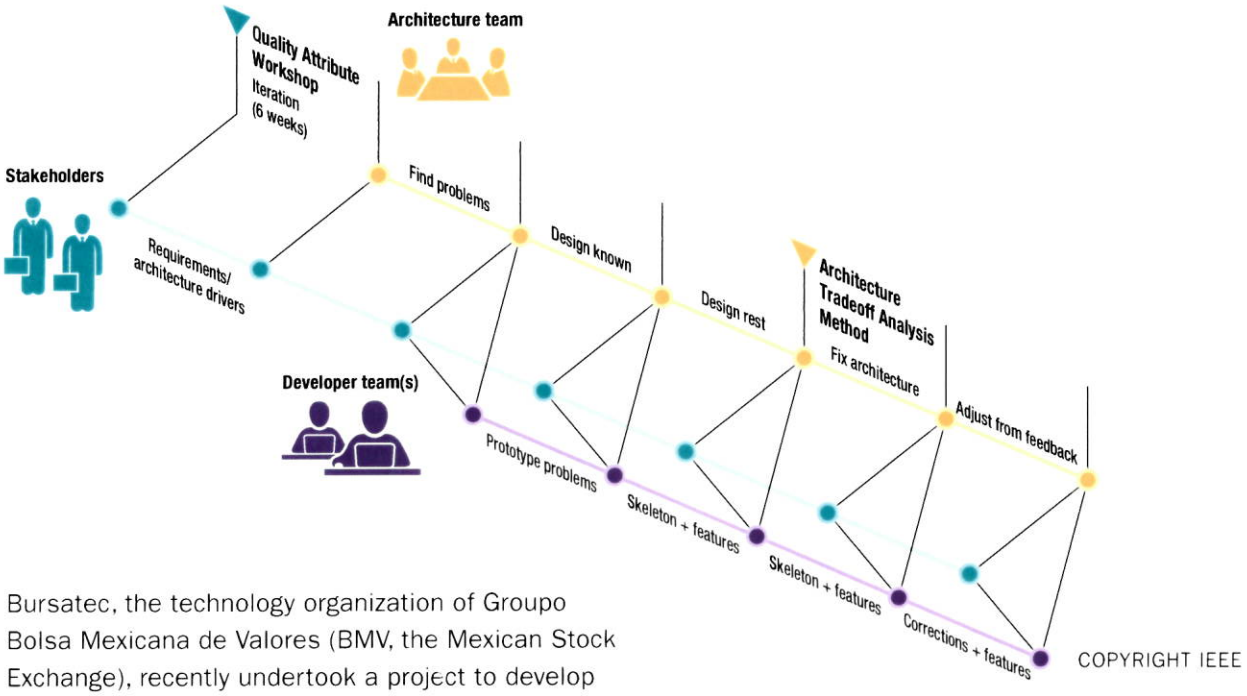
Working Together

The Team Software Process and Architecture-Centric Engineering



Bursatec, the technology organization of Groupo Bolsa Mexicana de Valores (BMV, the Mexican Stock Exchange), recently undertook a project to develop one system that would replace three existing trading engines. Given the competitiveness of global financial markets and recent interest in Latin American economies, Bursatec needed a reliable and fast new system that could work ceaselessly throughout the day and handle sharp fluctuations in trading volume. To meet these demands, the SEI suggested combining elements of its architecture-centric engineering (ACE) method, which uses software architecture to guide system development, with its Team Software Process (TSP), which teaches software developers the skills they need to make and track plans and produce high-quality products.

ACE methods focus on what to build; TSP methods focus on how to build it. ACE is the discipline of using architecture as a focal point for performing ongoing analyses to gain increasing levels of confidence that systems will support an organization's business goals.

The SEI created TSP to build high-performance teams that

- plan, manage, and own their commitments;
- produce quality products at lower cost; and
- achieve their best performance.

Approach

While TSP can be used to manage all aspects of the software-development phase, from requirements elicitation to implementation and testing, this was the first time that the approach had been applied to ACE methods. The combination of these approaches offered Bursatec architects and developers a disciplined method for developing the software for their new trading engine. Through 6 major development cycles including 14 or so iterations over 21 months, the overall team developed more than 260,000 lines of code, spending only about 12 percent of their effort on architecture and approximately 14.5 percent of effort in unit testing, performance testing, and integration testing.

