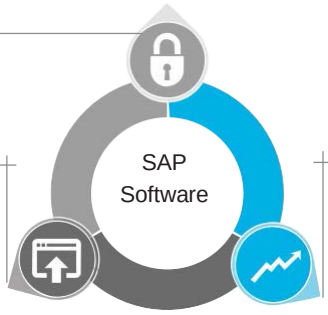
Deloitte.

Deloitte SAP Vulnerability Management

SAP Application Security

SAP application security alone can not remediate many of these vulnerabilities. Changes to system parameters and server configuration may be required.



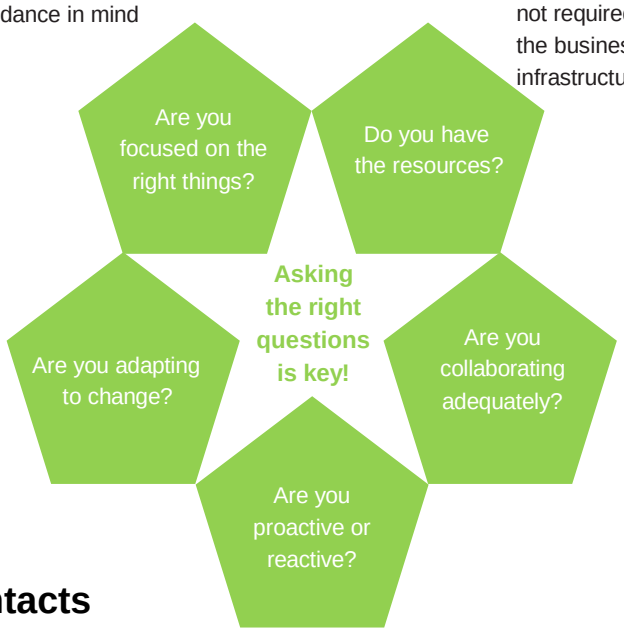
SAP Development

SAP developers are critical to the security of your SAP systems. They must work with the application security team and SAP Basis to make sure that system functionality is appropriately restricted and designed with the latest guidance in mind

SAP Basis

Many times, the SAP Basis team configures the systems based on business use cases and developer requirements. Developers bring insight related to the breadth of services and connectors needed; Basis should deactivate any that are not required to support the business or the infrastructure.

Remediation is a collaborative effort and takes more than just your application security team!



Contacts

Mike Kosonog
Partner
Enterprise Application Integrity Solution Leader
Cyber Risk Services
Deloitte & Touche LLP
+ 1 313 396 3622
mkosonog@deloitte.com

Kevin Heckel
Managing Director
Cyber Risk Services
Deloitte & Touche LLP
+ 1 330 283 2866
kheckel@deloitte.com

Ben Fitts
Senior Manager
Cyber Risk Services
Deloitte & Touche LLP
+1 678 362 6330
bfittsdeloitte.com

The CISO dilemma:

- I have to protect my whole organization…
- Cyber criminals only have to find a single point of entry…
- How can I be everywhere at once?

Vulnerability Identification & Remediation: Every SAP landscape is unique, but there are three areas that standout in this emerging area of risk.

Security Note Remediation—Since SAP released new guidance regarding the timely application of security notes, many companies have not been able to keep pace with the monthly security note releases, especially if there are significant projects on the horizon.

Hardening Remote Function Calls (RFCs)—As the main integration technology between SAP systems, it is imperative to secure these connections against vulnerabilities that may exist. Without adequate precautions in place, an attacker can swiftly move from a compromised non-production system to production systems.

Securing the Internet Communication Framework (ICF)—In the haste to stand-up new system environments, some organizations often unknowingly leave unused ICF services active expanding their threat landscape.

Threat Modelling: Using vulnerability assessment reports, we work with your technology and business teams to develop likely threat scenarios. This exercise profiles likely perpetrators, identifies desirable targets and contextualizes the assessment report findings to develop a tailored view of your threat landscape. With this perspective, remediation efforts can be focused on those vulnerabilities most likely to be exploited with the largest potential impact.

SAP Cybersecurity AMS: Integrating continuous monitoring capabilities with Deloitte's SAP experience, we can help identify and remediate emerging vulnerabilities. Detecting any "Net New" vulnerabilities that may be created by ongoing projects can help achieve remediation before they become a part of the production environment. This can substantially reduce risk and create significant cost savings or avoidance.