



Ultraviolet Penetration Testing

Service Description

TABLE OF CONTENTS

1	PENETRATION TESTING	1
1.1	DOCUMENT OBJECTIVE	1
1.2	SERVICE OVERVIEW	1
1.3	OFFERING DESCRIPTION	1
2	CUSTOMER AND UVC RESPONSIBILITIES	3
2.1	PLANNING	4
2.2	EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)	4
2.3	PHISHING	5
2.4	ACTIVE TESTING	5
3	SERVICES TERMS	7
3.1	SCOPE OF ADDITIONAL SERVICES	7
3.2	PORTAL ACCESS	7
3.3	OPEN-SOURCE INTELLIGENCE (OSINT)	7
3.4	EXTERNAL ATTACK SURFACE MANAGEMENT (EASM)	7
3.5	FINDINGS VIEW	7
3.6	ANNUAL PENETRATION TEST	7
3.7	VOODOO	8
3.8	REPORTING	8
3.9	UVC RECOMMENDATIONS	8
3.10	SERVICES MANAGEMENT AND GOVERNANCE	8
3.11	SECURITY ASSESSMENT	8
3.12	DEFINITION OF FINDINGS	9
4	FOCUSED TESTING METHODOLOGY	11
4.1	PREPARE	12
4.2	EXECUTE	12
4.3	PROSPER	13
4.4	ASSESSMENT DETAILS	15
4.4.1	<i>External and Web Application Penetration Testing</i>	<i>15</i>
4.4.2	<i>Internal Penetration Testing</i>	<i>19</i>
4.4.3	<i>Collaborative Cloud (Azure) Security Assessment</i>	<i>20</i>
4.4.4	<i>Mobile Application Penetration Testing Services</i>	<i>21</i>
4.4.5	<i>Social Engineering Penetration Testing Services (Phishing)</i>	<i>22</i>
4.4.6	<i>Internet of Things (IoT) Testing Services</i>	<i>23</i>
4.4.7	<i>Wireless Penetration Testing</i>	<i>25</i>
4.4.8	<i>Code Review Penetration Testing Services</i>	<i>25</i>
4.4.9	<i>Physical Control Penetration Test</i>	<i>26</i>
5	LEGAL TERMS	27
5.1	ORDER OF PREFERENCE	27
5.2	COMPLIANCE WITH LAWS	27
5.3	SALE VIA UVC AUTHORIZED RESELLER	27
5.4	LICENSE	27
5.5	SECURITY AND DATA PRIVACY PROGRAM	27
5.6	CONFIDENTIAL INFORMATION	28
5.7	TELEMETRY DATA	28
6	PERFORMANCE MANAGEMENT	29

6.1	CLIENT RESPONSIBILITIES.....	29
6.2	SERVICE LEVEL EXCEPTIONS	29
6.3	SECURITY AUDIT	30
6.4	GOVERNANCE AND ESCALATION	30

1 Penetration Testing

1.1 Document Objective

This document (“Service Description”) describes the service features, components, and terms for Penetration Testing (“PT” or “Services”) that UVC will provide to the designated customer listed in a contractual binding Statement of Work (SOW). The specific quantity and type of the Services purchased by Partner will be documented in a SOW between the parties.

1.2 Service Overview

The UVC Penetration Testing (referred herein as “PT” or the “service”) will provide Client cybersecurity assessment services. UVC will perform focused assessments of Client environment and provide analysis to Client explaining scope attack surface as well as the likelihood of success from various attack vectors.

1.3 Offering Description

UVC offers PT, coupling both system generated attack simulations as well as human modeled tradecraft using Focused Assessments. The offerings include the following services:

- Custom open-source intelligence gathering on company external data
- External network
- Internal network
- Windows Domain (Active Directory)
- Cloud security reviews (AWS, Azure, GCP)
- Desktop applications
- Web applications
- Mobile applications
- Source Code Review
- Hardware and IoT
- Social engineering via email, phone, or onsite
- Building and physical security
- Wireless Networks
- Operational Technology (OT)

Service deliverables are described in the table below.

Service Feature	Focused Assessment	Description
Focused Penetration Test	<input checked="" type="checkbox"/>	Focused Engagements or Penetration Tests will be conducted in accordance with the SOW identified for the engagement.
Interactive Findings	<input checked="" type="checkbox"/>	Self-service findings reporting within the capabilities offered in the portal
Custom Reporting	<input checked="" type="checkbox"/>	Access your reports by focused engagement or request report
Portal Account	<input checked="" type="checkbox"/>	Portal to view all findings related to assessments as well as any other related to the subscribed services
Export Findings to ITSM	<input checked="" type="checkbox"/>	Export your findings via API or .CSV into your internal ITSM to remediate
Attack Surface Management		
Continuous Open-Source Intelligence (OSINT)	<input checked="" type="checkbox"/>	UVC will continuously collect open-source intelligence on your company employing the tactics and tools honed throughout our careers as former NSA operators.
Continuous External Attack Surface Management (EASM)	<input checked="" type="checkbox"/>	UVC will continuously discover your external assets and enumerate them for information such as port/protocol/application information and alert you on changes to your external attack surface based on open source repositories
Continuous Cloud Security Posture Assessments (CSPA)	<input checked="" type="checkbox"/>	UVC will continuously discover new cloud assets and perform scheduled posture assessments using CIS benchmarks against discovered assets. UVC will also evaluate environments for known high risk configurations based on team experience, threat intelligence, and known successful attacks
Quarterly Threat Briefings	<input checked="" type="checkbox"/>	UVC will meet with you and your team to go over all findings which have occurred over the previous quarter along with Threat Intelligence
Phishing	<input checked="" type="checkbox"/>	UVC will engage in phishing campaigns against your organization on an agreed upon periodicity negotiated in the SOW to help you identify potential threats to your

Service Feature	Focused Assessment	Description
		security posture. These campaigns will attempt to bypass both email protections and MFA security measures.
Active Testing		
Continuous Automated Red Teaming (CART)	<input checked="" type="checkbox"/>	UVC will continuously perform automated checks against discovered assets via EASM as well as those entered by client into the portal for potential exploitation. UVC will work interactively with the client based upon the ROE established in the SOW to provide continuous penetration testing
Add-on Services: Coder Review IoT Assessments	<input checked="" type="checkbox"/>	UVC will customize an IoT assessment per Customer requirements

UVC will work with the Customer to advise on the appropriate Tier of service for their specific environment consideration of the following:

- Attack Surface Management Type
- Internal, Cloud and/or external scanning
- Phishing
- Adversary Emulation Services

2 Customer and UVC Responsibilities

The following responsibility assignment describes the participation required by both Customer and UVC in completing tasks or deliverables for a project or business process to facilitate successful service delivery.

Please note all continuous services will be limited to the duration of the engagement period and will end upon project completion. Customer may elect to upgrade to the Penetration Testing as a Service (PTaaS) offering to retain ongoing continuous activities.