In contrast, a typical project of this scale would normally expend at least twice this much effort in testing—an unfortunately realistic expectation in the software industry. System testing at Bursatec proceeded on schedule with a very low defect count (unusual for non-TSP projects). The early investment in architecture and a detailed, data-driven approach to managing both schedule and quality resulted in less testing throughout system development.

Another benefit of combining ACE with TSP is that the team of Bursatec developers was prepared for inevitable changes in requirements, indeed in changes of any sort over the 21 months of development. When the team received new requirements, it could evaluate them quickly for technical impact and implementation cost in terms of time and effort. With the quality-attribute requirements formally captured, the architecture in place, and detailed development plans at every step, a project with high risk potential in both technical and business terms ran on time, within budget, and generally without the drama that large development efforts often exhibit.

Results

The development of the new trading system for Bursatec, which was released in September 2012, progressed on schedule and within budget. Tests confirmed that the trading-system performance far exceeded the initial specifications. The combination of ACE and TSP proved an ideal approach for the development of the trading system. TSP brought discipline and measurement, while ACE provided a set of robust architectural techniques that focus on business goals and quality requirements. The approaches together support the entire development lifecycle, emphasizing business and quality goals, engineering excellence, defined processes, process discipline, and teamwork.

The architecture coaching coupled with the discipline of TSP helped Bursatec build a competent architecture team that produced excellent results: the team hit its milestones and the project finished on time; early performance tests and other quality measures indicated that reliability and quality goals were met along the way; no known defects carried into the final development cycle; and system performance goals were met.

"We are very happy with the results, said Dr. Enrique Ibarra, director general of Bursatec. "Because we are Mexico's only stock exchange, we're essentially a national utility. We could not bring the market down during this process. So, one of our key success indicators was zero disruption of service. We met this key indicator." Ibarra attributed this result to focusing a lot of attention on quality early in the software development process—a fundamental principle of SEI methods. "And that paid off," he added.

To Learn More

Developing Architecture-Centric Engineering Within TSP

This blog post describes the challenges Bursatec faced and outlines how working with the SEI and combining ACE with TSP helped them address those challenges. http://blog.sei.cmu.edu/post.cfm/developing-architecture-centric-engineering-within-tsp

Using TSP to Architect a New Trading System

This blog post focuses on the development of the system architecture for Bursatec within the TSP framework.

http://blog.sei.cmu.edu/post.cfm/using-tsp-to-architect-a-new-trading-system

Launch of High-Speed, High-Capacity Trading System Caps SEI's Successful Multi-Year Engagement with Mexican Bourse (news story on SEI website)

http://www.sei.cmu.edu/newsitems/BMV.cfm

Combining Architecture-Centric Engineering with the Team Software Process

Robert Nord, Jim McHale, Felix Bachmann

Technical Report

This report contains a description of an architecture-centric life-cycle model that uses the Carnegie Mellon Software Engineering Institute's architecture-centric engineering (ACE) methods embedded in a Team Software Process (TSP) framework and our experience in piloting the approach in an actual development effort. The SEI had the opportunity to realize this vision beginning in summer of 2009. At that time, the SEI began a project with Bursatec, the IT arm of La Bolsa Mexicana de Valores (the Mexican Stock Exchange), to replace its main online stock trading engine with one that would also incorporate trading of other financial instruments such as options and futures. The project had aggressive goals for performance and delivery, and as the face of Mexico's financial markets to the world, the new trading engine needed to function flawlessly. Download full report at http://www.sei.cmu.edu/library/abstracts/reports/10tr031.cfm

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412.268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

Cybersecurity Assurance: Creating Justified Confidence

How did this attack happen? Are they still in the network? Can we recover our systems? Are we certain they can't come back? These are questions an organization must be able to answer to ensure survival when faced with disruption. A comprehensive and integrated approach to cybersecurity is the only viable path to achieving predictability in uncertain times. Robust measurement of capability maturity coupled with realistic technical vulnerability assessment is required to truly understand your defenses and ability to withstand cyber-attack.

Can your organization survive a disruptive cyber event?

