Contents

Background 1
The case for software security CoEs 3
The EY approach 6
Summary 10
Background

Software runs virtually all organizations and is often the main point of contact with customers. Whether an organization develops, deploys or configures software, security flaws arise that provide attackers an avenue to gain access to an organization's sensitive data and intellectual property. In a corporate context, an attack at the software layer can not only damage an organization's brand and reputation, but can also result in steep financial damages, loss of competitive advantage and create legal or regulatory noncompliance.

In order to mitigate the potential damages caused by these flaws, organizations must deploy good software security practices to proactively identify threats in a timely manner. A software security Center of Excellence (CoE) helps provide the organization with capabilities to integrate software security practices in the software development life cycle (SDLC). However, deploying a software security CoE can create challenges, including creating the right processes and embedding a team with the right skillset for a cost-effective solution.
The case for software security CoEs

Software security Centers of Excellence help drive security efforts and make sure that security is integrated into the development life cycle and vulnerabilities are identified early.

In today’s evolving threat environment, where new software is developed, deployed and configured rapidly through multiple channels, the traditional “test and fix” approach is unsustainable. Failure to detect software defects early in the development life cycle not only increases the number of software defects introduced into production, but also increases the cost to remediate them as they progress further down the life cycle.

Software security CoEs help drive security efforts and make sure that security is integrated into the development life cycle and vulnerabilities are identified early. CoEs use dedicated security resources to configure scanning tools, on-board applications and manage the events generated by those tools. This allows developers to focus on remediating vetted vulnerabilities and frees up time to build the next great solution.

Challenges organizations face

Building a software security CoE with the correct balance between tools and processes tightly coupled with various stages of the SDLC can prove challenging. However, with the complexity of threats and reliance on tools, implementing a CoE correctly becomes crucial to derive maximum benefit. Typical challenges include:

- Lack of buy-in from development teams to integrate security in the SDLC
- Staffing the CoE with appropriately skilled resources who understand not just the security tools deployed, but also the development context associated
- Software security CoE and development teams overwhelmed with tool results from inadequately tuned scans, resulting in high false positive rates
- Scanning rules not aligned with the organization’s priorities for vulnerability reduction
- Providing software security CoE services in a cost-efficient manner

The inability to meet these challenges can result in a misalignment of the software security CoE with development teams, resulting in a challenging culture and recurring vulnerabilities from the same sources.
The EY approach

EY assists organizations in the planning, building and operation of software security tools.

Software security helps mature risk management practices by developing advanced risk identification processes and integrating them into the development life cycle. EY offers a holistic approach to the design, transformation and enhancement of software security programs: enhancement is achieved through managed software security services by automating testing processes and procedures, developing proactive risk analysis, and calibrating and tuning CoE capabilities against the contextual business environment.

The EY approach to managed software security services helps enhance:

- An enterprise-scale managed program for sustaining software security customized to an organization’s needs
- End-to-end security integration in the SDLC that drives business value and supports accelerated software development methodologies
- Improved business relationships between security and the development community with security seen as less of a hurdle
- Assimilation with new development methodologies that support faster go-to-market solutions

Leveraging our experience and skills we provide continuous integration and monitoring of organization’s application portfolios. Included in the managed software security services are operating testing tools, onboarding applications, performing scans, reviewing results and providing analysis of results.

Depending on the individual client’s needs, EY has the capabilities to assist clients with varying requirements for software security CoEs. Clients can augment their existing software security program with higher maturity services. EY can assist in the planning, building and operation of software security tools for dynamic application security testing (DAST), static application security testing (SAST), software composition analysis (SCA), integrated application security testing (IAST) and real-time application self-protection (RASP).

DAST evaluates applications at runtime from outside of the application by executing attack scenarios, monitoring the applications response and detecting vulnerabilities. DAST is commonly used for testing web applications both externally facing and within corporate networks. Common DAST technologies include IBM Appscan, HP WebInspect and Acunetix.

SAST analyzes source code, byte code and binaries to evaluate applications without executing the application. SAST can be used during all phases of the SDLC to identify where coding and design conditions indicative of vulnerabilities exists. Common SAST technologies include HP Fortify, CheckMarx and IBM AppScan Source.
SCA examines libraries from third-party and open source software that are commonly used in an organization’s applications to discover vulnerabilities. SCA enables organizations to continuously monitor common building blocks used in development and promote a secure software supply chain. Common SCA technologies include Blackduck and Sonatype.

IAST is a hybrid analysis technique that uses binary instrumentation to determine vulnerabilities in an application. IAST tools can be used for continuous integration into the testing platform. Common tools include Contrast Security and Quotium Seeker.

RASP protects applications at runtime by monitoring for malicious activity on the basis of behavioral characteristics. RASP technologies are directly embedded in applications or placed runtime environments so they can monitor all inputs and outputs of the application in real-time. Once malicious activity is identified, the RASP technology is then able to automatically take action to protect against the threat, including terminating sessions and sending security alerts to administrators to address threats. A common RASP technology in the marketplace is Contrast.