The key components of the services described are summarized and elaborated upon as follows:

1. Planning
2. External Attack Surface Management (EASM)
3. Phishing
4. Active Testing

2.1 Planning

Summary: UVC and Client will work together to provide details on the scope of the Services, and to define plan for establishing connectivity between UVC and the PT Components.

UVC Responsibilities

- Define the high-level scope of work required to transition the in-scope PT Components depending on selected tier, including assessing changes to the PT Components, Network, and processes in order to Activate the Services
- Define the API requirements necessary to Activate the PT Components
- Identify a single point of contact (SPOC) to engage with Client during the Service Transition
- Perform any other tasks designated as UVC's responsibility in the Transition Plan by the date specified in the Transition Plan

Client Responsibilities

- Unless as otherwise agreed in writing, provide the reasonably requested inventory and topology information by the dates provided in the Transition Plan
- Review and approve Transition Plan, including Activation date(s)
- Identify a SPOC to engage with UVC throughout the Service Transition period
- Perform tasks specified as Client's responsibility in the Transition Plan by the date specified in the Transition Plan
- Agree to rule of engagement as well as any SOW for focused assessment or continuous analysis services to which the client will be subscribed

Output: Transition Plan and Rules of Engagement

2.2 External Attack Surface Management (EASM)

Summary: UVC will help identify, validate, and exploit or prove-out likelihood and impact of a findings if a finding is discovered, detected or reported by PT Component of MAGE.

UVC Responsibilities

- Create Findings details within the portal from detected or reported Findings.
- Manage Findings by classifying, prioritizing, and providing remediation recommendations.

Client Responsibilities

- Review and act on all Findings
- Perform UVC or third-party recommended changes or assist in restoration of services to resolve the Incident.

<ul style="list-style-type: none"> ▪ If UVC can make the Changes to the PT Components to restore connectivity or logging, make Changes with Client's permission. ▪ Notify relevant parties about Findings. ▪ Make recommendation to resolve Findings. 	<ul style="list-style-type: none"> ▪ Advise or approve actions within the adversary emulation depending upon subscribed service level
Output: Incident Ticket; Change Request or recommendation to resolve Findings	

2.3 Phishing

Summary: UVC will perform phishing campaigns against the Client's approved email list as well as any email addresses identified during Attack Surface Discovery aimed at improving the security posture of the Client. Depending upon the service level and Client approvals these may or may not be utilized for an initial attack vector.

UVC Responsibilities

- Create regular cadence of phishing emails based on known TTPs.
- Manage Findings by classifying, prioritizing, and providing relevant information via the portal.
- Notify relevant parties about Findings.
- If PT service is enabled, create implant or other attack vector compromise to be utilized by the phishing campaign.

Client Responsibilities

- Review and take action on all Findings
- Advise or approve actions within the adversary emulation depending upon subscribed service level

Output: Incident Ticket; Change Request or recommendation to resolve Findings

2.4 Active Testing

Summary: UVC will perform active testing against Client's assets in accordance with the approved ROE and SOW emulating nation state level adversaries. We will work stealthily to achieve predefined mission objectives.

UVC Responsibilities

- Create Findings with details within the portal from detected or reported Findings.

Client Responsibilities

- Contact UVC if Client believes an Incident is in-progress or has occurred.

<ul style="list-style-type: none">▪ Manage Findings by classifying, prioritizing, and providing remediation recommendations.▪ Work with Client to create objectives for the Red Team▪ Notify relevant parties about Findings.▪ Create custom tradecraft to perform post exploitation activities using VooDoo.	<ul style="list-style-type: none">▪ Participate in diagnostic testing to identify the source of the Incident.▪ Review and take action on all Findings▪ Advise or approve actions within the adversary emulation
Output: Reports with recommendation to resolve Findings	

3 Services Terms

3.1 Scope of Additional Services

Unless the Services are expressly provided for above, all other UVC services are out of scope for this Service Description.

3.2 Portal Access

Client will receive login credentials and ability to create five (5) sub accounts into the MAGE portal. There you will be able to view top-level dashboards demonstrating your imminent risk across your entire attack surface (Cloud, Internal, External) as well as attack vector information derived from phishing and OSINT. Additionally, users will be able to create new annual penetration testing quotes, view historical penetration testing reports with attestation, view historical quotes, as well as view current penetration testing activities ongoing.

3.3 Open-Source Intelligence (OSINT)

UVC will utilize a variety of tactics employed by the Adversary to identify and display your attack surface. This can range from public facing IP Addresses, Domains, Sub-domains, Cloud instances, as well as any information available to the Adversary during reconnaissance. UVC will collect open-source intelligence on your company employing the tactics and tools honed throughout our careers as former NSA operators. We will gather information from all publicly available sources as well as the "Dark Web" to enable you to understand what your Adversary knows about you, your weakness, and potential leaks of sensitive information.

3.4 External Attack Surface Management (EASM)

Scanning public facing CIDR blocks to understand alive IP Addresses, Exposed Ports, Services running, Cloud Services or Domains associated with the client. Gathering information on users, public email addresses/phone numbers, GitHub repository information or secrets, Known Risks, etc.

3.5 Findings View

Within the MAGE portal users will be able to view detailed information regarding each finding from their annual penetration test as well as any future findings derived through the continuous assessment and analysis features associated with their PT tier. This will provide MITRE ATT&CK mappings, criticality ratings, descriptions, along with potential remediation action and/or detection capabilities.

3.6 Annual Penetration Test

UVCs world class cyber warriors will perform an annual penetration test meeting your specific requirements and industry attestation requirements. Penetration testing with the skills and techniques of a nation state! The UVC team experience includes decades of cyberwarfare operations, application development, exploit development, reverse engineering, hardware hacking and more. We attack environments with every publicly known approach and a few approaches that aren't publicly known. We don't emulate the adversary; we are the adversary.

3.7 VooDoo

UVC's proprietary post exploitation tool VooDoo will be employed within your environment to perform continuous internal assessments as well as covert red team exercises aimed at achieving one mission: making your security more adaptive to threats.

3.8 Reporting

UVC will provide, or make available via the Portal, the reports listed in the reporting documentation for PT Services. UVC reserves the right to add, change, or remove reports in its reasonable discretion. Client may review any reports with UVC. Client is responsible for reviewing, analyzing, and if needed (e.g. reporting inaccuracies), discussing with UVC the information contained in the reports provided.

3.9 UVC Recommendations

To the extent that Client fails to implement any reasonable UVC recommendations or requirements with respect to the PT Components or the Services, UVC shall have no responsibility for any delays or failure(s) regarding the performance of the Services or its impact to the Client.

3.10 Services Management and Governance

Client, not UVC, is responsible for coordinating any complementary services. If Customer wishes to directly receive data from a business partner(e.g. Security Incident tickets) and/or perform responsibilities or complementary services on Client's behalf, Partner will obtain written permission from Client and if requested, provide UVC with a Letter of Authorization from Client, allowing this sharing of data and coordination of Services.

