Case Study

Phoenix Defense Significantly Improves Its Overall Security Posture by Leveraging CMMI® Performance Solutions' New Security Domain

The Business Need

Phoenix Defense business units work in a highly competitive market, providing complex custom software and services to the defense industry. Securing their next defense contract win is highly dependent on their past performance and their ability to deliver a quality product at a cost-competitive price. Essential to those business goals are the:

- Reduction of delivered defects and any impacts to fielded operations
- Reduction of the cost of poor quality balanced with adequate cost of quality to strike the appropriate balance
- Developing and delivering the right product, the first time
- Streamlining our internal processes to avoid security issues, data compromises, rework, and inefficient processes

Since Phoenix Defense products are deployed into a secure environment, it is their responsibility to safeguard government data and develop their systems while employing safeguards to protect, identify, mitigate, and track security threats. With other models like the CMMC (Cybersecurity Maturity Model Certification) or ISO 27001 addressing specific aspects of Cyber or Information Security, (and some facing delays in rollout or updates), and the increasing hurdles in implementing models like CMMC for SMEs, the new CMMI Security domain and Managing Threats Practice Area provided Phoenix Defense with a holistic and comprehensive set of security practices, controls, and methods to keep their systems secure and improve their entire organization's posture on security including mission, personnel, physical, cyber and process related security needs.

Company Background

Phoenix Defense companies (which include Phoenix Logistics, PLI Manufacturing, Riptide Software and Phoenix Defense Germany GmbH) are an agile provider of engineering, manufacturing, information technology, and logistics & supply chain services to the defense, space, aerospace, and industrial markets. The organization is made up of talented experts, with years of defense and industry experience, who reliably solve technical and programmatic problems related to complex software development and sustainment, aerospace design and manufacturing, as well as logistical challenges related to the delivery of critical infrastructure (medical, energy, IT and transportation).

For more information,
go to **phx-defense.com**

PHOENIX DEFENSE

ISACA®

The Solution

Phoenix Defense, a CMMI Performance Solutions organization since 2005, has had its Operating Unit (OU) conduct multiple successful CMMI adoptions and appraisals. This long-term CMMI organization has been applying CMMI best practices to improve business performance for over 18 years, and first achieved Maturity Level 5 in 2020.

Phoenix Defense Maturity Level Milestones

2005	ML2 CMMI-DEV
2006	ML3 CMMI-DEV
2009	ML3 CMMI-DEV
2011	ML3 CMMI-DEV
2014	ML4 CMMI-DEV
2017	ML4 CMMI-DEV
2020	ML5 CMMI-DEV
2023	ML5 CMMI-DEV with SEC, EVSD

The main objectives of their second appraisal at Maturity Level 5 were:

- Incorporation of the Enabling Security and Managing Security Threats and Vulnerabilities Practice Areas, including establishing monitoring, automation, and predictive models for security to complement their existing NIST 800-171 practices and controls like CMMC V2.0
- Sustainment and upkeep of their previously appraised Practice Areas
- Continuous improvement in their processes, quality standards, and predictive models
- Incorporation of the Supplier Agreement Management Practice Area for the first time

In addition, the capabilities targeted for this appraisal were:

- Ensure Quality
- Design and Develop Products
- Planning & Management
- Maintain Habit and Persistence
- Improve Performance
- Manage Security
- Supply Chain Management
- Supporting Implementation
- Managing Business Resilience

> **"Adopting CMMI has been a game-changer for our organization. It has led to significant performance improvements across the board, enhancing our competitiveness and assisting in positioning us as a market leader."**
>
> **Al Funderburk, Chief Executive Officer, Phoenix Defense**

Key Performance Goals Achieved

Phoenix Defense's adoption of CMMI performance metrics to meet their quantitative goals is displayed in the Cyber Threat QPP model and the Physical Security Threat model. The Threat Intelligence model ensures robust security capabilities for the company. Incidents are analyzed and action taken based on analysis of cyber-related traffic. The company set a KPI rate (>=1) to ensure cyber traffic analysis leads to tangible actions. Prior to the incorporation of CMMI Security and the Managing Security Threats and Vulnerabilities Practice Areas inclusion in the model, Phoenix Defense did not fully quantitatively track attacks against the networks, or other data flows, because the organization has a closed network with no outward-facing applications. In addition, the organization relied on a third-party vendor to monitor threats and spam. Thanks to the CMMI SEC adoption, the IT manager, CTO and GM determined that a more robust approach was needed to ensure network security.