<table>
<thead>
<tr>
<th>Secure SDLC maturity</th>
<th>Enabling technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate</td>
<td>Dynamic analysis tools (DAST)</td>
</tr>
<tr>
<td>Adapt</td>
<td>Static analysis tools (SAST)</td>
</tr>
<tr>
<td>Anticipate</td>
<td>Software composition analysis (SCA)</td>
</tr>
<tr>
<td></td>
<td>Interactive application security testing tools (IAST)</td>
</tr>
<tr>
<td></td>
<td>Real-time application self-protection (RASP)</td>
</tr>
</tbody>
</table>
**Benefits**

EY’s software security service offering allows organizations to focus developer time on innovation and developing controls to mitigate validated threats, and can help organizations add value by:

- Improving customer trust by making software inherently more secure
- Centralizing compliance activities to eliminate redundancies streamlining efficiency of application development
- Reducing the total cost of development and generating a positive Return On Investment (ROI) by eliminating vulnerabilities early in the development process
- Increased speed of secure software delivery using processes such as Agile and DevOps.

The diagram below shows a simple waterfall development life cycle with a few of the software security services implemented. With identification and gate checks at each phase of the life cycle, the software produced has fewer weaknesses, helping improve customer trust and reduce the overall cost of development.
Detecting software vulnerabilities early in the development process can have significant cost savings over detection and remediation in later stages. According to the National Institute of Standards and Technology (NIST) and EY’s internal research, the cost of remediation of a vulnerability identified in the design phase is more than 30 times less than the cost of remediating a vulnerability in production; similarly, the cost of remediating a vulnerability in test is more than seven times the cost of remediating a vulnerability in development.

**Implementation**

Managed software security is a bespoke service that is tailored to each client’s needs. A typical managed software security engagement usually follows three key phases: plan, build and operate.

The first phase identifies a plan and gets the correct resources engaged and equipped from the client and the EY CoE. This typically includes decisions on technologies, defining processes and procedures, defining roles and responsibilities, and any necessary communications and is completed in the first four to six weeks of the engagement. The second phase focuses on integrating the technologies, then onboarding the initial applications to validate the scanning process. The build phase is typically completed in three months and can begin half-way through phase one. The third phase focuses on onboarding additional applications and identifying tuning opportunities for the tools and processes. The operate phase is on-going throughout the life of the program, beginning after the build kicks-off.

1. **Plan (four to six weeks)**
   - Identify technologies
   - Define processes and procedures
   - Define roles and responsibilities
   - Communicate program

2. **Build (three months)**
   - Implement tool set
   - On-board initial applications

3. **Operate (on-going)**
   - On-board additional applications
   - Tune tools and processes
Once applications are on-boarded to the respective toolset, the results are then reviewed by EY’s global teams to filter out false-positives. After triage between tier 1 and tier 2, results are passed along to tier 3 and the client for final review (see tier explanation below).
Why EY

For more than 15 years, EY’s global Advanced Security Center (ASC) team has been providing a range of cybersecurity services to many of the organization’s largest clients. These services fall within the organization’s recognized Cyber Threat Management (CTM) framework. Our software security service draws upon established skills and resources of our ASC professionals, who have a strong background in all phases of the SDLC in various development methodologies; and are experienced in delivering services in the CTM domain of vulnerability identification.

We differentiate our software security program by developing a customized secure software development life cycle framework that fits within your organization’s existing practices and business needs. Through global collaboration, we seek to build an overarching approach for end-to-end security integration in the SDLC that drives business value and supports accelerated software development methodologies. This framework addresses software security risk identification in internally developed, customized and third-party-developed software. By moving the identification and remediation of software weaknesses to the left of the development life cycle, we can help you reduce the total cost of development and generate a positive ROI by eliminating vulnerabilities early in the development process.

An enterprise-scale-managed program for sustaining software security usually follows three phases: “design”, “transform” and “optimize”. Local members of the ASC work closely with our clients to scope the engagement and undertake the design and transform phases. The optimize phase is undertaken via a collaboration between the global ASC team members.
Software security CoEs help integrate software security practices in the SDLC and can reduce the impact security flaws have on the organization’s software and business. However, with the ever-evolving threat landscape and emergence of faster development methodologies, building a software security CoE has many challenges.

Clients can leverage EY’s skills and experience in the design, transformation and optimization of their software security programs to enhance their current capabilities. EY offers managed software security services to provide clients continuous integration and monitoring of the organization’s application portfolio. Included in the managed software security services are operating multiple testing tools, onboarding applications, performing scans, reviewing results and providing remediation guidance to the development team.

The managed software security service offering supports dynamic application security testing, static application security testing, interactive application security testing and real-time application self-protection providing a three-tier review of identified security flaws in scanned software. This offering enables organizations to focus developer time on innovation, handle only verified vulnerabilities, use accelerated development methodologies in conjunction with security activities and improve customer trust by inherently increasing the security of deployed software.