UVC and Client will implement a governance function with the following goals: discuss alignment of the services to Client's business needs, identify opportunities to improve the Services (e.g., increase quality or reliability), and similar matters. The parties will conduct periodic governance meetings as mutually agreed. Both UVC and Client will make available appropriate members of its IT, business, and leadership organization for the governance meetings, as applicable.

3.11 Security Assessment

While performing PT, we will attempt to identify vulnerabilities in the applications and/or networks considered to be in-scope. If a critical vulnerability is identified, testing of that vulnerability will immediately stop, and the Client may be contacted for immediate resolution.

Client and UVC understand that due to the nature of the assessment being performed, unintentional service disruption is possible. Although every precaution will be taken to avoid unnecessary downtime, UVC will not be held responsible for downtime, outside of its control, as a result of the testing being performed.

Prior to any social engineering attack targeting employees, UVC will provide, for approval, a list of potential employees to be targeted in the attack to the Client's designated point of contact.

If exploitation of a targeted machine is successful, UVC may perform additional exploitation in an attempt to find additional network vulnerabilities. UVC will take extreme caution when performing additional exploitation by performing reconnaissance and/or exploitation.

Targeted and exploited machines can be implanted (e.g. install additional covert software) with tools to perform additional network reconnaissance. These tools are extremely covert and, in most cases, do not impact end users.

At the conclusion of the service, all targeted workstations will be completely cleaned of any and all network tools and/or implants used for the engagement.

While PT can increase awareness of potential security vulnerabilities as well as improve overall information systems security, complete coverage of every potential risk and vulnerability is impractical. Security risks constantly change and UVC cannot be held accountable for any future attacks or breaches.






3.12 Definition of Findings

Through the term of the service UVC will identify vulnerabilities and assign priority levels. UVC will adhere to an established criteria for risk scoring. The following describes the methodology and associated terminology used in determining the priority level of a Finding.

Risk Scoring Criteria

We use a risk scoring system that is calculated by multiplying the impact by the likelihood of attack to arrive at a total risk score. Impact is measured by the potential damage that could be caused to information systems, business operations, reputation, etc, which ranges from small to catastrophic. Likelihood of attack is measured by the circumstances in which an attacker could leverage the vulnerability into a successful attack and is rated from rare to certain.

Impact	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5
Likelihood					

	Critical	Poses a serious threat to an organization's security and should be fixed immediately. They may allow for a total system compromise, or cause severe disruptions to business operations. These should be fixed immediately.
	High	Poses serious risk to the organization's environment and significantly impact security posture as a whole. These should be fixed as soon as possible.
	Medium	Represents a moderate risk to the environment.
	Low	Minimal risk to the environment and often theoretical in nature or requires unique circumstances to leverage.
	Info	Has little to no impact to the security environment alone but could become a risk when combined with other circumstances or environmental changes.

UVC will adjust case priority in accordance with updated priority of impact or incident resolution. In addition, the ticket may be left open after containment or restoration for a prescribed period while remediation efforts are being assessed.

4 Focused Testing Methodology

We understand that the overall objective of a penetration test is to ensure that appropriate information security controls are implemented within Networks, Servers, Applications and Computing platforms to preserve integrity, confidentiality, and availability of its information and computing resources. The UltraViolet Cyber Methodology tests, discovers, and documents security vulnerabilities within information systems and services without affecting the availability of production systems. The UltraViolet Cyber Prepare, Execute, Prosper methodology is based on industry standards and best practices such as NIST SP 800-115, Penetration Testing Execution Standard (PTES), OWASP, as well as decades of experience. We support SOC2, FedRAMP and PCI compliance standards.

UltraViolet Cyber Penetration Testing methodology follows industry standards and provides a framework for consistent, high-quality services.



UltraViolet Cyber penetration testing services take a real-world offensive look at remotely accessible information systems to determine if systems, services, and/or applications contain vulnerabilities which can be leveraged to gain unauthorized access to data, information systems, and/or applications. We have honed this process delivering penetration testing and red team services on hundreds of engagements supporting enterprise, Fortune 500, Federal, State, and Local entities.

Our collaborative approach to penetration testing enables us to inform clients of their imminent risk quickly and consistently. Our portal provides information to Customer during the penetration test as well as serve as a basis for interacting with findings, reconnaissance data, Final Reports, and requesting future assessments.

4.1 PREPARE

A key component in every engagement is proper preparation and goal setting. It is imperative that the goals and rules of engagement are clearly articulated and both the Customer and UltraViolet Cyber are aligned on the overall objectives and criteria for success. During the Prepare phase, we confirm the goals for the assessment and determine which systems, networks, locations, applications etc. need to be in-scope to achieve the desired outcomes. Goals and scope for the assessment are reviewed and confirmed during the kick-off meeting. A plan must be dynamic as objectives and outside drivers can impact the plan. Updates to these goals and scope can then subsequently occur as needed throughout the assessment either via electronic communication (email/Slack) or via the portal.

Key Actions Taken	
◆	Review and Finalize Scoping
◆	Rules of Engagement (ROE)
◆	Review and Finalize Communications Plan
◆	Kick-off
◆	Project Schedule Approved

Once the plan has been approved and the engagement has begun, UltraViolet Cyber begins to perform open-source intelligence (OSINT) as well as other passive reconnaissance activities against Customer and the in-scope environments. As part of our process, we spin up a dedicated Customer infrastructure in our secure cloud environment using cloud native technologies we create a self-contained operation command center. All activities for the engagement are conducted via the centralized virtual environment which ensures Customer data never leaves or is exposed to possible loss either physical or logical.

This also ensure standardization of processes and tools used since each environment is started from a pristine state and eradicated at the end of the engagement with all outputs and data stored in the UltraViolet Cyber Platform Security Data Lake and presented to Customer via the portal. The output of the Prepare phase will be utilized to begin the active reconnaissance as part of the Execute phase.

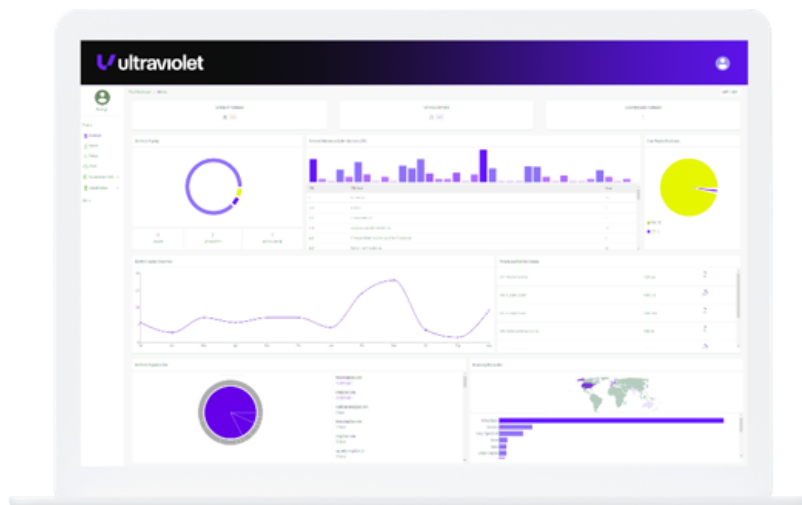
4.2 EXECUTE

Once we have completed the Prepare phase, UltraViolet Cyber expert red teamers are equipped with the necessary scoping and preliminary OSINT data to begin more active reconnaissance of the Customer targets. We harness the power of cloud native technologies and our MAGE platform to help us expedite reconnaissance data gathering. We will discover the Customer external attack surface and begin to map out the individual systems, ports, networks, applications, etc. that will serve as data points to form the Journey Map for the engagement.