> **"For over 18 years, our organization has been progressively applying CMMI practices to our Phoenix Defense organization to obtain a continuous improvement in quality and efficiency. *A surprise was how the application of CMMI has become a fundamental catalyst for introducing innovation into our processes and products."***
>
> **Barry Clinger, Chief Technology Officer, Phoenix Defense**

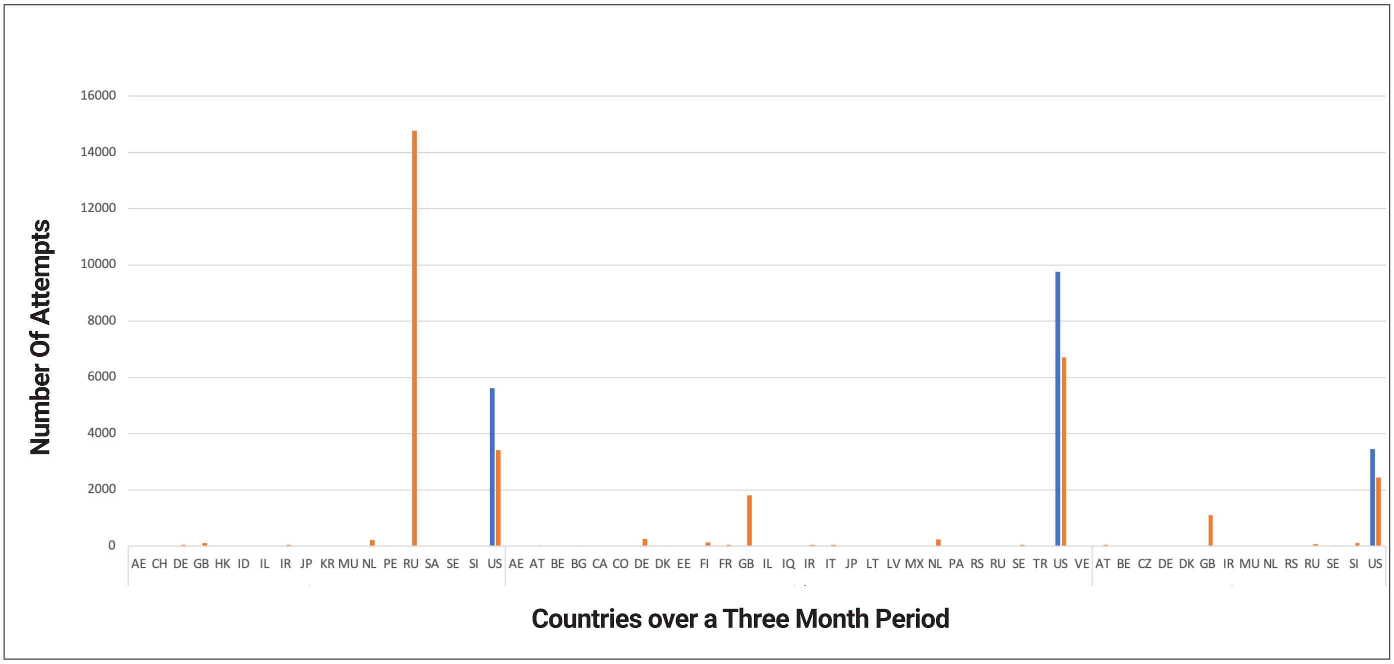
After the incorporation of the Enabling Security and Managing Security Threats and Vulnerabilities Practice Areas, Phoenix Defense developed three new models: the Threat Intelligence Model, the Physical Security Model, and the Mail Tracking model. Each model is used concurrently to ensure all network activity is monitored and analyzed. These models are used to track and block spam, track malware, and identify countries of origin, IP addresses, and number of attempts (successes and failures) against the network. The most notable and effective model is the Threat Intelligence model.

After the incorporation of the models, Phoenix Defense identified incidents and took action to prevent future occurrences. When the models were incorporated, the organization captured the baseline for attacks against the network. During the baseline reporting period, the IT team noted 18,616 attacks against the network in June. The IT department conducted a Causal Analysis Review and identified a series of corrective and preventive actions, implemented new protocols, and enhanced the corporate firewall. Subsequent runs of the data showed a significant decrease in network attacks in July and August: 48.9% in July and 79.4% in August.

