VULNERABILITY ASSESSMENT & PENETRATION TESTING

Our Vulnerability Assessment (**VA**) & Penetration Testing (**PT**) provides a comprehensive evaluation and complete view of your organizations' security posture. Our assessments are designed to proactively identify and prevent any potential exploitation of any existing security vulnerability. Our Covert Threat experts' objectives are to identify cybersecurity flaws and thoroughly test the extent of an intrusions effect compromising the network infrastructure through exploitation.

COVERT THREATS' BOX CLEVER APPROACH

KNOW THE DIFFERENCE!

	VULNERABILITY ASSESSMENT	PENETRATION TESTING
Frequency	Monthly, plus additional test after changes to network	At least yearly, typically quarterly or semi-annually
Reporting	Comprehensive list of vulnerabilities, including false positives	A detailed document listing all vulnerabilities successfully exploited
Performed By	In-house security or third-party vendor like **Covert Threat**	Third-party penetration testing services provider like **Covert Threat**
Value	Uncovers a wide range of possible vulnerabilities	Identifies & reduces weaknesses by validating through exploitation

ADVISORY SOLUTIONS

	VULNERABILITY ASSESSMENT	PENETRATION TESTING
Network	Network devices vulnerabilities; servers, switches & laptops etc	Network devices vulnerabilities exploited (internal & External Hosts)
Cloud	Discovery of vulnerabilities on the cloud (Azure, AWS, GCP)	Identifying and exploiting cloud vulnerabilities (Azure, AWS, GCP)
Web Apps	Identification of web app vulnerabilities using OWASP Top 10	Exploiting web app vulnerabilities to identify & remediate flaws
IoT	Exposing smart devices vulnerabilities connected on the network	Testing IoT defenses, uncovering vulnerabilities and exploiting them
Wireless	Enumerating wireless devices and uncovering vulnerabilities	Attempting to gain unauthorized access to wireless networks
Mobile	Uncover vulnerabilities on mobile apps; iOS (IPA) & Android (APK)	Testing of iOS (IPA) & Android (APK) apps through exploitation
Social Eng		Testing human defenses of an organization; emails, USB, phone etc.
Continuous PT		Continuous testing for frequent changes and newly developed code
Active Directory		Reconnaissance of active directory to attempt account takeovers

COVERT THREATS APPROACH & METHODOLOGY

VA	*PT*		
X	X	*Define Scope*	Detailed outline with the customer to define what assets are in scope.
X	X	*Information Gathering*	Map out the corporate infrastructure based on services, ports, hardware, software and operating system.
X	X	*Threat Modeling*	Determine mission critical and connected assets to corporate data through white, gray or black box approach.
X	X	*Vulnerability Analysis*	Utilize enterprise and custom scanning tools to uncover vulnerabilities.
	X	*Exploitation*	Exploit vulnerabilities discovered in the vulnerability analysis stage with custom and generic exploitation scripts.
	X	*Post Exploitation*	Successful exploitation's lead to privilege escalation and new vulnerabilities to test for exploitation.
X	X	*Reporting*	Creation of Executive and Detail technical reports for both management and remediation team.
X	X	*Exit Call*	Call scheduled with customers management & remediation team explaining detailed findings.

WHAT YOU RECEIVE

EXECUTIVE SUMMARY REPORT

Designed for managers, executives and board of directors.

This report contains a high overview of the organization's overall security posture with vulnerabilities and, or successful exploitation's ranging from critical to low.

DETAILED TECHINCAL REPORT

Designed for technical teams apart of the remediation.

This report contains a detailed description of all vulnerabilities and, or successful exploitation's ranging from critical to low with remediation recommendations.

CONSULTING

Our Consulting services provides assistance through governance and oversight on your organizations' current cyber program. Covert Threats' team of experts assist in the development of a comprehensive plan of action your organization requires to deal with risks to prevent potential future breaches and ultimately mitigate their impact. Our approach assists enterprises in designing a customized cyber program that aligns people, processes, and technology with enterprise business priorities and risks.

The design of a cyber security program is a complex task for a majority of organizations as it must address a continuously evolving environment. Our consultants work to establish a cyber program to create operational efficiencies, maximum return on technology investments, and advanced data protection.

WHY COVERT THREATS CONSULTING?

