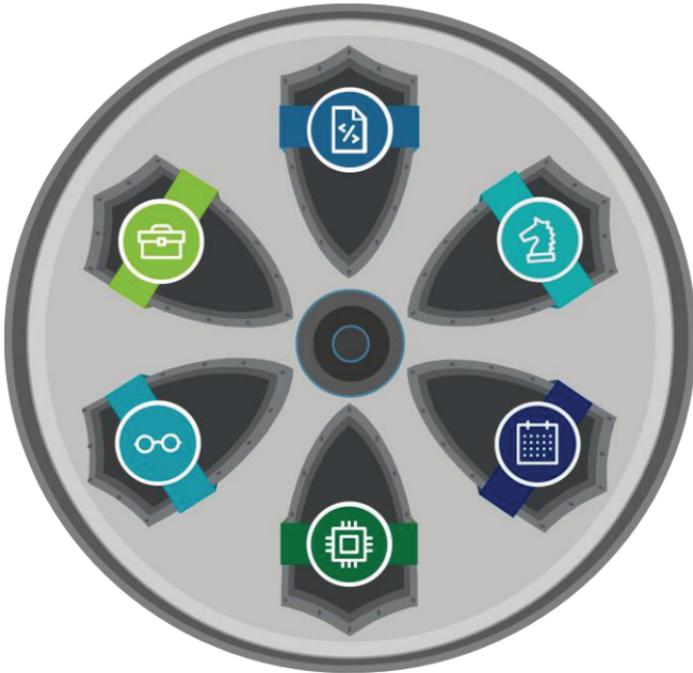


Deloitte.

Vigilant ShieldSM

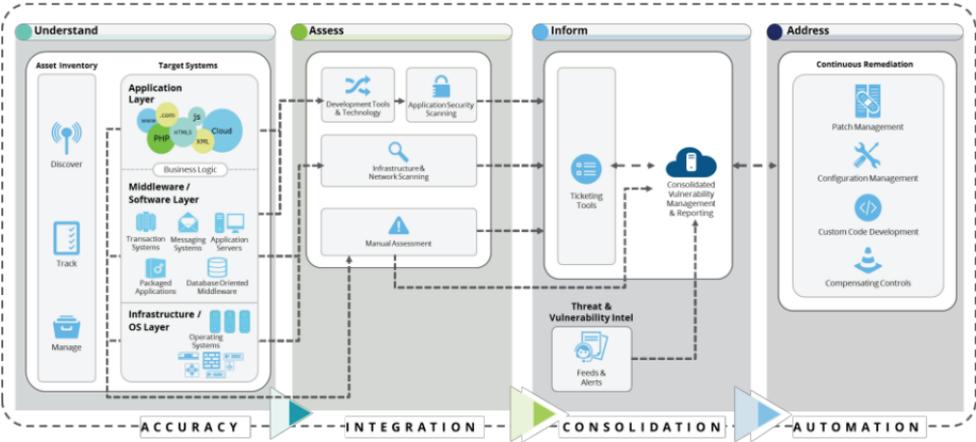
a better approach to vulnerability management and advanced testing



Most cyber breaches could have been prevented. Many system and application vulnerabilities remain unpatched for months (if not years) after a solution is available. Attackers exploit them. So why do we allow known vulnerabilities to persist?

The answer is not straightforward.

Numerous, interdependent parts must work in concert.



Deloitte's approach brings these components together while accelerating the maturity curve.

AUTOMATION & SECURE AGILE DEVELOPMENT

Program Development and Risk Reporting



Application Testing and Secure Development



Asset Discovery Support



Advanced Manual Penetration Testing



Infrastructure Scanning and Analysis



Patch & Configuration Management Support



Remediating critical vulnerabilities is not as simple as clicking a button and deploying a patch.

Large businesses operate dynamically across multiple lines and leadership hierarchies. Their technology footprint is always complex and often unwieldy. New and legacy technologies are forced to co-exist. Systems deemed to be critical are often interconnected with other less critical IT assets further blurring the lines.

COMPETING PRIORITIES

Finding ample, skilled talent



Knowledge and understanding of threats



Tracking all assets



Prioritizing remediation



Mapping the environment and monitoring traffic



Continuous testing and risk reporting



Meanwhile, applications are being developed at a breakneck pace. Scanning is challenging and is rarely straightforward, with security taking a second position behind speed to market. Worse still, many of those applications are co-developed by multiple teams and use components that are simply plugged in and trusted.

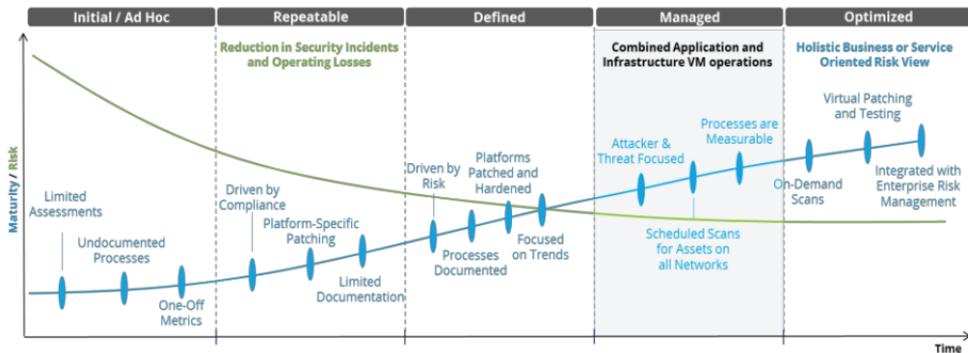
...and that's the 'known' environment.

IT infrastructure and applications often emerge outside the control of IT itself. It's hard enough to protect the assets you know about, it's impossible to protect those that are created in unsanctioned, ad hoc cloud environments.

Effective vulnerability management is difficult. Discipline and hygiene, while important components, are not enough.

Operational Capability Maturity Model

The Vulnerability Management (VM) Capability Maturity Model below acts as a reference roadmap for organizations looking to add and enhance operational capabilities throughout the VM lifecycle



QUALIFICATIONS

Global Financial Services Institution

Issues: Inability to execute on large volume of assessments. Static resource pool unable to scale up and down with fluctuating demand

Solution: Successfully implemented managed service to execute entire demand of application and network security testing to reveal the cyber risk exposure.

Value Added: Provided scalable and global delivery of services 24x5x365 to accommodate changing demand. Optimized execution efficiency of controls to yield higher throughput. Aggregated reporting to provide a consolidated view of risk enabling efficient remediation.

Fortune 200 Technology Company

Issues: Lack of awareness on vulnerability and patch management current state maturity. Lack of vision for target state programs

Solution: Performed risk-based assessment of the operating companies' vulnerability and patch management programs and developed recommendations to address gaps.

Value Added: Aligned assessment with overall operations. Defined steps and requirements to address gaps. Provided recommendations to assist in improvement initiatives. Incorporated industry context to describe target state against industry peers.

For more information please contact:



Lior Kalev
Head of Cyber Risk Services
Deloitte Israel
lkalev@deloitte.co.il
03-6085222
052-3463496



Avi Sarfati
Senior Manager,
Cyber Risk Services
Deloitte Israel
asarfati@deloitte.co.il
03-6085222
054-5664744

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.