VERSPRITE

Application Security

– BlackHat Mindset to Emulate Real World Attacks

A key goal of testing exploits is determining how easy and impactful successful exploits are against target networks, systems, and applications. Whitehats in today's industry can often become more enamored with the hunt versus improving technique and truly understanding impact or attack viability as part of a broader threat context.

VerSprite's Application Security Services (AppSec) group focuses on emulating cybercrime and simulating test scenarios that not only reflect current attack patterns, but also threat motives. Our group also focuses on integrated security testing to help organizations integrate AppSec initiatives sooner within a given SDLC process.

Penetration Testing

The key differentiator of a VerSprite penetration test is in our ability to look at the bigger picture. By not limiting our approach to encompass only one set of controls (network, application, physical, system) to defeat, we are able to simulate a true attack scenario. A true attacker will not stop if the front door of your network is locked, and neither will we.

Red Teaming

Our red team exercises are designed to be a comprehensive test of physical, logical, and process based controls. We use a combination of physical, social engineering, mobile, web, networking, and wireless attacks to bring a full arsenal of security tests aimed at exercising your current defensive security posture.

Mobile Security Testing

Mobile applications are being deployed each and every day with a trove of vulnerabilities that find their roots in the lack of proper security assessments. VerSprite recognizes that mobile technologies are leading the future in enterprises and small businesses alike. We offer exclusive security services for mobile application penetration pesting, source code review, and threat modeling. Secure and protect your application, product, and image.

VERSPRITE

Application Security

Application Threat Modeling

To accurately and thoroughly assess the security of a web application requires not only a combination of automated and manual testing, but also an understanding of the software behind the application. Gathering comprehensive information through reconnaissance and analyzing it effectively does not stop at running tools. Having a background in a wide variety of technologies leads to efficient use of attack vectors and successful security assessments.

– AppSec Approach Based on Threat Modeling

1. **Look Ma No Tools**: Tools are great for breadth, but they dull the senses when getting behind the wheel of exploitation. Our team codes techniques to better enumerate, fuzz, and reverse application components in scope. We emulate cyber-criminal intent far beyond the bounties and traditional pen testing groups.

2. **Application Threat Models**: What are you testing for? Our tests fit into a bigger picture of an application threat model that encompasses not only app components, frameworks, and use cases, but also threat motives, architecture, deployments, actor permission sets, and more.

3. **S-SDLC Integration**: Still pen testing like it is 2005 (post-development, post-implementation)? VerSprite provides cost effective unit security testing to mirror client SDLC methodologies to find issues within the development process and build remediation in sooner.

4. **A Better Consistent Craft**: Our team stays hungry, never resting on a 'standard' set of techniques. Attack patterns change, as does our team's craft. Consistency is also important as we pride ourselves in ensuring that our peer review process in every facet of our approach leverages ideas and skill sets of a collective team.

VerSprite Consulting
Pro Service Listings 2019

Atlanta, GA • VerSprite.com • Info@VerSprite.com

VERSPRITE

Service ID	Service Type	Service Description
APPSEC01	**Web Application Testing**	Manual testing, business logic exploitation, fuzzing techniques to identify weaknesses in web applications and the underlying DOM calls made to other layers of the application environment. Expose programmatic and architectural application flaws for web applications.
APPSEC02	**Source Code Analysis**	Manual review of code sets in order to derive possible security holes in programming logic and function.
APPSEC03	**Application Threat Modeling**	Apply PASTA risk-centric threat modeling methodology and correlate to software and security workflows based upon risk levels derived threat analysis and likely attack patterns identified for a client application environment or set of environments. Integrates with SAMM maturity modeling.
APPSEC04	**S-SDLC/SDL-IT**	Work to develop a Secure System Development Lifecycle (S-SDLC) for development teams. Training hours encompassed to address key application threats and vulnerabilities that should be repeatedly addressed by the SDLC/SDL-IT process.
APPSEC05	**Organizational Threat Model**	VerSprite's adversarial red team is focused on emulating criminal cyber-criminals that seek to extract IP, PII, or achieve other nefarious motives against a target physical, logical entity. Exercises are conducted to determine if targeted attacks against specific logical, targets would be plausible.
APPSEC06	**Mobile Security Testing**	Static and dynamic security analysis of mobile software. Mobile web APIs are inspected and fuzzed with rogue parameters that are focused on injecting malicious payloads, circumventing authorization model, exfiltration stored data, and more.
APPSEC07	**Countermeasures as Code**	Identify coding flaws within applications prior to the general availability of an application product produced and providing remediation work to rectify insecure coding flaws that introduce risks to the application, its data, and the overall company.
BCP01	**Business Continuity Planning**	VerSprite provides a repeatable, customized, and executable business continuity plan. Prepare for the unexpected and ensure that key service components remain operational.