About

The Cybersecurity Assurance team creates tools and methods to empower organizations to gain justified confidence in their cybersecurity posture. We use techniques to evaluate the fundamental processes required to manage operational risk and technical safeguards that surround your most important assets. We draw on well-established principles of process measurement, such as the CERT® Resilience Management Model (CERT®-RMM) and leading-edge technical vulnerability assessment methods in developing solutions. The team has an established and prominent role in protecting our nation's critical infrastructure. Our approach takes assessment beyond the routine compliance checklist and traditional "pen test" and delivers measures of capability.

Our researchers, engineers, and subject matter experts often lead the national conversation on critical infrastructure protection and supply chain risk management. The collective lessons of years spent measuring and evaluating organizations in all 16 sectors informs our approach. The Cybersecurity Assurance team has worked with organizations of all sizes and composition. Deriving practical tools and methods from the best concepts that academia has to offer and best practices from private industry is at the heart of our work.

Key Capabilities

Process Assessment – Using models and techniques, we understand how to rigorously measure the cybersecurity capabilities of an organization.

Technical Vulnerability Assessment – We understand how to examine an organization's susceptibility to technical vulnerabilities and cybersecurity exploits.

Supply Chain Risk Management – Through the application of capability measurement and the modeling of dependencies, we understand how to reduce vulnerability, manage risk, and ensure resilience within your supply chain.

Data Analytics & Visualization – We understand how to analyze complex datasets and turn them into practical insights for use by organizations.

```
<meta http-equiv="content-type" content="text
<meta property="og:type" content="website" />
<meta property="og:url" content="http://www.s
<meta name="robots" content="
```

Solutions

Working with our stakeholders, we identify and solve problems using comprehensive solutions such as the Cyber Resilience Review, Risk and Vulnerability Assessment, and External Dependencies Management Assessment.

Cyber Resilience Review (CRR) – Created by the CERT Division for the U.S. Department of Homeland Security (DHS), the CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains (based on CERT RMM) including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.

CRR

Risk and Vulnerability Assessment (RVA) – An RVA identifies vulnerabilities and ensures that security implementation actually provides the protection that organizations require and expect. An RVA is conducted collaboratively by CERT subject matter experts and DHS using open source and commercial security tools to conduct vulnerability scanning and manual penetration testing. These scans and tests determine whether, and by what methods, an adversary can defeat security controls on a live or simulated network. The main goals of the RVA are to help secure against known vulnerabilities and threats by providing mitigation strategies to reduce risk, and aggregate vulnerability data so executives can make informed decisions regarding the security and safety of information systems.

RVA

External Dependencies Management (EDM) Assessment – The EDM Assessment evaluates an organization's risk management when forming relationships with external entities, ongoing management of third-party relationships, and the ability to sustain services when external entities fail to meet the terms of service or are otherwise disrupted. The EDM Assessment, offered by the DHS Cyber Security Evaluation Program, is a no-cost, voluntary, non-technical assessment to evaluate and communicate the EDM capability of critical infrastructure organizations.

EDM

Applied Research Areas

Cyber-Physical Systems – We are working to determine if there are management practices and techniques unique to protecting cyber-physical systems, the role sector requirements have in shaping cyber-physical protection strategies, and how organizations can best identify and manage risks resulting from cyber-physical systems.

Cyber-Exercise Diagnostic – We are working to advance the state of the practice of cyber exercise by extending its use as a measurement instrument. We believe cyber exercise can be employed as an effective validation of capabilities in many dimensions.

Next-Gen Penetration Testing – We are developing tools and methods to bring increased value and robust measurement to the performance of technical vulnerability assessment.

Get Started Today

The Cybersecurity Assurance team is ready to help your organization, and we hope that you engage with us to support your improvement efforts. Use our tools, participate in our workshops, collaborate with us, request an assessment, explore our digital library, sponsor some research and development, or attend an event. For more information visit www.cert.org or contact us at 412.268.7090.

Software Engineering Institute
Carnegie Mellon University

LEAP(4BD): Lightweight Evaluation and Architecture Prototyping for Big Data

Make more informed decisions about Big Data system design

Ensure scalability as your data grows

Choose NoSQL databases that can support your future scalability needs

The exponential growth of data in the last decade has fueled a new specialization for software engineering—*big data* software systems. At the heart of big data systems is a collection of database technologies that are simpler and more lightweight, and provide higher scalability and availability than traditional relational databases.