CONSULTING BENEFITS

- *Provides the board with greater visibility on cyber risk*
- *Provides framework and guidance for ongoing improvement*
- *Reducing the number of risks a business faces*
- *Reducing the costs arising from these risks*

CONSULTING SERVICE GOALS

- *Identifies and protects key items, what matters most.*
- *Develops a road-map, bringing a greater level of security maturity.*
- *Recommends best practices to assist enterprises to better execute their security program.*

CONSULTING SOLUTIONS

GAP ANALYSIS
Expert analysis to Identify security gaps between current and ideal state of an enterprise's security posture

RISK ASSESSMENT
Reveal risks associated within an organization. Perfect balance between compliance and security

EXTERNAL THREAT ASSESSMENT
Reveal end-points exposed externally which malicious attackers may target with attempts to gain access to your network

BUSINESS CONTINUITY PLANNING
Comprehensive planning to continue business functions in a time of crisis through in-depth evaluation of current business processes

DISASTER RECOVERY PLANNING
In the event of a crisis, a well-established back-up and recovery plan is vital to ensure business can continue it operation

VENDOR MANAGEMENT
Comprehensive outsourcing risk management program to govern and mitigate risk from third parties involved in the business process

POLICIES & PROCEDURES
Cyber risk and security program review and development for your organizations current policies and procedures

VIRTUAL CHIEF INFORMATION SECURITY OFFICER

Enterprises have adopted a logical approach, both strategic and financially, to outsource their cybersecurity functions. At Covert Threat, the Virtual CISO (vCISO) designed to make top-tier security professionals available to your organization for security expertise and guidance. Our team of experts have decades of real cyber world experience that will work WITH your organizational objectives and show measurable improvements in your current organization's security posture.

vCISO APPROACH

The role of a CISO is crucial to the success of a business, we recognize the high costs that are associated with a direct hire of a CISO. Consequently, Covert Threat has developed a service that allows enterprises to employ a virtual CISO. A vCISO carries out the same role as a traditionally appointed CISO, however at a much lower cost. The benefits of this make it a worthwhile consideration for all organizations that value cyber-security. Not only does a vCISO reduce costs but they allow flexible working times and days to suit your organizational needs. A Covert Threat vCISO brings results and ensures that all operations are running smoothly without placing pressure on company finances. It is the ideal way to improve your enterprises cyber-security infrastructure and reduce vulnerable attack surface area.

WHY COVERT THREAT vCISO SERVICES?

Covert Threat's mission is to fix the broken information security industry, we've made it our objective to work with clients to develop their current programs with our experienced professionals who work firmly and truly care about the protection of people's information.

vCISO SERVICES

MENTORING & SUPPORT

Our vCISO mentoring program, designed to work with your current designated ISO by reducing the gaps through mentoring and overseeing the organizations security posture.

COMPLETE OUTSOURCING

Our vCISO Outsourcing program, designed for organizations who currently do not have a Cyber Security leadership position filled (CISO). Covert Threat's vCISO program provides your organization with a highly qualified cyber security expert who serves as an additional knowledgeable key figure who is responsible for the development, implementation and management of your organization's corporate security function.

vCISO BENEFITS

- *Assess External Threat Risk*
- *Technical Assistance*
- *Budget*
- *Communicate with Executives*
- *Technical Guidance*
- *Organize security training*
- *Develop Security Plan, Policies & Procedures*
- *Manage Vendor Risk & Compliance Regulations*
- *Implement Remediation Plans*

With our cyber security industry leading professionals working throughout the entire U.S. and Australia we can confidently say we've been in your business, talking to your boards, and solving your problems.

We understand what you need to stay compliant and increase the quality of your business.

SCADA Services

Oil and gas, alternative energy, manufacturing and utility companies increase demand for proper tool implementations to allow remote access to controlling and regulating SCADA and other industrial control systems. The advancements in technology allow organizations to connect seamlessly to their environments, though there are noticeable risks emerging which exposes the environment to the public.
Stakeholders who require such seamless remote connectivity are:

- *Accountants*
- *Maintenance*
- *Purchasing Departments*
- *Other SCADA platforms communicate over the internet*

The remote access necessary to perform organization duties with ease come with inherent risk as the level of exposure increases resulting in a rise in potential malicious attacks. Cybercrime is one of the greatest threats facing the world, the level of impact on a global scale is unmeasurable.
There are many reports of devastating incidents of organizations resulting in a breach, generating severe losses and physical damages to the corporate infrastructure.

Testing Your SCADA Network

With inevitable cyber-attacks continuing, security professionals in critical infrastructure face enduring pressures, which affect organizational priorities. They require improved flow of information and innovative strategies in risk management.

No organizations are completely resistant to cyber-attacks, though a proactive, all-encompassing strategy can eliminate a majority of threats. At a time when one small exposure can devalue an organization's brand, getting security right is imperative.

Why Covert Threats SCADA Services?

Covert Threats industry security experts can assist asset owners protect SCADA and other critical infrastructure from emerging cyber threats. SCADA systems should be analyzed for threats and vulnerabilities.