Service ID	Service Type	Service Description
BCP02	**Disaster Recovery Planning**	Outsourced or co-sourced Disaster Recovery Planning against logical and physical threats to business continuity.
BCP03	**Business Impact Analysis**	VerSprite quantifies the risks of security in real and measurable business terms. Our examination stems from regressive financial analysis of internal cost structures and other costs not clear to those unfamiliar with operational dependencies across varying industries. VerSprite works with Finance, Operations, and Risk Management in order to derive business impact levels.
BCP04	**Redundant Data Storage**	Provide redundant cold or warm site to clients with <500 TB of data needs.
BCP05	**Tabletop Exercises**	VerSprite provides tabletop exercises around threat scenarios depicted in Business Continuity Planning or Disaster Recovery Planning in order to exercise client plans and evaluate response times, actions, and overall effort. VerSprite develops the content and facilitates the event with roundtable meetings.
CLD01	**Cloud Security Auditing**	VerSprite assesses public Cloud security posture against common frameworks and standards. VerSprite provides remediation recommendations that are customized to each client environment.
CLD02	**Cloud Security Monitoring**	VerSprite provides continuous Cloud security auditing, monitoring all changes in a public Cloud environment and providing notifications of any changes which introduce vulnerabilities or weaken an organization's security posture.
CLD03	**Real-Time Cloud Security Enforcement**	VerSprite provides customized security monitoring services which react immediately to enforce policies on every change within an environment. VerSprite writes LAMBDA scripts that fire when there are changes within an AWS environment and force compliance by either undoing the most recent malicious change, or by powering down systems that are being deployed in a non-compliant way. Customized to each unique environment.
CMP01	**3rd Party Security Audits Management**	VerSprite provides clients with a service to address compliance-related requirements.. Many of these audits are based on industry standards and regulatory requirements. (Also serves as generic compliance readiness and control testing.)

Service ID	Service Type	Service Description
CMP02	**HIPAA Compliance**	Security audits around HIPAA's Security and Breach notification rules. Reviews safeguards as defined by the law and helps clients review, test, and evaluate the control effectiveness for controls protecting PHI. Encompasses both a technological and non-tech review of an organization's defined controls. (Also includes breach readiness and use of BA contracts.)
CMP03	**PCI Readiness Assessment**	Pre-audit PCI Testing of controls mandated by PCI-DSS. Helping clients evaluate the scope of systems in and around an their CDE and to define where acceptable controls may be leveraged or developed in order to meet regulatory guidelines. This service can also encompass the remediation efforts that clients may have around PCI compliance gaps.
CMP04	**Data Privacy Assessments**	Evaluate the exposure level of data, managed by client services and products, which may have infringements around various privacy laws and general guidelines of use. Data identification, data flow analysis, retention, management, and impact of loss and misuse are all covered as part of data privacy security assessments. Focus on privacy laws like HIPAA, GDPR, Mass Privacy and more can also be leveraged to share with clients how they fare with regard to requirements around data importing/exporting.
GPR01	**Geo-Cyber Risk Exposure Advisory Service**	Comprehensive assessment of risks and opportunities at the intersection of cybersecurity and geopolitics, helping companies understand their vulnerabilities and anticipate how changes could affect business continuity as they contend with a changing operating environment.
GPR02	**Market Entry Advisory Service**	Comprehensive reports in preparation for a company's decision to explore or enter a new market or sector segment, to identify risks and opportunities in new business and security environments.
GPR03	**Mergers & Acquisition / Joint Partnership Due Diligence Advisory Service**	Due diligence assessments in support of M&A processes and prospective joint partnerships, to identify any possible problems or legal and reputational risks associated with such ventures.
GPR04	**Supply Chain Risk Advisory Service**	Assessments of a comprehensive supply chain security strategy which aggregates vendor risk and partnership due diligence, evaluating threats to the collective data flow supply chain.
GPR05	**On-Demand Consultation**	Hourly on-demand consultations with a senior member of the Geopolitical Risk practice to answer questions, provide insight, and suggest offerings customized to address immediate needs.