These highly scalable "NoSQL" databases are typically designed to scale horizontally across clusters of low-cost, moderate-performance servers. They achieve high performance, elastic storage capacity, and availability by replicating and partitioning data sets across a cluster. Each database specifies its own proprietary data model and query language, as well as database-specific mechanisms for achieving distributed data consistency and availability.

This specification means that for software engineers building scalable, big data applications, there's a dizzying range of potential databases that can be used as building blocks for a solution. The range of choices makes database selection a crucial software architecture decision, as selecting a database technology that can't meet system requirements will be costly, reduce downstream productivity due to rework, and even lead to project cancelation. Therefore, architects must carefully compare candidate database technologies and features and select platforms that can satisfy application quality and cost requirements. In the inevitable absence of up-to-date, reliable technology evaluations, this comparison exercise is in practice a highly exploratory, unstructured task that uses an Internet search engine as the primary information gathering and assessment tool.

LEAP(4BD)

To meet the challenge of selecting a database for big data systems, the Software Engineering Institute (SEI) has developed the Lightweight Evaluation and Architecture Prototyping for Big Data (LEAP4BD) method. The LEAP(4BD) method provides a systematic approach for a project to select a NoSQL database that can satisfy its requirements.

A key feature of LEAP(4BD) is its NoSQL database feature-evaluation criteria. This ready-made set of criteria significantly speeds up a NoSQL database evaluation and acquisition effort. To this end, we have categorized the major characteristics of data management technologies based on the following areas:

- Query language
- Data model
- Data distribution
- Data replication
- Consistency
- Scalability
- Performance
- Availability
- Modifiability
- Administration and management

Within each category, we have detailed evaluation criteria that will differentiate big data technologies. These evaluation criteria are reusable across projects and pre-populated to capture the capabilities of most popular NoSQL technologies.

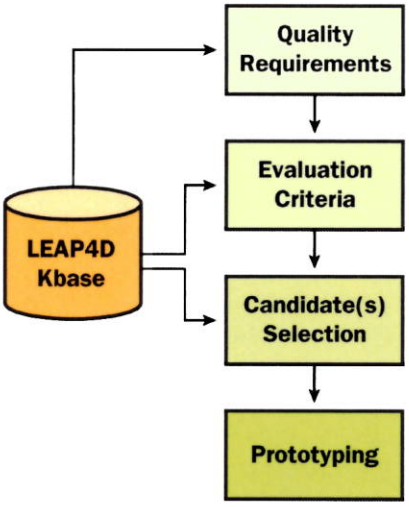
LEAP(4BD): Lightweight Evaluation and Architecture Prototyping for Big Data

How Does LEAP(4BD) Work?

In LEAP(4BD), we first work with the project team to identify features pertinent to the system under development. These features help identify a specific set of technologies that will best support the system. Then, we weight individual features according to system requirements and evaluate each candidate technology against these features.

The LEAP(4BD) method employs five steps to produce both qualitative and quantitative evaluation results:

1. **Specify requirements.** First, we elicit the high-priority functional and quality requirements for the system. For big data applications, we focus on specific requirements for performance, scalability, availability, consistency, and security. We also define a use case that is representative of the customer's application domain. The use case defines both a data model and workload that will be used as the basis of performance and scalability assessment in Step 4.



2. **Select candidate NoSQL databases.** Next, we select two to four candidate NoSQL databases for deeper evaluations. Selection criteria are both contextual (e.g., experience with a specific technology) and technical, and require evaluating database features against the requirements developed in Step 1.

3. **Design a use case–specific data model.** Based on the use case defined for evaluation, we map the application's logical data model to the physical model supported by the candidate NoSQL databases. We also deploy the database and load the test data (synthetic or actual) into the database instances.

4. **Execute performance and scalability tests.** We implement a test case driver that executes the specified workload on each database. Load is scaled by increasing the number of concurrent client requests to assess how each database reacts to increased workloads.

5. **Report results.** The evaluation report includes both qualitative and quantitative results. The report details the performance and scalability results that we obtained from testing each NoSQL database in a consistent environment. It also describes how easily the logical data model maps to the specific NoSQL data models that were tested, and the specific features of each database that will influence the identified quality requirements for the application.