The outputs from the active and passive reconnaissance phases are displayed for Customer via our UltraViolet Cyber portal via dashboards to provide insights into what information is available to adversaries and demonstrate data elements to help identify the Customer external attack surface. This information includes data which one would expect to be uncovered during this phase of reconnaissance (Live IP Addresses, Ports, Cloud Providers, FQDNs, Leaked Credentials, Email Addresses, Application information, Vulnerability data, Certificate details, Application Spidering, etc.). We utilize a host of micro-serviced tools to accomplish this information gathering.

Armed with both the active and passive reconnaissance data our expert red teamers hypothesize attack vectors as well as formulate the Journey Map to achieve the goals and objectives outlined in the Prepare phase. We utilize vulnerability information from our internal databases as well as public databases, such as the National Vulnerability Database (NVD), to identify vulnerabilities which we can exploit to gain access manually. To find high and critical findings more effectively, we attempt to locate interesting parts of the target infrastructure such as rare and/or unique services, set those services up in a similar manner locally, and dig through them for new potential access vectors others may not be aware of. We then test any access vector locally to ensure it is safe to be used on an engagement.

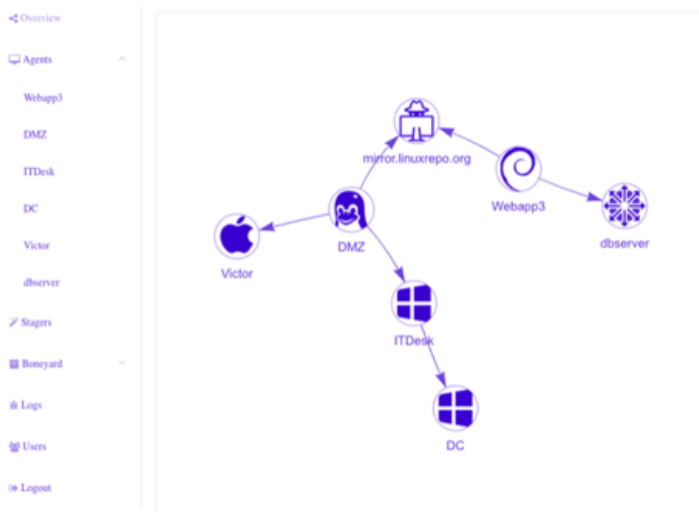
UltraViolet Cyber's Dashboard will display reconnaissance data in near real-time throughout the engagement to provide Customer insights into their external attack surface.



Once we have our attack plan, we communicate with Customer the path forward and begin to exploit identified targets. Each target attack surface type will have a different assessment and exploitation methods and processes which are outlined in subsequent sub sections. This is by no means an exhaustive list but provides more details into our methods by attack surface.

4.3 PROSPER

We utilize various methods to achieve initial access or exploitation of the target. When we discover an access vector that is safe to try against a target, we attempt that same access vector to see if the target system is also vulnerable.



UltraViolet Cyber's proprietary post exploitation tool VooDoo provides stealthy C2 as well as lateral movement and chaining across multiple operating systems and platforms.

Once we gain Remote Code Execution (RCE) via a vulnerability discovered within the target information system, we can then assert that the vulnerability is in fact a threat to the security of the information system and assess what the potential impact would be if an attacker were to also exploit this same vulnerability. This is where we enter the PROSPER phase of our methodology and provide true insights into the imminent risks the Customer is facing. This provides answers to the goals and objectives for Customer. Can it be exploited and if so, what are the ramifications of the exploit? How deep does the rabbit hole go and how can it affect my cyber resiliency? For efficient post exploitation activities, we deploy our proprietary post exploitation tool VooDoo. VooDoo is commercially available and is utilized by Federal Governments, Fortune 50 Red Teams, and other penetration testing companies for post exploitation activities. We utilize VooDoo to perform our C2 activities. VooDoo runs in memory only and can be utilized on all operating systems and chipsets, including IoT devices. Once we have established C2, we look to escalate our privileges on the acquired system and begin to map relationships to the asset to expand initial access. This begins the Privilege Escalation and Pivot tasks within the Prosper phase.

This enables an organization to identify attack paths that would otherwise remain unknown. These attack paths are often highly complex but once laid out in a network map type topology, organizations can begin to easily understand the core weakness in current security designs and work towards implementing additional security controls which will effectively prevent attackers from gaining access to the most critical assets within the organization.

Once we have begun to move laterally or expand our access, we begin the methodology again from the EXECUTE phase as we have initialized a new set of reconnaissance activities and identified a host of new assets and attack surface to begin to target and exploit.

Tasks and Activities may include...	Expected Results may include...
<ul style="list-style-type: none"> ♦ Pivoting from Internal Access to Critical Systems ♦ Analysis of Credentials to Discover Exploitation Paths ♦ Bypassing of Network & Host-based Security Controls 	<ul style="list-style-type: none"> ♦ Level of Effort to impact critical business functions ♦ Discovery of critical endpoints via graphing of accounts ♦ Recommendations on how to harden attack surfaces

4.4 Assessment Details

4.4.1 External and Web Application Penetration Testing

Ultraviolet Cyber External Penetration Testing takes a real-world offensive look at remotely accessible information systems to determine if systems, services, and/or applications contain vulnerabilities which can be leveraged to gain unauthorized access to data, information systems, and/or applications. External Penetration Testing is designed to find the weakness in Internet facing information systems, which may be exploited by a remote attacker. Ultraviolet Cyber utilizes our external attack surface management (EASM) modules to safely employ hundreds of open and closed source external reconnaissance techniques and assessment checks without disruption to operations to create leads for our expert red teamers to follow. This expedites reconnaissance activities and enables Ultraviolet Cyber to spend more time exploiting vulnerabilities and demonstrating our ability to move laterally and test as many assets as possible within the defined timeframe and scope. Because of our EASM we can give Client the benefit of a bug bounty program within the confines of this external assessment. Mapping out the entire external attack surface (to include cloud and SaaS if applicable) and employ checking dynamically to provide a wholistic map for our experts to follow.

Our methodology includes more than an in-depth testing of a variety of vulnerabilities. Going beyond the surface, we apply advanced attacker tactics and techniques targeting the infrastructure including databases, middleware, messaging queues, routers, servers, firewalls, network segmentation, and any other services.

Domain Discovery	<ul style="list-style-type: none"> ◆ Amass - https://github.com/caffix/amass ◆ GoBuster - https://github.com/OJ/gobuster ◆ Search Engines (e.g., Google)
	<ul style="list-style-type: none"> ◆ Masscan - https://github.com/robertdavidgraham/masscan ◆ Nmap - https://nmap.org/ ◆ UDP Proto Scanner - https://github.com/portcullislabs/udp-proto-scanner ◆ Nmap - https://nmap.org ◆ Ultraviolet Cyber- Custom Port Scanner
	<ul style="list-style-type: none"> ◆ Service Discovery - Nmap - https://nmap.org/ ◆ Web Service Testing - Burp Suite Professional - https://portswigger.net/burp ◆ Web Service Content Discovery - Gobuster - https://github.com/OJ/gobuster ◆ Interactive Service Probing – Ncat - https://nmap.org/ncat/ ◆ Interactive Service Checks - Exploit Database - https://www.exploit-db.com/ ◆ TLS Vulnerability Checking - testssl.sh - https://testssl.sh/ ◆ Automated Vulnerability Scanning - Nessus Professional - https://www.tenable.com ◆ Automated Vulnerability Scanning - OpenVAS - https://www.openvas.org/ ◆ Weak Credential Checking - Hydra - https://github.com/vanhauser-thc/thc-hydra
	<ul style="list-style-type: none"> ◆ Dark Web ◆ Crunchbase, LinkedIn, Search Engines
	<p>Vulnerability Scanning with expert validation and prioritization</p> <ul style="list-style-type: none"> ◆ Use of insecure services & protocols ◆ Checking for Weak Credentials within Application and Services ◆ Content discovery within web services for linked and unlinked attack surfaces ◆ Probing of web applications for common vulnerabilities such as Cross-Site Scripting (XSS), SQL Injection (SQLi) and XML External Entity (XXE) attacks
	<ul style="list-style-type: none"> ◆ Buffer Overflows ◆ Command Injection ◆ Server-Side Request Forgery (SSRF) ◆ Insecure Direct Object Reference (I<CLIENT>)
Outcomes	<ul style="list-style-type: none"> ◆ Prioritized vulnerability information to focus limited resources on high yield activities

During our highly interactive web application penetration testing services, our experts methodically perform an in-depth analysis specifically designed to meet your goals and requirements for the assessment. Web application testing for the Client includes the following:

- ◆ Performing open source (OSINT) research to identify other potential targets
- ◆ Reconnaissance to build a profile of the target's IT environments and employees
- ◆ Interactive Testing performed by industry experts to identify vulnerabilities
- ◆ Dynamic Application Security Testing (DAST) to pinpoint vulnerabilities in source code
- ◆ Automated testing specifically designed not to negatively impact the availability of information systems
- ◆ Forging custom exploits to craft the attack that is best suited for each target
- ◆ Testing for both horizontal and vertical privilege escalation attacks
- ◆ Assessing the risk associated with each finding based off the impact and likelihood of being exploited.
- ◆ Identifying realistic countermeasures that can be implemented in a timely manner
- ◆ Effectively transferring knowledge of all vulnerabilities via both reports and briefings

Tasks and Activities may include...	Expected Results may include...
<ul style="list-style-type: none"> ◆ Spidering ◆ Site mapping ◆ Mapping process flows 	<ul style="list-style-type: none"> ◆ Site map ◆ Resource list ◆ Understanding interactions

Automated testing is intended to cover a lot of ground in a short amount of time. Automated web application scanners are limited in their scope but are effective at identifying the most common issues and can save a significant amount of time in the testing process. The scanner can be configured to execute with or without a valid account on the web application and this has a major effect on the type and depth of testing it can provide. During this stage, we execute a network level vulnerability scan of the web server to find exploitable weaknesses in the server's operating system.

Tasks and Activities may include...	Expected Results may include...
<ul style="list-style-type: none"> ◆ Unauthenticated scan ◆ Authenticated scan ◆ Server vulnerability scan 	<ul style="list-style-type: none"> ◆ Common vulnerabilities ◆ Injection points ◆ Misconfigurations

Dynamic Application Security Testing (DAST) is a form of testing designed to detect security vulnerabilities in an application in an operational environment. DAST is generally used to refer to the testing of web applications, but the concept applies to the security testing of software in general. DAST involves a comprehensive review of the target application's functionality followed by probing of specific features using carefully manipulated input in order to identify

security vulnerabilities. The security logic of the application is also tested for insecure conditions or assumptions that have been built into the application leading to vulnerabilities.

We review any findings and perform interactive (i.e. manual) testing as part of this service. The interactive testing process reduces as much as possible the occurrence of false positives, thereby improving the accuracy of testing results. Tasks and activities may include the following:

Interactive Testing Items	Description
Injection Attacks	Injection attacks are generally regarded as the most critical of issues that web applications face and yet are very common. They include attack groups such as database (SQL) injection, Cross-Site Scripting (XSS), command injection attacks. Should any of these flaws be discovered then a process of measuring the real risk that they pose to the application, data, and users will be carried out.
Authentication Testing	Web applications generally require an authentication process to separate authorized users from others. This testing process will include logon page weaknesses, cookie manipulation, and password attacks etc.
Multi-stage Process Testing	Automated scanners are not suitable for testing multi-stage process such as account registration or payment processes. This phase focuses the tester on these multistage processes and aims to identify persistent Cross-Site Scripting (XSS) flaws, downstream database injection flaws etc.
Privilege Escalation	User separation is critical for securing the potentially sensitive data that a user has access to. Escalation attacks will attempt to break from one user to another of the same peer level and is referred to as horizontal escalation. Escalation also attempts to elevate privileges by breaking from a user to a higher-level account such as an administrative account; this is referred to as vertical escalation.
Web Services Information Gathering	The first phase of testing is focused on identifying in-scope services through various methods of gathering web service entry points and communication schemas. Web Service Discovery (DISCO) and UDDI are used to discover the WSDL descriptors and other XML documents.
XML Structure Testing	We will validate that the XML structure is well-formed to ensure proper function. Structure is tested for SQL injection, cross site scripting (XSS), and XPATH injection attacks.
XML Content Testing	We will perform testing for XML content by executing web services functions, validate web service using higher privilege, if authenticated, or execute commands on the database. Parameters are checked for invalid content including SQL constructs, HTML tags, etc.
RESTful Web Services Testing	We will perform testing for RESTful Web Services by validating the maximum and minimum string lengths, ensure properly validation including payload, and validate parameter names.
HTTP Get Parameter Testing	We will perform testing of HTTP GET parameters, including replay testing and inspection for sensitive data.

Expected results from this type of interactive testing may include:

- ◆ Multi-stage vulnerabilities
- ◆ Injectable inputs and input validation attacks
- ◆ Persistent injection vulnerabilities
- ◆ Cross-site Scripting (XSS) flaws
- ◆ CGI vulnerabilities
- ◆ Authentication weaknesses and/or Cookie theft
- ◆ Web server insecurity
- ◆ User privilege elevation
- ◆ Web site construction/detailed code analysis (Server/Client side)
- ◆ 3rd party software vulnerabilities
- ◆ Database vulnerabilities

All of our testing can be conducted with minimal to zero knowledge of your environment, processes, or applications. To be comprehensive in testing, we take into consideration the capabilities and permissions an authorized user may have on the systems. We normally use multiple user accounts - usually a representation of two normal or anonymous users and two authenticated or privileged user roles - to test what an authorized user may accomplish.

This is primarily a manual exercise to test, at a minimum, the following:

- ◆ Authorized user's ability to elevate privileges
- ◆ Authorized user's ability to view other user/account data
- ◆ Authorized user's ability to add/modify/delete other account data
- ◆ Authorized user's existing access is appropriate based upon role

A credentialed web application assessment evaluates several additional risks beyond what an anonymous assessment provides. The first set of risks is that an authorized user account may gain unauthorized access to (1) the application itself; (2) other Client data; and (3) the host server or platform. these risks are important because even trusted people can have their account credentials stolen. Second, we confirm user account tracking and validation is done properly by ensuring user cookies or tokens can't be easily hijacked. Lastly, we identify issues where a legitimate user can fall victim to an attacker through various means (XSS, CSRF, or SQL Injection).

4.4.2 Internal Penetration Testing

After a user's endpoint (laptop or desktop) has been compromised, via a phishing attack or browser exploit, the next step for a determined attacker is to pivot off this endpoint within the target network, leveraging the user's access to a trusted Local Area Network (LAN) and credentials to move towards their intended goal within the targeted organization.

We simulate this scenario by installing the agent for Ultraviolet Cyber custom red team toolkit (Voodoo) onto a laptop or desktop which models a typical user's experience at our office environments. Our red team toolkit enables us to test the Level of Effort (LoE) required to

compromise additional information systems from the vantage point of a typical endpoint compromised via a client-side attack. In this way, attackers frequently leverage access from the outside (e.g. Internet) to become a virtual insider threat, all the while moving towards accessing information systems critical for the goal(s) set out at the beginning of the assessment (e.g. access to credit card processing systems, etc...).

Tasks and Activities may include...	Expected Results may include...
<ul style="list-style-type: none"> ♦ Pivoting from Internal Access to Critical Systems ♦ Analysis of Credentials to Discover Exploitation Paths ♦ Bypassing of Network & Host-based Security Controls 	<ul style="list-style-type: none"> ♦ Level of Effort to impact critical business functions ♦ Discovery of critical endpoints via graphing of accounts ♦ Recommendations on how to harden attack surfaces

This assessment enables an organization to identify attack paths that would otherwise remain unknown. These attack paths are often highly complex but once laid out in a network map type topology, organizations can begin to easily understand the core weakness in current security designs and work towards implementing additional security controls which will effectively prevent attackers from gaining access to the most critical assets within the organization.

4.4.3 Collaborative Cloud (Azure) Security Assessment

During our highly interactive Cloud focused security assessment services, our experts methodically perform an in-depth analysis specifically designed to meet your goals and requirements for the engagement.

The Client has identified the following top goals, action items, and outcomes for the engagement:

- Provide a set of best practices by tenant and resource group based on the Cloud environment's current configurations.
- Identify which, if any, Cloud services are not being fully utilized to help secure the Cloud environment and help reduce Cloud costs.
- Determine which policies, logs, alerts, etc. should be enabled for better visibility into actions being taken within Cloud environments.
- Furnish a comprehensive list of who has access to what resources within the Cloud environment and highlight any paths that users/principals/applications may currently be providing an access vector to privilege escalation within the cloud environment.
- Pinpoint additional services provided within Cloud environments which would enable the Client to execute their mission more effectively and securely.
- Discovery of publicly exposed services that are public facing or accessible through the commodity Internet. Document which services are accessible regardless of whether or not they are vulnerable.
- Performing open-source research to identify Cloud secrets exposed via third party services (e.g. FQDN Similarity-based detections, Crtsh, Wayback Machine, etc.)
- Examining Cloud Storage Services (e.g. Blob Storage) for the unintentional exposure of sensitive data.

- ❑ Investigating the cloud-based identity and access management services (e.g. Azure AD) for overly permissive policies and permissions.
- ❑ Evaluating the cryptography being used by database services to ensure Transparent Data Encryption is enabled and in use.
- ❑ Investigating potential gaps and other security concerns associated with logging via Azure Monitor Logs, Log Analytics, Dashboards, Workbooks, Insights, Log Alerts, etc.
- ❑ Review Azure network configurations and network services (e.g. NAT) for security best practices. (Review of Palo Alto Azure Firewall rules are out of scope.)
- ❑ t Assessing the risk associated with each finding based off the impact and likelihood of the Client's information and/or information systems being negatively affected.
- ❑ Identifying realistic countermeasures and configuration changes that can be implemented in a timely manner.
- ❑ Effectively transferring knowledge of all action items via formal reports and briefings

Typically, in a collaborative assessment, the Client provides a secure read-only view into the in-scope Cloud accounts. UVC leverages that view to perform an audit of the environments current configuration, to make informed recommendations on how to harden the system's design and configuration.

UVC goes far beyond what other automated solutions can provide by having cyber security experts apply their critical thinking skills to discover unique recommendations, specific to the way your organization is currently leveraging Cloud services in Azure.

4.4.4 Mobile Application Penetration Testing Services

We will also test mobile applications and the information systems that support mobile applications. Often these mobile systems are integrated into an organization's core business processes with access to critical information, hence mobile applications are becoming high-value targets for attackers and should be examined thoroughly to ensure the confidentiality, integrity, and availability of the Client's information.

Testing these mobile applications and supporting information systems requires a strong knowledge of coding techniques, mobile technologies, and software frequently used in delivering mobile applications and services.

Tasks and Activities may include...	Vulnerabilities often discovered may include...
<ul style="list-style-type: none"> ♦ Examination of the application's processes ♦ Manual testing of inputs and outputs of mobile application ♦ Examination of trust points between applications, services, and various APIs ♦ Automated non-destructive mobile application crawling ♦ Measurement of limitations of defined variables 	<ul style="list-style-type: none"> ♦ Insecure Communications / Weak Cryptography ♦ Authentication Bypass Vulnerabilities ♦ Insecure Data Storage ♦ Platform Usage / Failure to Leverage iOS Keychain ♦ Reverse Engineering Attacks ♦ Hard coded sensitive information stored within application ♦ Code Tampering / Bypassing in-app purchase process ♦ Account lockout not properly implemented

Tasks and Activities may include...	Vulnerabilities often discovered may include...
	<ul style="list-style-type: none"> ◆ Privilege Escalation ◆ Session Fixation Attacks ◆ Improper MSISDN verification ◆ Malicious File Upload

4.4.5 Social Engineering Penetration Testing Services (Phishing)

As part of a comprehensive penetration test our expert red teamers will perform internal penetration testing as well as social engineering techniques to gain access to internal resources. If access is garnered through a pivot from external, cloud, or application testing the methods and techniques utilized to move about within the Client environment are detailed in the Prosper phase of our methodology.

Social engineering will be used to test the human element and user awareness of security within Client and

often demonstrate the weakest link in our defenses, humans. This can be tested via phishing, USB drops, social media, telephone, or even physical testing. A phishing assessment enables an organization to measure the security awareness of its users and, when executed correctly, helps users understand that they can have a profound and positive impact on their organization by staying aware of the common cybersecurity pitfalls that attackers frequently leverage to gain access to information systems.

We provide a report detailing the results of the phishing assessment to help Client and its internal organization structure to better understand and reduce the risk of being compromised via these client-side, social engineering, and phishing attack vectors. The report helps Client better understand how susceptible its organization is to phishing attacks and help Client make an educated decision on where further actions is needed within your organization such as additional user training. The final report includes the assessment's goals, attack vectors attempted, results from each attack vector, statistics based on these results, the overall phishing campaign effectiveness, conclusions drawn from the phishing campaign, and recommendations on how to improve the organization's overall security posture.

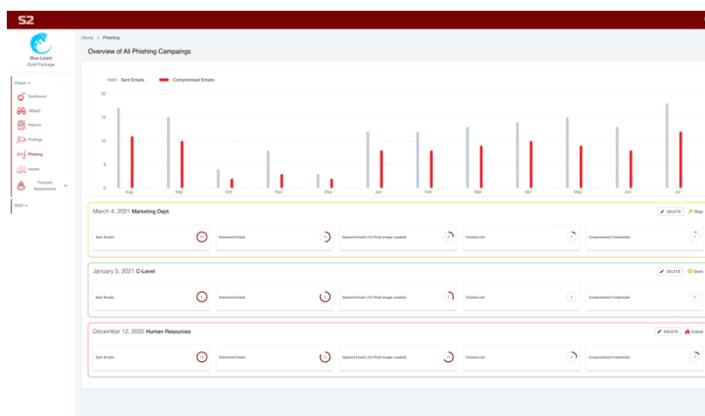


Figure 1 - UVC's Phishing Dashboard will show the results of the phishing campaign. This will enable Client to quantitatively look at the success of the engagement and areas in which to improve defenses.

Techniques	Methods	Outcomes
Phishing	Creation of Custom Phishing Email Content Implants within Email Data gathering	Run malicious code within the browser and/or exploit the user's browser Implants within Email

Techniques	Methods	Outcomes
	Exploitation of user's browser via common social engineering techniques	Capture of users' submitted data into forms to triage for sensitive information disclosures. Remote Code Execution (RCE)
Social Media/Telephone/Physical (USB Drops etc.)	Creation of Custom Social Media Content Phone calls to extract sensitive information Malware or other droppers within USB Physical access to on-network systems	Capture of users' submitted data into forms to triage for sensitive information disclosures. Gain Remote Code Execution (RCE) to the user's desktop environment via UVC's custom browser exploitation toolkit

4.4.6 Internet of Things (IoT) Testing Services

UVC penetration testers tailor our assessment to the unique set of capabilities, requirements, and potential security risks of your device. This means that we work with the Client to identify the relevant attack vectors that your device may face from the following list:

- Hardware based (e.g. Open UART / Developer Access Ports, etc.)
- Firmware based (e.g. Hardcoded Secrets, etc.)
- Network based (e.g. MitM Attacks, Weak Encryption, etc.)
- Radio based (e.g. WIFI, BLE, GSM, CDMA)
- Management & APIs (e.g. Management APIs, Cloud Services, MQTT Services, etc.)

Each of these attack vectors represents a different way in which your device may be compromised. For each vector, UVC penetration testers employ a different set of public and custom testing techniques to address the vulnerabilities present within that vector.

Vector	Tasks and Activities may include...	Expected Results may include...
Hardware	Dumping flash memory JTAG exploitation Open UART ports Firmware extraction Tampering	Hardware encryption keys Debug/Developer access Firmware image
Firmware	Binary analysis Reverse engineering Analyzing file system	Application key and certs Vulnerable/exploitable applications

Vector	Tasks and Activities may include...	Expected Results may include...
	Identifying keys and certs Modification of firmware	Discovery of any backdoors
Network	Fuzzing protocols Harvesting Insecure data transfer Timing attacks Session stealing	Credential harvesting Replay attacks MitM data attacks Unauthenticated Firmware updates
Radio (WIFI, BLE, GSM, CDMA)	Exploitation of communication protocols Sniffing radio packets Jamming based attacks Modifying / replaying packets	Credential harvesting Replay attacks MitM data attacks
Management & APIs	Android and iOS code review Application reversing Hardcoded API keys Cloud credentials Web dashboards	Credentials for cloud accounts Injection via management dashboard Keys or certificates

IoT testing begins with automated tools to gather a baseline of the security of the device. Testers then use that baseline to support manual testing with expert techniques. The following is a sampling of some of the tools which may be used:

Tools	
Hardware	Baudrate Esptool Flashrom Minicom Jlink OpenOCD
Firmware	Binwalk Strings IDAPro Ghidra Qumu
Network	Wireshark mitmproxy
Radio (WIFI, BLE, GSM, CDMA)	Gatttool Hcitrust GNURadio Killerbee
Management & APIs	BurpSuitePro Gobuster SoapUI

Where safe to do so, UVC will attempt to exploit any identified vulnerabilities and provide detailed documentation of the exploit process. This documentation will detail all vulnerabilities

discovered including risk ratings, proof of exploitation (e.g. screenshots), and recommendations for how to remediate the risk associated with the vulnerability.

4.4.7 Wireless Penetration Testing

Your cyber-attack surface does not end at the front door of your building. Wireless networks add complexity to any organization's network which leads inevitably to a greater attack surface especially if not configured properly. Misconfigurations, poor encryption, insecure guest wireless networks, rogue access points, and more can allow an attacker to join your network, intercept your traffic, and capture sensitive data that could result in a significant compromise or the disclosure of sensitive data. UVC's testers are deeply familiar with the common and uncommon vulnerabilities found within wireless networks. Our testers will examine the Client wireless infrastructure and determine where an attacker would most likely compromise the network. Through a comprehensive and methodical approach, we will assess your wireless networks and systems using various techniques. Wireless testing begins with a wireless survey during which testers will identify all wireless networks (including those with hidden SSIDs). Testers then examine the encryption levels on the various networks to determine if any are easily susceptible to known attacks. The access points are examined for any rogue points that might provide an easy way into the network. Deauthentication attacks are attempted with Man-in-the-Middle techniques to attempt to force a client device to send its track through an attacker-controlled proxy. A high-level overview of our approach is included in the following table.

