Sean Brady

sbrady@sei.com | sei.com

PROFESSIONAL BACKGROUND

Sean is a technology professional with over 15 years of cyber security, system administration, and technical support delivery. He has focused on delivering business and technology solutions with an emphasis on product implementations, subject matter expertise, and product ownership. Throughout the many successful implementations Sean has gained extensive experience with product lifecycle management including concept and design, development, testing, implementation and product support. Sean has effectively worked with both technical resources and executives to deliver a variety of IT and business sponsored projects. He enjoys building effective relationships with his colleagues and project teams to ensure all team members are engaged and equally driven to succeed. He is a goal-oriented professional that values client delivery satisfaction and project success for each client he works with.

SELECTION OF RELEVANT EXPERIENCE

IT Project Manager | Security tool suite and Endpoint rollout

Sean was the IT project manager as part of a merger project to help transition the security tools and endpoints seamlessly over the course of 6 months. This project was closely integrated with several other merger projects and pulled together the necessary internal resources and external experts to ensure there was no impact to business as endpoints were migrated and new security tools were integrated into the environment. End user impact was minimal, all endpoints were scheduled and delivered on time. Auditing of migrated endpoints to ensure the security tool suite was installed correctly and providing protection as expected. Troubleshooting and follow-up after auditing continued until completion and project sponsor approval that the project was successful.

Implementation Manager and Product Owner | Sentinel One Endpoint Security

Sean served as the project implementation manager on Sentinel One Endpoint Security. He led a team that was tasked with implementing a new security solution that would help prevent the threat of ransomware and other malicious programs from executing on endpoints. Prior to implementation, the organization utilized a combination of Malwarebytes for Business and Windows Defender. The product was deployed to over 350 endpoints that included remote and onsite staff computers. In addition, over 65 servers in 8 locations including Mexico and USA. In order to successfully implement the product without disrupting services, a plan to deploy the product in test mode was utilized. The program was monitored for over two weeks and an exception plan was executed to limit the number of false positives that might be triggered. The project was implemented and fully installed on all endpoints over a 3-month period. With the capability to better detect threats and a ransomware rollback feature, Sentinel One was a successful and valuable addition to the cyber security framework. Sean continued as the product owner and subject matter expert after implementation.

Industry Experience

- Manufacturing
- Chemical
- Technology
- Government
- IT Services

Functional Expertise

- Program/Project Management
- Software Implementation
- Process Automation
- System Administration
- Change Management
- Process Improvement
- Risk Assessment
- Security Awareness

Sean Brady

sbrady@sei.com | sei.com

SELECTION OF RELEVANT EXPERIENCE

Implementation Manager and Product Owner | Proofpoint Insider Threat Management

As part of a company strategy to move towards a zero-trust framework, Sean served as the implementation manager on Proofpoint Insider Threat Management (ITM). He led a team that was tasked with identifying a tool that would give greater insight into user activities and provide clarity that company sensitive data was being protected. Over a 9-month timeframe, the team selected Proofpoint ITM and worked with a Proofpoint software implementation engineer to setup the software specifically for the needs of the internal security team. The software was deployed to all endpoints that included remote and onsite staff computers. Alerts were setup for high severity actions to quickly help the team secure sensitive data or investigate actions that were considered suspicious. Sean continued as the product owner and subject matter expert after implementation.

Project Manager and SME | Auditing and Penetration Testing

Sean served as the project manager and SME on the cyber security side for the annual company requirement of auditing and penetration testing for both internal due diligence and Department of Homeland Security (DHS) compliance. Compliance with DHS consisted of a combination of on-site auditing in conjunction with the physical security project lead, DHS representatives reviewing internal policies, reviewing audit findings and ensuring remediation took place with responsible employees. Internal due diligence consisted of a various activities such as selecting a 3rd party to externally and internally conduct penetration tests, capture the flag exercises, tabletop exercises, and social engineering drills such as phishing and calling employees for company information. Once the exercises were completed, reports were generated and if findings were present a remediation plan was generated. Over the 7+ years of executing in this role, many vulnerabilities were uncovered that were later patched, processes updated to prevent data loss, and policies strengthened due to findings while auditing.

Product Manager and SME | Microsoft Intune Mobile Device Management Rollout

Sean was the product manager for the Microsoft Intune Mobile Device Management (MDM) rollout. Key activities included vendor selection, capabilities review, cost analysis, and deployment planning. Sean acted as the product manager and once implemented became the SME for the company. Microsoft Intune gave the company the ability to secure company data on both corporately owned and personally owned mobile devices. Rollout of the software took place over a 9-month timeframe which included the key activities above and testing prior to full implementation.

Implementation Manager and Cyber SME | Security Awareness Program

In a strategical move to strengthen the company security awareness posture, Sean was tasked with implementing a security awareness program. It was determined to protect the company fully, employees needed to be engaged and aware of the many ongoing risks from both a cyber and physical security perspective. Prior to implementation, the company had no formal cyber security training. The program once developed consisted of annual computer-based training, monthly communications by email, quarterly newsletters, and monthly email phishing assessments. The program also worked closely with the physical security SME to create a combination of training that helped employees learn both cyber and physical security awareness. Security awareness training was also baked into the new hire program to help new employees hit the ground running fast and to understand the risks associated with their positions. A major success in the program resulted from the monthly phishing assessments. Baseline failure rate was at 10% for the phishing assessments at program implementation and most recently the failure rate dropped to under 4% annually.

Technology Expertise

- Microsoft Azure
- Microsoft Defender for Cloud
- Active Directory
- Microsoft Intune Mobile Device Management
- Microsoft Office 365
- Sentinel One Endpoint Security
- Proofpoint Insider Threat Management
- LogRhythm SIEM
- KnowBe4 Security Awareness
- Microsoft Exchange 365
- Microsoft Teams
- Windows Server
- SharePoint
- System Center Configuration Manager (SCCM)
- Project Online

Deliverables

- Program/Project Plans & Strategy
- Software Implementation
- Vendor/Software Selection Planning
- Product Lifecycle Management
- Communication Plans