DEMYSTIFYING SECURITY ARCHITECTURE

WHAT DO SECURITY ARCHITECTS DO?

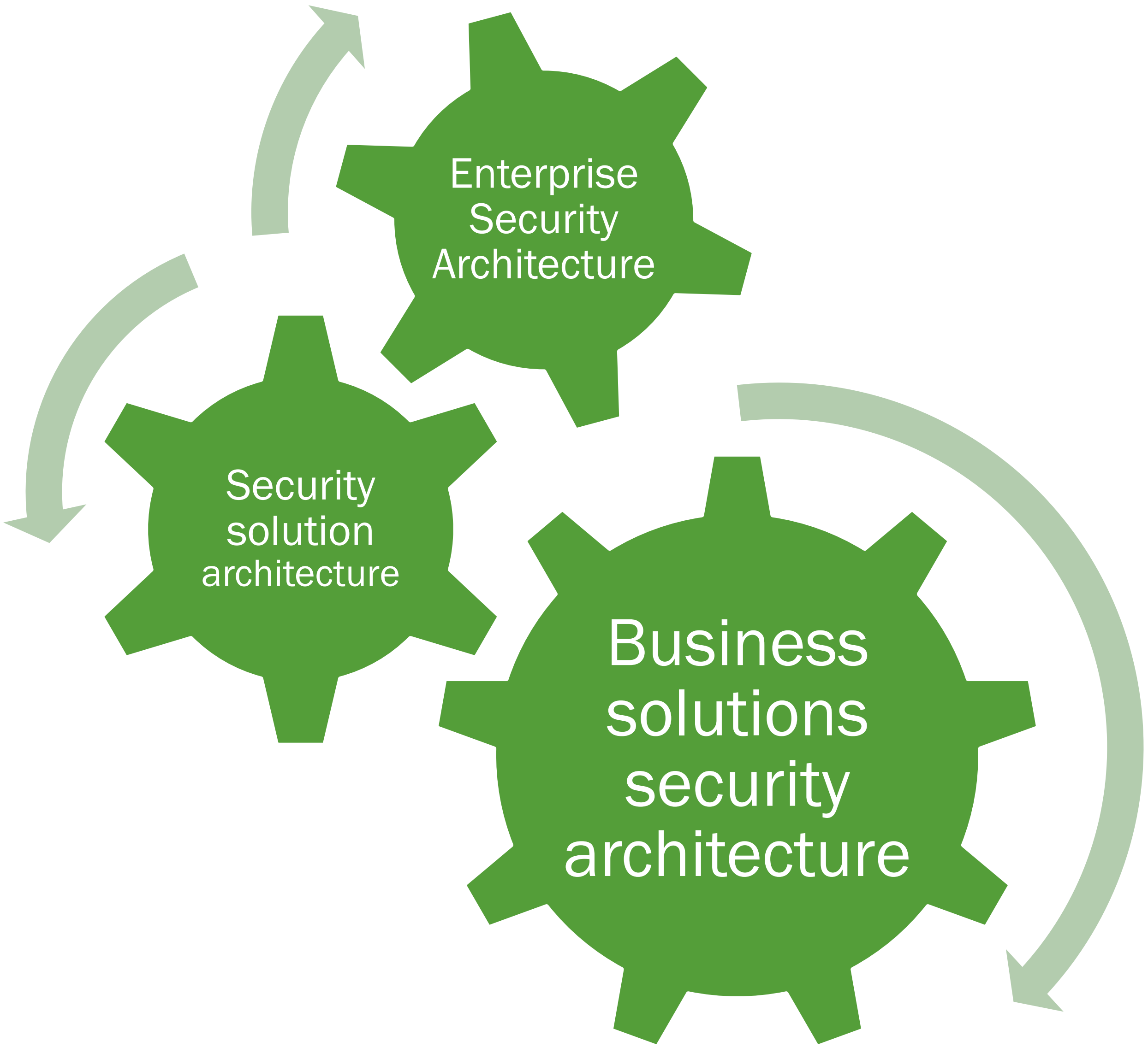
WHY ARE THEY DOING IT?

BY ILYA POLYAKOV

CHIEF SECURITY ARCHITECT AND IDAM PRODUCT OWNER AT DEPARTMENT OF PLANNING, HOUSING AND INFRASTRUCTURE, NSW GOVERNMENT

INTRO

TO KNOW WHY, LETS SEE WHAT IS SECURITY ARCHITECTURE



Enterprise Security Architecture

Security solution architecture

Business solutions security architecture

ENTERPRISE SECURITY ARCHITECTURE

- Most important but under-appreciated part of security architecture
- Aligns organisation goals to the security capabilities
- Takes into account compliance requirements and risk appetite
- Maps how security capabilities of organisation are either managing security risk or enabling organisation to grow

Common deliverables:

- Security subdomain reference architectures
- Security technology roadmaps
- Security strategy

Common skills of the practitioners:

- Enterprise architects with deep understanding of security domain
- SABSA, TOGAF

SECURITY SOLUTIONS ARCHITECTURE

- Works hand in hand with ESA
- Security Architect is architecting and designing solution to create security capability defined by ESA

Common deliverables:

- High level architecture for the security capability
- Detail design for the security capability
- RFP/RFQ documentation
- Tender evaluation and technology selection

Common skills of the practitioners:

- Solution architects with deep understanding of security domain
- Primary: Some flavour of solution design methodology, technology that is being used, project management, product management, vendor management
- Secondary: understanding of SABSA, TOGAF

BUSINESS SOLUTIONS SECURITY ARCHITECTURE

- By far the most widespread understanding of “Security architecture”term
- Works mainly as compliance mechanism for the business solutions
- Performs security controls assessment for business solutions
- Performs threat and risk assessment for business solutions
- Consulting to the business how to meet security requirements of the organisation
- Creating security patterns for org wide reuse to improve compliance and speed of solution implementations

Common deliverables:

- Maturity assessments
- Control assessments
- Security patterns
- Security recommendations to the business
- Various audits

Common skills of the practitioners:

- Knowledge of various standards and frameworks (ISO 27001, NIST, MITRE, Essential 8, Cyber Security Policy of NSW, ISM etc.
- Knowledge of organisation’s internal policies and standards
- Primary: security audit, threat and risk assessment, risk management, risk mitigation, CISSP, CISM other comprehensive security certifications
- Secondary: understanding of SABSA, TOGAF

BUSINESS SOLUTIONS SECURITY ARCHITECTURE

- The most time-consuming sub-capability
- Current business problem – limited budgets and low appetite to hire extra people

Study case:

- DPHI portfolio is around 20,000 end users
- 5 architects in security architecture
- 80% of assessments is done within 3 days

HOW?!?!

BUSINESS SOLUTIONS SECURITY ARCHITECTURE – THAT'S HOW

- We created online form with list of questions that are mapping to security controls important to our security objectives and compliance with policies (76 questions)
- Business representatives fills in the form, the task is created automatically and assigned to the team queue
- Controls assessment: It is picked up the same day, security architect makes a decision based on answers if the risk in the solution is high enough to do formal assessment (), otherwise recommendations are sent to the business and the solution is approved in >80% of cases. This takes 1-2 business days.
- Formal threat and risk assessment: risk-based approach <20% of cases are referred to do formal assessment (5-20 days depending on the system)

Why does it work?

- Security architect is empowered to make a call and approve the solution
- Security architect is empowered to give recommendations or reject a solution
- The team was engaged and heavily involved in resolving our business problem, so deep sense of ownership is embedded in the team
- The questions are clear and easy to understand
- They cover just enough

QUESTIONS?

Feel free to reach out to me directly ilya@polyakov.au

Or via LinkedIn https://www.linkedin.com/in/ily-polyakov/