LEAP(4BD) is supported by a knowledge base that stores the results of our evaluations and comparisons of different NoSQL databases. We have pre-populated the LEAP(4BD) knowledge base with evaluations of specific technologies (e.g., MongoDB, Cassandra, and Riak) with which we have extensive experience. Each evaluation of a new technology adds to this knowledge base, making evaluations more streamlined as the knowledge base grows. Overall, LEAP(4BD) provides a systematic, quantitative, and highly transparent approach that quickly ranks the various candidate technologies according to project requirements.

Engage with Us

If you would like to use LEAP(4BD) in your next acquisition of a big data system, please contact SEI Customer Relations at info@sei.cmu.edu or 1-412-268-5800. We would like to work with you to select a NoSQL database that can support your future scalability needs.

Additional Resources

An Approach to Managing the Software Engineering Challenges of Big Data (podcast), http://url.sei.cmu.edu/iq

Related Web Sites

www.sei.cmu.edu/architecture
blog.sei.cmu.edu/archives.cfm/category/big-data

For Course Registration

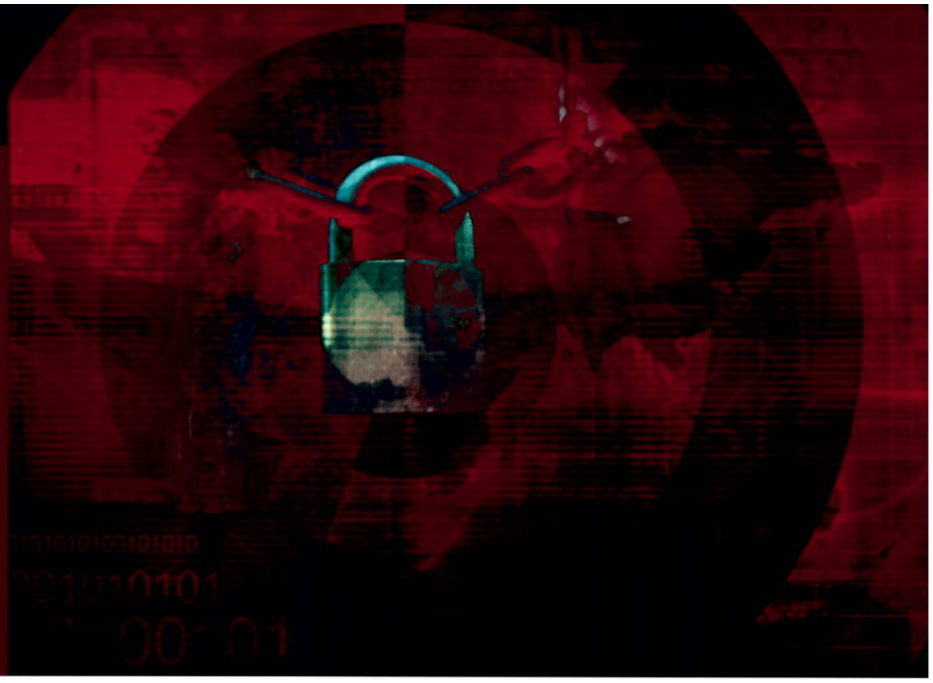
www.sei.cmu.edu/go/big-data

For General Information

For information about the SEI and its products and services, contact
Customer Relations
Phone: 412-268-5800
FAX: 412-268-6257
info@sei.cmu.edu
www.sei.cmu.edu

CERT | Software Engineering Institute
Carnegie Mellon University

Secure Lifecycle Solutions



About

The Secure Lifecycle Solutions (SLS) team delivers innovative engineering methods and solutions to challenging cybersecurity problems. By leveraging in-house technical expertise and longstanding collaborations with leading researchers from world-class academic institutions, our experts develop custom methods and systems to meet customer needs. We apply cutting-edge research and technologies to provide secure software solutions that bring real value to support the mission of our government and industry stakeholders and advance the state of the practice.

Our team of researchers, software architects, and engineers are experts in software engineering technologies and process with decades of hands-on experience delivering proven results to customers. SLS staff have deep technical expertise in software/systems design and architecture, systems integration, distributed systems, web and open source technologies, real-time collaborative systems, Big Data analytics, and data visualization.