Our team of security experts can assist you with:

- *SCADA Vulnerability Testing*
- *Risk Management*
- *Social Engineering*
- *Educate Officers, Managing Directors and Board Members on cyber risks*
- *Application & Database Vulnerability Testing*
- *Employee Security Awareness Training*
- *Educate employees to improve their knowledge and competency regarding cyber-security*

SCADA Targets

- One third of industrial sites are connected to the Internet.
- 60% of industrial sites have passwords traversing over networks in plain text.
- 50% are not running anti-virus protection software on their endpoints.
- IT security implementation. Most organizations have not fully deployed their IT security programs.
- About 20,000 different malware samples were found in ICS belonging to over 2,000 different malware families in 2016.
- Incomplete knowledge about network-connected devices. Legacy systems paired with newer technology may result in sacrificing mission-critical security.
- Casual patching practices. Consistent firmware and software updates, including patching bundled vendor packages is imperative.
- Incomplete monitoring. Many organizations are not getting actionable real-time threat alerts about security exploits.
- Discontinuity in system and user authentication can allow unauthorized users access to the system.
- Disparate policies and procedures. A unified security policy protects both information technology (IT) and operational technology (OT).

COMPLIANCE

Enterprises within the regulatory compliance sectors are wise to assess their readiness prior to an official audit. Adopting this strategy puts the organization in the best possible position for a successful audit and a sound security infrastructure. Addressing these risks with a strengthened remediation road-map is arguably the most critical step in the process.

Covert Threat can assist enterprises by reviewing their current IT infrastructure controls, network designs, segmentation of critical assets, application architecture, policies, procedures, identify any gaps or possible flaws prior to an official audit.

Our team of industry leading experts are well in-tuned with all compliance sectors and readily available to assist organizations prepare for their next audit.

COMPLIANCE READINESS & STANDARDS OFFERINGS

Majority of industries retain personally identifiable information (PII) which is the forefront of all compliance audits.

PCI-DSS
Banking and Financial Industry utilizing credit card payments

HIPAA
Health Industry retaining protected health information (PHI)

GLBA
Financial institutions protecting and sharing their customers private information

SOX
Internal financial record controls for publicly traded companies

CCPA
California resident's privacy law regarding personal information

GDPR
Data protection and privacy in the European Union and European Economic Area

NERC CIP
Reliability standards for the energy utility sector in North America

CIS
Internet security benchmarks to improve an organizations security posture

ISA99
Industrial control systems standard in operation technology

SECURE CODING

Developers are faced with constant pressure to produce new or modified code on a daily basis for organizations. The reality is, no code is **100% bug-free**. Organizations must ask themselves, what kinds of bugs are within their code? Are individuals' jobs on the line when they are expected to identify all bugs in the code before pushing to production? What if a value has been hardcoded, something that if the code was decompiled would reveal the SA (System Administrator) password to your SQL Server?

These are a select few our Covert Threat experts look for when conducting a comprehensive code review. Our industry leading experts take a hybrid approach utilizing a combination of automated and manual assessments. To name a few our team inspects your organizational code for logic, security issues and any other areas where a vulnerability may exist if discovered and abused.

WHEN TO PERFORM A SECURE CODE REVIEW

Security should be a focus throughout the entire development life cycle. Creating threat models during the design phase, educating developers on secure coding practices, and performing frequent peer reviews of code with security personnel involved will all help increase the overall quality of the code and reduce the number of issues reported (and hence that need to be fixed) by the secure code review.

However, a secure code review is best used toward the end of the source code development, when most or all functionality has been implemented. The reason for waiting until late in the development phase is that a secure code review is expensive and time consuming. Performing it once toward the end of the development process helps mitigate cost.

SECURE CODING MANUAL & AUTOMATED

There are two primary limiting factors that can make a secure code review tricky: humans and automation. For a human, the limiting factor is the relatively limited lines of code that an expert individual can review in a work day. A human may be able to review several hundred lines of code in a day. Considering that modern software is often comprised of tens or even hundreds of thousands of lines of code, it is highly unlikely for a human to manually review every line of code. It would require nearly as many reviewers as developers to approach the process using manual methods alone.

Automated tools can review code much faster than humans. The trade-off, however, is that automation is far more prone to missing security implications (false negatives) as well as falsely identifying them (false positives). In addition, automated tools often don't understand the context in which code is written.

To overcome these limitations, a review should be performed through a combination of manual and automated efforts. Automated tools can quickly scan the code base to identify areas of interest and potential vulnerabilities. Triaging automated findings guides the manual investigation into those potential vulnerabilities. Manual reviews are also useful when reviewing the code for certain classes of flaws such as authentication and cryptography.

The best approach for a secure code review is to understand the advantages and disadvantages of each method and to incorporate both as appropriate.

