EzeCastle INTEGRATION

Eze Managed SIEM

As threat actors continue their highly profitable, and relentless barrage of attacks on businesses, information technology (IT) vendors are diligently working to deliver hardware and software products that provide critical security data in the form of log files, alerts, messages etc.

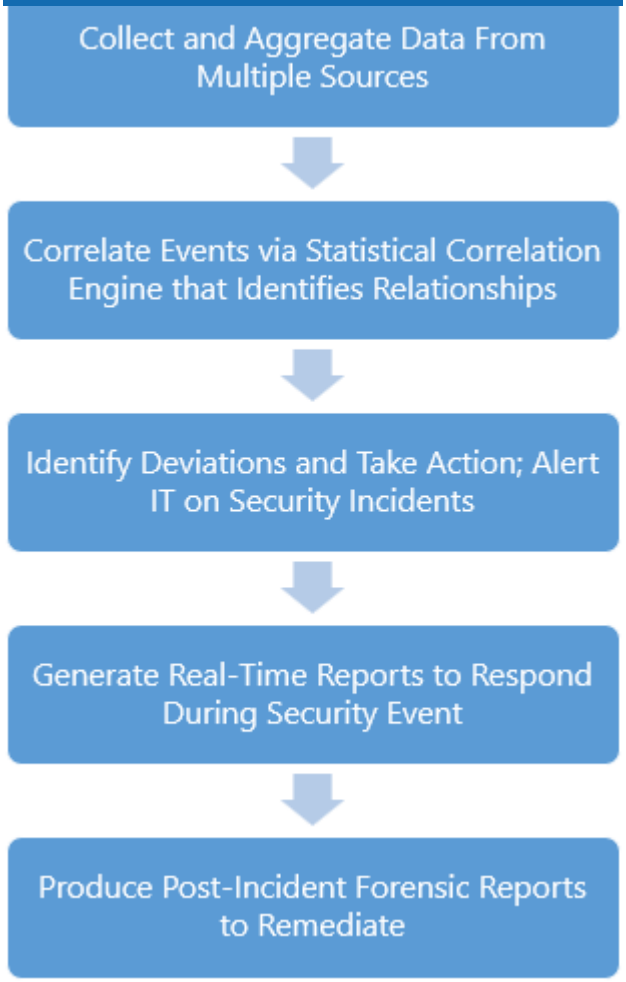
The goal is to arm end users with the data they need to reverse the trend of operating in a reactive, damage control mode because they're seemingly always one-step behind the cyber-attackers.

However, as is frequently the case with technology, the pendulum has swung from not having enough security-oriented data to having too much and unfortunately, not all the data is helpful or relevant. Too much data can lead to delays in performing preventative measures.

But how are businesses supposed to sift through the mountains of data to determine what is meaningful? This task is impractical and not one that is in line with most businesses' strategies.

This is where **Eze Managed SIEM** (security information and event management) service comes in.

How SIEM Works



Eze Managed SIEM

The Eze Managed SIEM provides real-time security analysis of data to proactively identify potential security risks. Machine learning technology is used to apply correlation algorithms that systematically transform raw data into useful information.

Eze Managed SIEM efficiently provides statistical analysis of data to identify anomalies, patterns, and trends which might indicate a current or future security risk. Log file and alert data is rapidly ingested, parsed, normalized, indexed and enriched using relevant third-party data.

The Eze Managed SIEM service was designed from the ground up to ensure all information is filtered through a Security Operations Center (SOC) to eliminate "the noise," resulting in the succinct reports and recommendations that our clients need to address cybersecurity challenges.

Features & Benefits

- **Deployment:** A successful SIEM implementation relies on a deployment plan that covers enough breadth – making sure that all supported sources send their logs to the SIEM – and depth – making sure that all supported sources are configured to capture all relevant logs with the right level of verbosity.
    - With 22 years of experience in IT systems architecture and engineering, Eze Castle Integration can uniquely ensure successful implementation of a complex SIEM platform that adheres to regulatory standards (GDPR, NYDFS, OCIE) and cybersecurity guidelines such as ISO27001, NIST, CIS.
- **Systems Integration:** From workstations and servers to applications and cloud platforms, Eze works to integrate systems and technologies that matter most to our clients.
- **Visibility:** Clients have visibility into security events and incidents through their Eze Castle client portal/dashboard.
- **Response:** Armed with the knowledge and expertise in cybersecurity, Eze staff provide 24x7x365 support in handling of alerts, filtering out the noise, and responding to actionable events in a timely manner.
- **Customization:** Eze can create custom alert definitions based on industry best practices, regulatory compliance requirements, and our clients' needs.

Solution Highlights

- Powerful single endpoint agent installs in seconds
- Complete data collection, regardless of structure of data capture
- Monitor end points for running process and behaviors
- Fine-grained risk scoring via intelligent data analysis for thousands of indicators of potential attack situations
- Systems are evaluated against best practice standards and regulations
- Endpoint analysis for weak configurations and improvement recommendations
- 24x7 Security Operations with rapid triage by Eze Castle Integration

About Eze Castle Integration

Eze Castle Integration is the leading provider of managed services and complete cloud solutions to the investment industry. The company's products and services include Technology Consulting, Outsourced IT Support, Eze Cloud Services, Cybersecurity Solutions, Business Continuity Planning and Disaster Recovery, Project and Technology Management, Telecommunications, Archiving, Storage, Colocation and Internet Service. Eze Castle Integration is headquartered in Boston and has offices in Chicago, Dallas, Hong Kong, London, Los Angeles, Minneapolis, New York, San Francisco, Singapore and Stamford.

Learn more by calling +1 800-752-1382 (US), +44 207 071 6802 (UK) or visiting www.eci.com.