By leveraging EY’s Advanced Security Center’s expertise, our managed software security services can help to bring end-to-end security integration into the SDLC. With an enterprise-scale, bespoke service that drives business value and supports accelerated software development methodologies this service aims to reduce the total cost of development and generate a positive return on investment (ROI) by helping eliminate vulnerabilities early in the development process.
Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective. Please visit our Insights on governance, risk and compliance series at ey.com/GRCinsights.

How do you find the criminal before they commit the cybercrime? A close look at cyber threat intelligence
ey.com/CTIservices

ey.com/GISS2015

Enhancing your security operations with Active Defense
ey.com/activedefense

Using cyber analytics to help you get on top of cybercrime: Third-generation Security Operations Centers
ey.com/3SOC

Achieving resilience in the cyber ecosystem
ey.com/cyberecosystem

Cybersecurity and the Internet of Things
ey.com/IoT

If you would like assistance or further information in relation to our CTI services, please feel free to contact one of the following ASC team members:

**Americas**

Rishi Pande
Email: rishi.pande@ey.com
Phone: +1 305 415 1908

**EMEIA**

Simon Collins
Email: simon.collins@ie.ey.com
Phone: +353 1 221 2176

**Asia-Pacific**

Steve Lam
Email: steve-yk.lam@ey.com
Phone: +65 6309 8062

Salvatore Coiro
Email: salvatore.coiro@au.ey.com
Phone: +61 39288 8437
If you were under cyber attack, would you ever know?

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly relentless. When one tactic fails, they will try another until they breach an organization's defenses. At the same time, technology is increasing an organization's vulnerability to attack through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services, and the collection and analysis of big data. Our ecosystems of digitally connected entities, people and data increase the likelihood of exposure to cybercrime in both the work and home environment. Even traditionally closed operational technology systems are now being given IP addresses, enabling cyber threats to make their way out of back-office systems and into critical infrastructures such as power generation and transportation systems.

Anticipating cyber attacks is the only way to be ahead of cyber criminals. With our focus on you, we ask better questions about your operations, priorities and vulnerabilities. We then collaborate with you to create innovative answers that help you activate, adapt and anticipate cybercrime. Together, we help you design better outcomes and realize long-lasting results, from strategy to execution.

We believe that when organizations manage cybersecurity better, the world works better.

So, if you were under cyber attack, would you ever know? Ask EY.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2016 EYGM Limited. All Rights Reserved.

1601-1814830
EYG no. 01030-163GBL
ED None

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

About EY’s Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

Through a collaborative, industry-focused approach, EY Advisory combines a wealth of consulting capabilities – strategy, customer, finance, IT, supply chain, people advisory, program management and risk – with a complete understanding of a client’s most complex issues and opportunities, such as digital disruption, innovation, analytics, cybersecurity, risk and transformation. EY Advisory’s high-performance teams also draw on the breadth of EY’s Assurance, Tax and Transaction Advisory service professionals, as well as the organization’s industry centers of excellence, to help clients realize sustainable results.

True to EY’s 150-year heritage in finance and risk, EY Advisory thinks about risk management when working on performance improvement, and performance improvement is top of mind when providing risk management services. EY Advisory also infuses analytics, cybersecurity and digital perspectives into every service offering.

EY Advisory’s global connectivity, diversity and collaborative culture inspires its consultants to ask better questions. EY consultants develop trusted relationships with clients across the C-suite, functions and business unit leadership levels, from Fortune 100 multinationals to leading disruptive innovators. Together, EY works with clients to create innovative answers that help their businesses work better.

The better the question. The better the answer. The better the world works.

EY Risk Advisory Leaders are:

<table>
<thead>
<tr>
<th>Global Risk Leader</th>
<th>+31 88 40 71271</th>
<th><a href="mailto:paul.van.kessel@nl.ey.com">paul.van.kessel@nl.ey.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>+1 612 371 8537</td>
<td><a href="mailto:amy.brachio@ey.com">amy.brachio@ey.com</a></td>
</tr>
<tr>
<td>EMEIA</td>
<td>+971 4 312 9921</td>
<td><a href="mailto:jonathan.blackmore@ae.ey.com">jonathan.blackmore@ae.ey.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>+61 8 9429 2486</td>
<td><a href="mailto:iain.burnet@au.ey.com">iain.burnet@au.ey.com</a></td>
</tr>
<tr>
<td>Japan</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:azuma-yshhr@shinnihon.or.jp">azuma-yshhr@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>

Our Cybersecurity Leaders are:

<table>
<thead>
<tr>
<th>Global Cybersecurity Leader</th>
<th>+44 20 795 15769</th>
<th><a href="mailto:kallan@uk.ey.com">kallan@uk.ey.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>+1 513 612 1591</td>
<td><a href="mailto:bob.sydow@ey.com">bob.sydow@ey.com</a></td>
</tr>
<tr>
<td>EMEIA</td>
<td>+44 207 951 6930</td>
<td><a href="mailto:sgelber@uk.ey.com">sgelber@uk.ey.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>+65 8691 8635</td>
<td>paul.o’<a href="mailto:rourke@sg.ey.com">rourke@sg.ey.com</a></td>
</tr>
<tr>
<td>Japan</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:nagao-shnchr@shinnihon.or.jp">nagao-shnchr@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>