Regency Protect

Regency IT Consulting have been providing Protective Monitoring expertise to clients from our earliest days and our fully Managed Service 'Regency Protect', since early 2007.

During this time we have deployed and used many of the leading SIEM (Security Incident and Event Management) products as well as developing tools and scripts of our own. Together, these tools and the experience of our staff allow us to tailor protective monitoring solutions to the specific business requirements of our clients whether they be Government Departments working with Good Practice Guide (GPG) 13 and concerned about the protection of Government protectively marked or personal data on their systems, or commercial enterprises having to meet PCI-DSS or Sarbanes Oxley reporting requirements.

The challenges of protective monitoring and the Regency Protect approach

There is no 'one size fits all solution' - no single appliance or software tool will meet all requirements. We work with our clients to ensure the service we offer compliments your business requirements whilst meeting the security and reporting needs.

'Accounting logs are not uniform' - we use a range of scalable tools to capture all logs relevant to your business and then pass them through a correlation and reporting tool to provide comprehensive reporting in line with business requirements.

What about large volumes of accounting data? We retain all data securely for an agreed period of time and use intelligent filtering tools to highlight anomalous activity. Logs can either be shipped to our SOC for storage or kept on the client site and analysed remotely over a secure link.

Sometimes we hear "We have more than one business critical system." We can correlate information from multiple systems and produce single reports or report on systems independently if preferred.

Within a busy organisation where resources are limited and technical expertise to implement complex monitoring solutions is either not available or does not exist, the Regency Protect solution can provide a service that fulfils the regulatory or policy requirements with minimal business effort. This allows the business and IT departments to focus on what adds value to their products.

Why use Regency Protect?

For some, the use of protective monitoring is necessary requirement in order to meet a

mandatory standard (PCI-DSS, HMG Standards, etc); others recognise it as providing defence in depth forming an integral component in their suite of defensive tools and processes. One of the primary benefits is that protective monitoring provides situational awareness of activity on the monitored system but, should the unthinkable happen, it is also essential in the effective response and management of security incidents and provides objective evidence to support the damage assessment allowing you to state where and when specific data records were accessed, and who by. Above all however, a well run and publicised protective monitoring regime acts as a significant deterrent to those who may be thinking about attacking systems or misusing data.

Additional Benefits

As well as providing significant benefits to the confidentiality and integrity of system data, a well run protective monitoring regime can help in the detection of non-security related system errors such as system misconfigurations and component failures. Coupled with the bandwidth monitoring capabilities, Protective Monitoring can help to provide increased system efficiencies and provide information required for capacity planning - themes, trends and network usage. It also enables the business to track change controls ensuring that only the agreed changes were made and that they took place during the agreed maintenance window.

Technology Independent

The technology required to meet an organisation's security needs is rarely found in one technology, however Regency's experience and partnerships with the leading security vendor technologies including ArcSight, NitroSecurity and Tier-3, allows for a technology-independent approach enabling us to choose the right tool for the job and maximise any security investment. Regardless of the technology, the interface to the customer can remain consistent through a centralised Security Portal.

Key features

- Flexible service designed around customer requirements, policies, risk assessments and service levels.
- Options for 24x7x365 Monitoring providing real time awareness and analysis of events
- Centralised monitoring, correlation and comprehensive reporting
- Secure storage and transport of log information
- Government Certified Secure Operations Centre built to Government security standards (List X)
- All Engineers government Security Check (SC) cleared (or higher)
- ITIL-based Service Desk with clear escalation lines for incident handling
- Security Portal access providing ticket and incident management, reports, service announcements and security statistics for the monitored system.
- Technology impartial

Technical support and peace of mind

Regency has adopted an ITIL based Service Management framework to support the technical services and products we provide. Our Service Desk manages customer reports, incidents, Requests for Change (RFC), customer queries and communication updates and is located within our Government Certified Secure Operations Centre (SOC). That's one single point of contact for all of all support requirements and enquiries.

All Regency products have 'Underpinning Contracts' with our 3rd Party Support Vendors. This allows us to provide comprehensive Service Level Agreements (SLAs) in-line with industry-recognised Best Practice.

Further Information

For further information please contact Regency on +44 (0)1242 225680 or email managedservices@regencyitc.co.uk