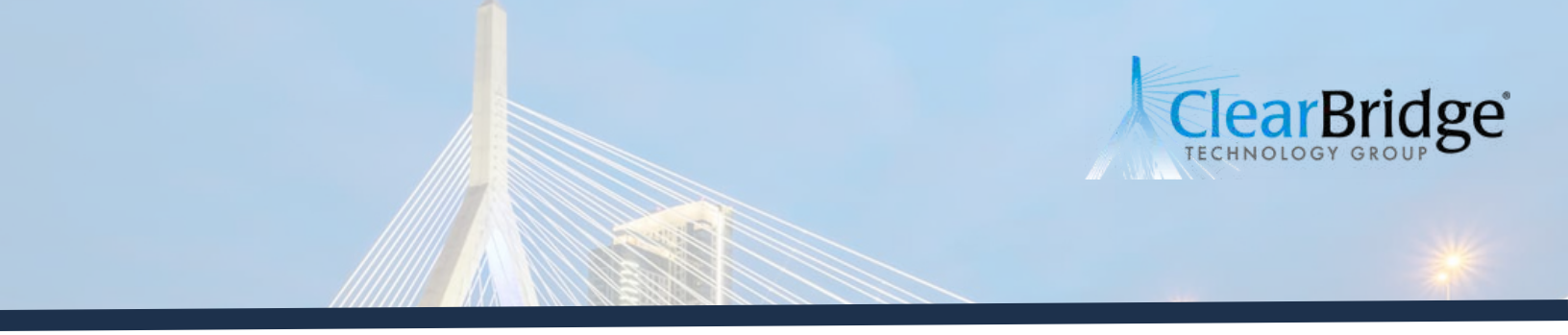

# Information Security Case Studies

## BRIDGING THE TECHNOLOGY GAP FOR INFORMATION SECURITY

Leveraging years of experience, our information security consultants build security and GRC strategies and implement solutions for all aspects of each organization's unique concerns.

### CSIRT TEAM

Our client needed help supporting their Security Operations Center due to limited resources.

ClearBridge provided a Cyber Security Incident Response Team (CSIRT) who were responsible for Incident Response for advanced targeted attacks working on SIEM/Log Management (Splunk), Incident Detection and Response (CrowdStrike), and forensic/malware analysis tools (FireEye NX) doing operational triage. The CSIRT performed root cause analysis, conducted research & intelligence gathering on advanced threat actors, and analyzed the issues.

### CYBERSECURITY ENGINEER

Our client, a large government contractor, needed a Cybersecurity Engineer to support their efforts to maintain their radar systems' security.

ClearBridge's consultant was responsible for implementing information security tools into their radar system, including ACAS, LogRhythm, DISA ESS Endpoint security suite, and backup and restore capabilities. The Cybersecurity Engineer worked within the Risk Management Framework (RMF) to identify controls and overlays, generate testable requirements, identify resilient architecture design, configure, run, and script audit tools, provided analysis of vulnerability analyses, and conducted verification testing for compliance assessment.

### DATA CENTER ENGINEERS

Our client needed help supporting a disaster recovery and rebuild effort due to a ransomware attack.

ClearBridge provided a team of Data Center Engineers with extensive experience in Linux, VMware, Nutanix, Commvault, and NetApp. The team was responsible for rebuilding infrastructure and virtualized infrastructure, rebuilding storage, implementing new hardware, and working to rebuild existing hardware and OS.

### SECURITY ARCHITECT

Our client, an enterprise retailer, needed a Security Architect for their Digital eCommerce team.

ClearBridge provided a consultant with a strong foundation in Cloud Security, who actively worked with the development teams to perform security architecture reviews, served as the subject matter expert to interpret the results from vulnerability scans (dynamic testing and static code analysis), and worked with developers to remedy vulnerabilities. The consultant also monitored and triaged vulnerabilities reported by vendors and researchers, developed application security policy and standards/best practices, and conducted penetration testing of internally developed applications.

### DESIGN ARCHITECT

Our client, a government integrator, asked ClearBridge to provide a DoD cleared Cyber Security Design Architect to lead their cybersecurity architecture efforts.

ClearBridge's secret cleared consultant was responsible for the process to implement and mature their internal security posture & tool implementation, including understanding of frameworks, documentation requirements, security tools, policies, and processes to protect sensitive information & monitoring technology around the infrastructure & systems hosting the environments. The Architect also served as a Security SME to advise their clients on applicable security solution technology, practices, and managed services.

### SECURITY ANALYST

Our client, a large healthcare organization, needed a Security Analyst to join their Incident Response team.

ClearBridge's consultant supported a variety of functions including developing, implementing, maintaining, and administering the organizations IT security systems, policies, and procedures. The Analyst performed vulnerability scanning with Rapid 7, SIEM with Splunk and QRadar and endpoint security with CarbonBlack and Crowdstrike.

sales@clearbridgetech.com www.ClearBridgetech.com 716.916.2284