Islington Borough Council achieves PSN and PCI compliance with CNS Group's Managed Security Services

The Client

Islington Borough Council provides services such as housing, social care, health, transport and leisure, to approximately 216,000 inner London residents. As a public sector organisation, Islington must protect a large and disparate data store of around 300 TB of confidential and sensitive information. The Council has to meet all the regulatory and statutory compliance requirements placed upon it by government and also to maintain its connection to the Public Services Network (PSN).

The Challenge

Every UK local authority must meet a minimum level of detailed security alert logging and monitoring for business critical systems to meet the Good Practice Guide Protective Monitoring standards – known as GPG 13. Although no longer mandatory, GPG 13 still provides an excellent benchmark for an organisation to determine their security logging and monitoring requirements. These specific requirements form part of PSN compliance that gives councils controlled access to internet content and shared services. But getting alert monitoring and analysis right is a challenge for many resource-strapped local authorities. Too little focus can quickly result in non-compliance, but with a growing number of systems to monitor, it is all too easy for security teams to become overwhelmed with alerts – many of which may be irrelevant. This can have the effect of distracting security professionals from actioning issues that pose a real risk. In addition, operating true 24/7 security manned monitoring is exceptionally expensive for most organisations. Islington Council was committed to getting the balance between compliance and contextual analysis right by evolving a workable set of processes and resources to correctly monitor, understand and action alerts to ensure best practice compliance.

"We were eager to establish the appropriate levels of comprehensive, 24/7 monitoring to comply with both PSN and PCI compliance. We chose to use the Comply and Secure Managed Security Service from CNS Group as the most effective way to have a better view of the risks and rapidly achieve our objectives," **said Patrick McCarty, Project Lead, Islington Borough Council.**

The Solution

Whilst evaluating its options, Islington met with CNS Group eager to hear more about their previous success providing PSN compliance for other councils and local authorities.

"CNS Group's breadth of public sector experience and accreditations, excellent technical and project management teams and proven delivery to organisations like Islington gave us great confidence in their managed services," **says Patrick McCarty.**

Islington evaluated the Mosaic Comply and Secure (HMG) service as a way to comprehensively log, track, and analyse user and system activity, whilst eliminating the technology and resource burden of building, configuring, maintaining, and monitoring an in-house data collection solution. The new service would provide an outsourced capability for:

Event generation Event parsing

Alert generation Secure event relay and collection

Event filtering Event correlation

Event normalisation Event analysis

CNS Group employs a number of CCP, CISSP and CESG Certified Professionals, and has been offering information assurance to the UK Government for over 15 years. CNS has an extremely deep understanding of what is required for attaining and maintaining HMG accreditation across a wide range of Government sectors.

The Mosaic COMPLY & SECURE (HMG) module is a customised set of services that specifically assists Government Agencies, Departments or entities that require to comply to HMG standards, including the legacy Government Protective Marking Scheme (GPMS) caveats of IL2 and IL3 and the new Government Classification Policy (GCP) caveat of OFFICIAL.

Using the Comply and Secure service has helped Islington to establish a clear process for linking access to system components, especially access provided through administrative privileges such as root, to each individual user. The security team now has access to audit trails for all system components with synchronised critical system clocks and timestamps – securing this data so that it cannot be altered.

The service is now fully operational and CNS analysts are monitoring Islington systems on a 24/7/365 basis, working to agreed parameters. The team liaises with council staff to determine whether a security event represents suspicious activity and should be considered a threat. If this is the case, the CNS analyst notifies the assigned Islington contact, irrespective of the time of day.

All CNS consultants that provide the Comply and Secure service are certified professionals with SC clearance and have been either Non Police Personnel Vetted (NPPV) or Management Vetted (MV).

The Benefits

1. Islington has established a successful working partnership with CNS that has helped it to address several resourcing and compliance objectives
2. Islington has been able to maintain its compliance and connection to the PSN
3. Islington now has a more contextual view of alerts, reducing the growing level of 'noise' that allows it to be more effective and targeted in its response.