PASTA THREAT MODELING RACI DIAGRAM

APPLICATION THREAT MODELING ACTIVITIES per STAGE	BU/Product Groups						Corporate Functions							3rd Party	
	MGT	PMO	BA	ARC	SWE	QA	SYS	SOC	RL	PC	SA	EA	CTO	VA	PT
STAGE 1 - DEFINE BUSINESS OBJECTIVES - Est. New TM = 2-4 hours | Est. Repeat TM = < 1 hour	A	R	R	A	I	I	I	–	I	R	I	I	R	–	–
Obtain business objectives for product or application	A	I	R	A	I	I	I	–	I	–	–	I	I	–	–
Identify regulatory compliance obligations	A	I	I	A	I	I	I	–	I	R	–	I	I	–	–
Define a risk profile or business criticality level for the application	A	I	I	A	I	I	I	–	I	C	I	I	R	–	–
Identify the key business use cases for the application/product	A	R	R	A	I	I	I	–	I	–	–	I	I	–	–
STAGE 2 - TECHNICAL SCOPE - Est. New TM = 3-4 hours | Est. Repeat TM = 1-3 hours	I	I	C	A	R/A	C	I	–	I	–	I	C	I	–	–
Enumerate software applications/database in support of product/application	I	I	C	A	R/A	C	I	–	–	–	–	C	I	–	–
Identify any client-side technologies (Flash, DHTML5, etc.)	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Enumerate system platforms that support product/application	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Identify all application/product actors	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Enumerate services needed for application/product use & management	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Enumerate 3rd party COTS needed for solution	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Identify 3rd party infrastructures, cloud solutions, hosted networks, mobile devices	I	I	C	A	R/A	C	I	–	–	–	I	C	I	–	–
Obtain business objectives for product or application	I	I	C	A	R/A	C	I	–	I	–	I	C	I	–	–
STAGE 3 - APPLICATION DECOMPOSITION - Est. New TM = 8 hours | Est. Repeat TM = 4 hours	I	I	I	A	R	C	C	–	I	–	–	C	–	–	–
Perform data flow diagram of application environment	I	I	I	A	R	I	C	–	–	–	–	C	–	–	–
Define application trust boundaries/trust models	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
Enumerate application actors	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
Identify any stored procedures/batch processing	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
Enumerate all application use cases (ex: login, account update, delete users, etc.)	I	I	I	A	R	C	C	–	–	–	–	C	–	–	–
STAGE 4 - THREAT ANALYSIS - Est. New TM = 6 hours | Est. Repeat TM = 2 hours	I	I	R/A	A	R/A	R/A	C	C	–	–	–	I	–	–	–
Gather/correlate relevant threat intel from internal/external threat groups	I	I	R/A	A	C	I	C	C	–	–	–	C	–	–	–
Review recent log data around application environment for heightened security alerts	–	–	I	A	R	R/A	I	C	–	–	–	C	–	–	–
Gather audit reports around access control violations	–	I	I	A	R	C	I	C	–	–	–	C	–	–	–
Identify probable threat motives, attack vectors & misuse cases	I	I	I	A	R/A	C	I	C	–	–	–	C	–	–	–
STAGE 5 - VULNERABILITY ASSESSMENT - Est. New TM = 12 hours | Est. Repeat TM = 6 hours	I	I	I	A	R	C	I	C	I	–	–	I	–	R/A	R
Conduct targeted vulnerability scans based upon threat analysis	–	–	–	A	R	C	I	C	I	–	–	I	–	R	R
Identify weak design patterns in architecture	–	–	–	A	R	C	I	–	–	–	–	C	–	R	C
Review/correlate existing vulnerability data	I	I	I	A	R	I	I	C	–	–	–	I	–	R/A	I
Map vulnerabilities to attack tree	–	I	I	A	R	I	I	–	–	–	–	C	–	C	I
STAGE 6 - ATTACK ENUMERATION - Est. New TM = 10 hours | Est. Repeat TM = 5 hours	I	I	I	A	R	R	–	–	I	–	–	C	I	I	R/A
Enumerate all inherent and targeted attacks for product/application	I	I	I	A	R	C	–	–	I	–	–	C	I	I	R/A
Map attack patterns to attack tree vulnerability branches (attack tree finalization)	–	–	–	A	R	C	–	–	I	–	–	C	–	I	A
Conduct targeted attacks to determine probability level of attack patterns	–	–	–	A	C	R	–	–	I	–	–	C	–	I	R/A
Reform threat analysis based upon exploitation results	I	I	I	A	R	C	–	–	I	–	–	C	I	I	C
STAGE 7 - RESIDUAL RISK ANALYSIS - Est. New & Repeat TM = 5 days (inc. countermeasure dev.)	C	I	I	A	R	C	C	C	I	I	C	C	I	I	R
Review application/product risk analysis based upon completed threat analysis	I	I	I	A	R	C	I	C	I	I	C	C	I	I	R
List recommended countermeasures for residual risk reduction	I	I	I	A	R	C	C	C	I	I	C	C	I	I	R
Re-evaluate overall application risk profile and report.	C	I	I	A	R	C	I	I	I	C	C	C	I	I	I

MGT *Product Mgmt*
PMO *Project Mgmt*
BA *Business Analyst*
ARC *Architect*
SWE *Software Engineer*
QA *Quality Assurance*
SYS *SysAdmin*
SOC *Security Operations*
RL *IT Risk Leader*
PC *Product Compliance*
SA *Software Assurance*
EA *Enterprise Architect*
CTO *Administration*
VA *Vuln Assessor*
PT *Pen Tester*

Corporate Functions

Office of the CTO
Compliance
Security (ISRM)

RACI Legend

R	Responsible
A	Accountable
C	Consulted (2 way)
I	Informed (1 way)

VERSPRITE

VerSprite's Process for Attack, Simulation and Threat Analysis (PASTA) benefits stakeholders by assessing threats to your application environment by designing secure applications and deciding how to mitigate risks by applying risk mitigation strategies. Examples include Architects, Developers, Security Testers, Project Managers, Business Managers, and Information Risk Officers. **Learn more >>**