Phoenix Defense also reduced its time to identify threats: the previous average was greater than 72 hours, the current average is less than 12 hours. The organization also dramatically reduced their time to resolve security threats: the previous average was approximately 4 hours; the current average is 15 minutes.

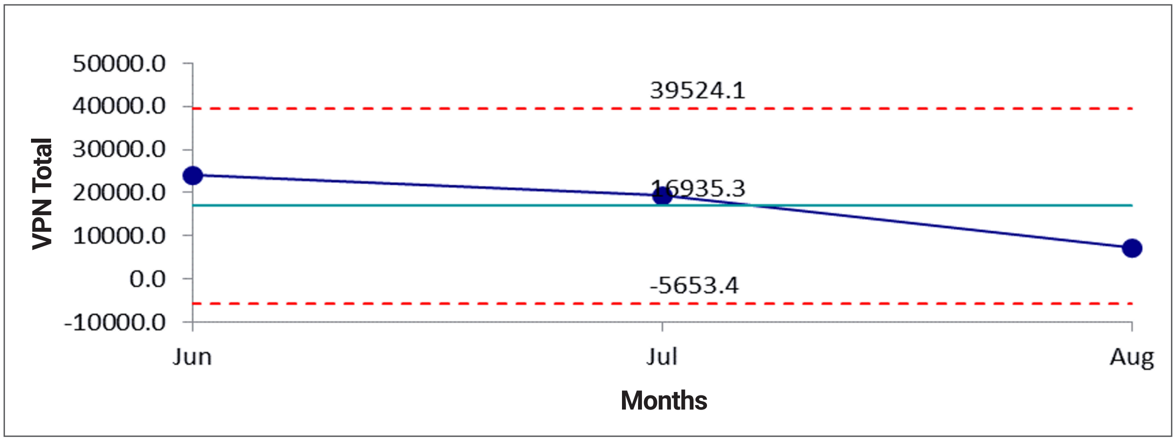
These select charts represent the 'before' and 'after' analysis of threats, and threat intelligence analysis coupled with a strong set of best practices implemented from ESEC and MST areas, which ensured a tangible and direct action, reducing the threats. Phoenix Defense continues to use this and further improve the models and leverage modern threat intelligence analysis techniques and tools, to enable even more resilience in the organization.

CONNECTION SUCCESS AND FAILURE PER COUNTRY



Number of external connect attempts by geography, by month, shows a significant reduction per country after statistical models were used and processes improved.

REDUCTION OF EXTERNAL THREAT ATTEMPTS OVER THREE MONTHS



This chart shows the reduction of external connect attempts over a period of 3 months, after the implementation of statistical and quantitative models and process interventions.

Lessons Learned

Organization: Phoenix Defense found that working with their lead appraiser, Kris Puthucode at SQC, well in advance of the formal appraisal timeframe helped to validate improvements and understand more fully the new SEC Practice Areas.

Sustaining Habit and Persistence: Phoenix Defense conducts periodic self-assessments of compliance adherence at the project and staff levels. This ensures a commitment to continuous improvement by all team members.

Improving Performance: Phoenix Defense found that continuous education and incorporating CMMI principles into their foundational corporate culture was essential to success. The organization begins this process during the staff onboarding process for new employees, and it continues through lunch & learns, formal training, on-the-job training, quality audits, and checklists, and more. This process provides constant awareness of the importance of CMMI Performance Solutions' best practices and helps make these practices stronger, persistent and habitual.

> **“Phoenix Defense has led the way in adopting CMMI best practices for nearly two decades, and now included the Security best practices. This adoption has yielded quantifiable benefits, enhancing security posture across Mission, Personnel, Physical, Process, and Cybersecurity domains. Additionally, incorporating Virtual work best practices has standardized virtual meetings and events, boosting efficiency.”**
>
> **Kris Puthucode, Certified CMMI High Maturity Lead Appraiser, Software Quality Center LLC**

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its more than 165,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

RESERVATION OF RIGHTS

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Support: support.isaca.org
Website: cmmiinstitute.com