In addition to technical capabilities, SLS staff are thought leaders in engineering process and best practices, advancing the state of art in secure software engineering methodologies. Our expertise in DevOps process and tools, resilient system design and implementation, and requirements gathering and analysis enables us to develop comprehensive engineering processes tailored to unique customer needs, or improve existing processes to meet evolving challenges by leveraging emerging technologies. Built on proven SEI software engineering methodologies and CERT cyber security expertise, SLS engineering processes lead to efficient, successful, and secure product development and deployment.

Our Process

We combine agile software development and Human-Centered Design into our modern, adaptive, and iterative Secure Development and Operational Process. Each applied research project within SLS goes through five stages: (1) scope and define, (2) explore and synthesize, (3) create and implement, (4) test and refine, and (5) launch and transition. This rigorous and data-driven process ensures that the solutions delivered are correct, usable, and highly aligned with specific customer needs.

Key Capabilities

Evaluate, improve and define secure lifecycle solutions, workflows and methodologies

Design, develop, and deploy custom software and systems solutions in the cybersecurity domain

Transition research findings into DevOps tools and methods for government and industry technology development and acquisition

Provide expert guidance in Open Source, web, and cyber security emerging technologies and practices

Solutions

Working with our stakeholders, we identify and solve problems using comprehensive solutions such as:

Critical Infrastructure Protection
We develop powerful systems for the protection of critical infrastructure systems and facilities. By developing both custom hardware and software, we provide secure solutions specifically tailored to stakeholder operational needs.

Cybersecurity Tools & Systems Development
We develop robust tools for digital forensic acquisition, systems assessment, and security analysis. Leveraging our broad experience in the cybersecurity domain, we anticipate and assess stakeholder needs and apply state-of-the-art technologies to develop custom solutions.

Application Technologies & Security
Using cutting-edge web and desktop technologies, architectures and security practices, we envision, design, build, and assess systems that meet identified stakeholder security needs and usability standards.

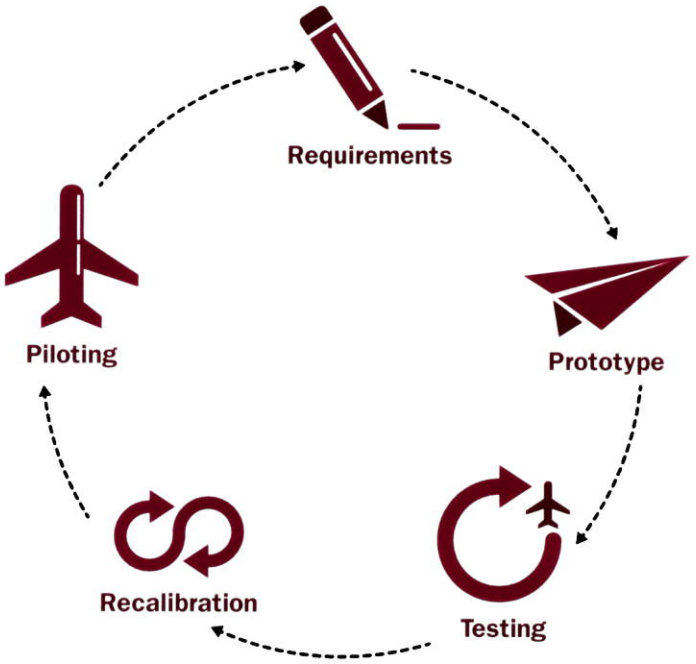
Mobile Application Security
We analyze and develop solutions to implement best security practices on mobile platforms, improving and protecting user identity and privacy.

Applied Research Areas

Secure, Repeatable and Modern Development and Operational Practices
Our expertise in every phase of software development and operational needs on a wide variety of platforms enables us to evaluate, create, improve, and extend secure development process and methodologies based on unique needs and constraints.

Big Data Analytics, Storage & Visualization
Our expertise in high-volume and real-time data systems enables us to create solutions capable of collecting, synthesizing, analyzing, and visualizing complex data sets.

Machine Learning & Computer Vision
We apply machine learning and computer vision technologies to create systems that can learn from data and their environment. Through collaboration with leading research experts at Carnegie Mellon University, we utilize groundbreaking research from decision sciences, language technologies and computer science.



About

For more than 25 years, the CERT Division of the Software Engineering Institute has been a leader in cybersecurity. Originally focused on incident response, the division has expanded into areas of network situational awareness, malicious code analysis, secure coding, resilience management, insider threat, digital intelligence and investigation, and workforce development.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412.268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu