Top 20 Security Controls
- Based on common IT security best practices
- Perform accurate tuning of the correlation - engine/rule's based on the customer's specific use cases
- Based-lined configuration support
- Tuning of the out-of-the-box features

CUSTOM AND COMPLIANCE REPORTS

- Implemented during the design phase
- Maintained later on by the Security Operations Centre

SIEM OR MSSP? - COMPARING CAPABILITIES

Features	SIEM	MSSP
Monitors log events	☑	☑
Helps attain regulatory compliance	☑	☑
Flexible service delivery		☑
Provides 24/7 analysis by security analyst		☑
Stores logs off-site in forensically-sound facility*		☑
Provides security intelligence and expertise as part of the solution		☑
Built-in disaster recovery and business continuity planning (DR/BCP)		☑
Predictable fixed cost		☑
May require additional infrastructure (server, network devices, storage, etc.)	☑	

*Optional store raw log data on customers' premises, which may involve additional cost, and where it may not be protected against alteration or theft.

BENEFITS OF CARETOWER'S SIEM MANAGED SECURITY SERVICE

SPEED OF IMPLEMENTATION

Our SIEM Managed Security Service seamlessly integrates with your network and can be up running within days, not months. We deliver instant results through visibility of events and analyse on a live dashboard with in-depth reporting.

SIMPLIFIED COMPLIANCE

Our SIEM Managed Security Service enables companies to fulfil their compliance requirements by providing you with on demand, enterprise-wide reports that demonstrate the security status of your systems. The SIEM service can provide auditing against the following industry standards (e.g.):

- PCI DSS Compliance
- ISO 27001
- Protective Monitoring (GPG13)
- SOX
- HIPAA
- PSN

FLEXIBLE DASHBOARDS AND ROBUST REPORTING

Our SIEM Managed Security Service brings you comprehensive technical, operational and trend reports that communicate security status and satisfy compliance requirements. Dashboards are available out-of-the-box and Caretower delivers customisable dashboards to each and every customer based on their requirements.

24/7 CARETOWER SECURITY OPERATION CENTRE

Our SIEM Managed Security solution allows you to be a SIEM user, not an administrator. This means that you have access to SIEM to view the data and run required reports whilst maintaining a certain level of privileges. The SIEM service is constantly monitored by our 24/7 Security Operations Centre where the team will carry out monitoring, management and incident response to security events and alerts.

WHY CARETOWER?

As an independent IT security specialist, with over 17 years experience, Caretower provide comprehensive solutions to individual problems, thus allowing our recommendations to be unbiased. Over the years, we have quickly established many long standing relationships with all of our vendors, achieving the highest status within these organisations based on the level of expertise within our internal sales, support and professional services teams.

This relationship ensures we provide our customers with key changes within the industry which assists in their on-going security management strategy.

- To provide live 24/7 McAfee SIEM Managed Service in Europe
- Dedicated GIAC Certified Digital Forensic Security Engineers (SANS (SysAdmin, Audit, Networking, and Security) Institute)
- Full-onsite and hosted architecture options, depending on your requirements
- We are CSA (Cloud Security Alliance) member and ISO 27001 Accredited

GET IN TOUCH:

020 8372 1000

INFO@CARETOWER.COM

WWW.CARETOWER.COM