SECURE CODING OBJECTIVES

- *Security by design*
- *Practice defense in depth*
- *Sanitization of data*
- *Define security requirements*
- *Error handling and logging*
- *System configuration*
- *Threat modeling*
- *Cryptographic practices*
- *Input validation and output encoding*
- *Heed complier warnings*
- *Password management*
- *Access management and least privilege*

DIGITAL FORENSICS

Covert Threats digital forensic experts investigate the underlying causes, impacts and outcomes of cyber incidents and assist your organization achieve their forensic analysis objectives. Our industry leading experts are highly dedicated and experienced, able to work with a variety of systems and technologies to unfold the facts. At the conclusion of Covert Threats forensic investigations, we provide a comprehensive report detailing what our experts have discovered and recommendations.

DIGITAL FORENSIC SOLUTIONS

INCIDENT RESPONSE

After-Incident occurrence, digital forensic services, assist your organization to uncover the course of events, recover your data and more.

PCI-DSS INVESTIGATION

Covert Threat assists in recovering data from a breach in environments impacting PCI-DSS environment.

INTELLECTUAL PROPERTY THEFT

Covert Threat will investigate Intellectual Property, fraud and theft, and advise your organization on what is the best course of action through to prosecution.

TRIAL LAW-ENFORCEMENT

Utilize our experts for legal consultation, trial support in commercial, civil litigations including calling our experts as witnesses in court.

WHY COVERT THREATS DIGITAL FORENSIC SERVICES?

Covert Threat's forensic investigators mission is to identify the cause of the data breach, and provide solutions to minimize and repair the damage an organization has encountered.

Our team of digital forensic experts hold industry qualifications such as CHFI (***computer hacking forensic investigator***) and have years of industry experience in all sectors of the workforce.

Covert Threat's technology and vendor independence allows for thorough, in-depth, and unbiased recommendations to move an organization beyond a breach and help prevent future breaches.

Our experts work closely with the PCI Security Standards Council and the card brands to continually support improvements in the many standards.

COVERT THREATS DIGITAL FORENSIC OBJECTIVES

- *Windows, MacOS Forensic Intrusion Analysis*
- *Mobile Device Forensic Analysis*
- *Web Application Forensic Intrusion Analysis*
- *Law Enforcement Digital Forensic Intrusion Analysis*
- *Detailed Select User Activity Analysis*

With our digital forensic leading experts working throughout the entire U.S. and Australia, our team is ready to assist you in any location remotely or onsite.

Our experts hold industry recognized digital forensic certifications with extensive knowledge ready to assist with your forensic needs.

Covert Threat understands your organizational urgency to identify the point breach and recommendations to ensure a breach does not occur.

BUG BOUNTY

"COVERT THREATs ARMY OF ALLIES"

Covert Threat's security researchers and front-line defenders understand the importance of investigating and responding to security issues. We reduce risk with coverage, powered by our bug bounty network of cybersecurity experts. Go beyond vulnerability scanners and traditional penetration tests with trusted security expertise that scales — and find critical issues faster.

Covert Threat's fully-managed Bug Bounty program fuses analytics, automated security workflows, and human expertise to identify and resolve more critical vulnerabilities.

WHY COVERT THREATs BUG BOUNTY PROGRAM?

SKILLS & INCENTIVES

Uniquely-skilled hackers compete to find vulnerabilities that traditional testing misses.

CONTINUOUS COVERAGE

Continuous testing helps you stay ahead of software release cycles.

TRIAGE & RESULTS

Let your team focus on things that really matter, and ensure devs gets all the info they need to fix faster.

BUG BOUNTY OFFERINGS

CONTINUOUS

Continuous programs provide on-going assessment of targets. We recommend this approach for all customers, especially those with high-value targets and those with rapid or agile development lifecycles.

PROJECT BASED

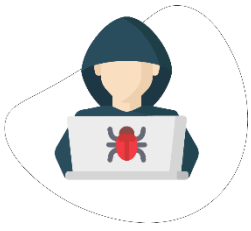
Project-based programs offer a time-bound assessment, similar to a traditional penetration test.

PRIVATE PROGRAM

Invite-only programs are only accessible to the Elite Covert Threat assessors. Some managed bug bounty programs start as private while we help your team define the business processes necessary for a public bug bounty program.

PUBLIC PROGRAM

Public programs are open to the public. These are shared to the public; they often attract a wider variety of testing skills and experience to help you find critical vulnerabilities.



Our elite bug bounty experts working throughout the entire U.S. and Australia, our army is ready to assist you in all your bug bounty needs. The Covert Threat army comprise of highly knowledgeable white-hat cyber security experts and are ready to assist with your bug bounty needs.

Covert Threat's army of allies understand your organizational bug bounty needs. – *Let the pros do it!*