Service ID	Service Type	Service Description
GPR06	**Interactive Diagnostic Simulation**	Anticipate and respond to changing operations conditions and crises. Understand which business processes are effective, insufficient, or inadequately integrated to workflows. Perform hypothetical situation exercises featuring various scenarios to prepare for potential threats.
GPR07	**Interactive Analytic Simulation**	Answer questions interactively, with the involvement of representatives from departments across the company, to explore issues from multiple perspectives and create cohesive strategies for pursuing a business goal. Perform hypothetical situation exercises. Receive a summary report and recommended actions.
GPR08	**Interactive Training Simulation**	Integrate new processes, practice business continuity plans, and prepare employees to see their daily work through the lens of cyber-geopolitics. Perform hypothetical situation exercises. Receive a summary report and recommended actions.
GV01	**Governance Related**	Development of security policies, standards, guidelines and other enterprise-wide or issue-specific artifacts that sustain security governance and the ISM program (does not include secure coding standards).
GV02	**Maturity Modeling**	Measure maturity levels of processes and controls relative to maturity models.
GV03	**Benchmark Testing**	Measure existing security and/or compliance controls against an internally-defined or externally-defined benchmark or framework of controls.
GV04	**Security Awareness/Training**	Outsourced security awareness training or development of security awareness materials that are tailored to client environment and business.
GV05	**Security Architecture Services**	Provide security architecture expertise on client server application environments within private, semi-public, and public networks.

Service ID	Service Type	Service Description
GV06	**Secure Coding Standards**	Develop a suite of tailored secure coding standards that prescribe secure coding requirements for various frameworks/languages.
GV07	**ISM Program Dev**	Develop a sustainable and tailored ISM program for clients.
IR01	**Intrusion Handling & Response**	Provide intrusion detection and analysis of client networks and encompassing assets in order to derive source, problem, and remediation planning efforts.
IR02	**Forensic Analysis**	In-depth forensic analysis of data retrieved from client networks in order to clearly identify issues related to cause, accountability, and likely attack patterns used. Customizable for legal response.
IR03	**IR Tabletop**	Conduct a simulation breach or security incident or series of incidents that test the responsive nature and IR plan. Organize a cross section of key leaders and individuals in order to have them weigh in on post incident actions. Assess their response levels and actions based upon recommended security best practices and in consideration of business impact.
IR04	**Compromise Assessments**	Engagement to evaluate whether or not a defined scope of client infrastructure is actually already compromised by a threat actor or malware agent. This helps to ensure that a clean baseline of infrastructure activity is monitored versus one that is tainted with an active compromise.
RM01	**Risk Assessment Services**	Application of risk assessment methodology to derive business risk resulting from security threats or incidents.
RM02	**Vendor Risk Assessments**	Security risk analysis against client vendors in order to identify high risk vendors, assign risk priorities, identify risk issues, and broker remediation efforts.

VerSprite Consulting Pro Service Listings 2019
Atlanta, GA • VerSprite.com • Info@VerSprite.com

VERSPRITE

Service ID	Service Type	Service Description
RM03	**Hybrid Risk Assessment**	Advanced risk assessment that is aimed to correlate risk analysis efforts across multiple technology and business domains in order to identify and quantify financial risk levels.
RM04	**Remediation Management**	Outsourced service for managing remediation workflow and providing assistance with HIGH risk remediation items, while adhering to client change control procedures.
RM05	**M&A Security Assessment**	Assess security posture of company to be acquired or merged with client organization.
RM06	**Red Teaming/ Social Engineering**	Provide social engineering attacks in order to identify holes in security awareness amongst company personnel. Conducted in person, over phone, email, IM, and SMS.
TVM01	**DevSecOps / SecDevOps Training/Consulting**	Cloud based security audits that focus on both operational and technical security controls that can be optimized for the security, compliance, and more efficient ways to manage Cloud infrastructure sprawl and prevent misconfigurations that can lead to data leakage and web-related threats.
TVM02	**Managed Log Management/ Monitoring**	Managed and monitored centralized logging for your environments. You ship your logs to our service, our AI/ML framework watches the logs for anomalous behavior, and we notify you of malicious or suspicious activity following your custom escalation policy. Logs made to be searchable and allow you to archive them at no additional charge.
TVM03	**Threat Hunting**	Tailored threat analytics for clients, based upon a client-defined threat model. Threats will be hunted, researched, and correlated to a client's threat model in order to identify the susceptibility of threat actors against client target applications, Cloud infrastructure, networks, etc.
TVM04	**Vulnerability Assessments**	VerSprite provides vulnerability scanning services to identify network and platform-related security weaknesses or holes.
TVM05	**Penetration Testing**	Application of exploitation frameworks in order to exercise attacks against network and platform related vulnerabilities.
TVM05	**Vulnerability Information Sharing Threat Analysis (VISTA)**	VerSprite's VISTA platform facilitates the management of vulnerability scanning, validation of false positives associated with vulnerability results, correlation to relevant threat feeds, and overall reflection of a current threat model anchored by both qualified vulnerability and threat intelligence data.
TVM06	**vSOC**	VerSprite provides 24/7 enterprise security monitoring using cloud-based architecture, which allows a completely remote team to deliver the same experience of having an in-house SOC. This virtual approach allows for flexibility and scalability.