Approach	Techniques	Outcomes
Weak Encryption Implementation Determine the presence of known vulnerabilities and assess their exploitability	Deauthentication Attacks Capture Client Authentication Cracking Encryption Keys	Safely removing clients from wireless networks Encryption Key Disclosure Access to private wireless networks
Client-Side and network side wireless attacks	Evil Twin Attacks Man-in-the-Middle (MitM) Decrypt Traffic Identify Sensitive Data	Lure clients into fake network Sensitive Data Collection Credential Collection
Identify Rogue Access Points Collect wireless traffic and enumerate the wireless environment	Add a rogue AP Identify insecure rogue AP Gain access to rogue AP	Internal Network Access Sensitive Data Collection Credential Collection
Map out public and private wireless networks and access points with geolocation data	Hotspot attacks Gain access to protected networks & information systems Circumvent network boundaries	Customer data collection Internal Network Access Bypass VLAN controls Attack information systems protected from a direct Internet connection

4.4.8 Code Review Penetration Testing Services

Code review penetration testing services often use the most effective techniques for discovering and triaging security flaws. When used in combination with UVC's other security related services, code review will act as a force multiplier to significantly increase the severity

and raw number of vulnerabilities discovered. Security code review provides insights into the “real risk” associated with your code, often providing the context into how a system was designed and what the business impact will be when the system is breached. These services often are effective at finding the following types of vulnerabilities:

- Concurrency issues
- Unsafe usage of APIs
- Buffer overflow exploits
- Memory corruption exploits
- Use-after-free exploits
- Integer overflow exploits
- Resources leaks
- Dereferences of NULL pointers
- Use of uninitialized data
- Control flow issues
- Incorrect expressions
- Error handling issues
- Insecure data handling
- Unsafe use of signed values

4.4.9 Physical Control Penetration Test

A physical control penetration testing helps identify real-world vulnerabilities that attackers could be used to exploit and infiltrate Client’s physical properties and data. Holes in your physical systems may seem like a lesser issue when compared to other penetration tests, but some of your most valuable assets are stored at the physical location where your company operates.

As part of the overall attempt to test physical security of your assets, Ultraviolet Cyber may use the following methods:

- Map the entrances and perimeter to assess weaknesses, easy targets, and exit points
- Lock picking of padlocks and physical locks on High Value Assets (HVAs)
- Bypassing cameras and sensors to avoid detection
- Social engineering through tactics like impersonating an employee, family of an employee, or another authorized visitor of a physical place
- Access sensitive information such as site manuals, information left in the open, or through other means
- Test substation gates, doors, wires and cables
- Dumpster diving to attain information that may be helpful in infiltrating a location

5 Legal Terms

5.1 Order of Preference

This Service Description is subject to the applicable reseller agreement between the parties (“Agreement”). If there is a conflict between this Service Description, an Ordering Document, the applicable Agreement, or any Supplement to this Service Description, the following priority will apply (from highest to lowest):

- a) any Ordering Document, as applicable
- b) any Supplement(s)
- c) the Service Description
- d) the applicable Agreement

5.2 Compliance with Laws

UVC will comply with applicable laws, rules and regulations, including, but not limited to, all applicable export control laws and regulations. Client will comply with all applicable laws, rules, and regulations related to the receipt and use of the Services and will obtain all approvals and licenses required by any third parties related to the PT Components, Client’s locations, systems, software, and network as are reasonably necessary for UVC to provide the Services.

5.3 Sale via UVC Authorized Reseller

Authorized reseller is responsible for obtaining appropriate agreements with Client reflecting the applicable terms of this Service Description, including (without limitation) requiring the performance of Client responsibilities. If Client has purchased these Services through a UVC Authorized Reseller and were not provided a Service Description by the Reseller, then this Service Description is incorporated into the agreement between the UVC Authorized Reseller and Client governing the Authorized Reseller’s provision of the Services to Client (if applicable, the “Agreement”).

5.4 License

Client receives a limited, non-transferable, non-sublicensable, internal use, license to use the executable version of Portal, and any software provided by UVC as part of the Services only to the extent and duration reasonably required to receive the Services. There are no warranties associated with these items outside of their use as part of the Services. Upon expiration or termination of the Services, the license to the Portal and any associated software will automatically terminate. Note, this license is separate from the licensing and rights associated with the PT Components, which are licensed separately.

5.5 Security and Data Privacy Program

UVC, and Client will maintain a reasonable information security and data privacy program with appropriate technical, administrative, and physical safeguards designed to prevent any (i) unauthorized access, use, distribution, or deletion of Client’s data and (ii) compromise of the PT Components or AS/DR. If UVC and Client do not have a mutual data protection agreement in

place (or equivalent privacy and data protection terms), the following Mutual Data Protection Agreement is incorporated into this Service Description.

5.6 Confidential Information

The ticket information, including recommendations to resolve Security Incidents, Charges, Portal, and Service Level performance information are Confidential Information. This information may not be used for any purpose other than in connection with Client's use of the Services.

5.7 Telemetry Data

UVC may collect data on Client's usage of the Services in order to maintain, improve, market, or promote the Services. In addition, UVC may use anonymized and aggregated data on Client's use of the Services, Managed Component performance (UVC products only), and network performance ("Telemetry Data") to create or improve its products and services. UVC will comply at all times with applicable law related to UVC's collection and use of the data above and will use reasonable physical, technical, and procedural means to protect the Telemetry Data that contains Personal Data in accordance with the UVC Online Privacy Statement, which is made available at or such other site(s) as UVC may publicly communicate from time to time.

6 Performance Management

UVC will use its standard processes and tools for measuring its performance and determining whether the Service Levels were achieved using Key Performance Indicators (KPIs). KPIs are performance indicators only and there are no financial or legal penalties if UVC does not achieve them. Performance will be managed as follows:

- The window to measure performance against the Service Levels is the Measurement Period. The first Measurement Period will begin 60 days after Service Activation.
- Within thirty (30) days of the end of each Measurement Period, UVC will provide to Client a report on the Service Level Performance for the relevant Measurement Period (“Performance Report”).
- Within 30 days of receiving the Performance Report (“Review Period”), Client should review the report and submit a written claim for Service Credits or dispute the report.
- If Client disputes the Performance Report, the parties will review the matter, including providing underlying information to support or dispute the contents of the Performance Report.
- The Performance Reports and any underlying data provided to Client to support the Performance Report is Confidential Information and may not be publicized.

6.1 Client Responsibilities

Client will provide UVC with a single point of contact to cooperate with UVC and respond to any UVC requests to help verify Service Level Performance

Client will provide such information and assistance that UVC reasonably requests to help UVC verify Service Level Performance.

Client will comply with all of its responsibilities as described in the Service Description for PT Services, including any referenced documents.

6.2 Service Level Exceptions

Any failure by UVC to achieve the Service Levels will be excused if caused by:

- a) A material act or omission by Client in breach of the terms and conditions of the Agreement, the Service Description, and/or the Ordering Document;
- b) Client’s failure to comply with its obligations or responsibilities under the Service Description or this SLA;
- c) Any mutually agreed schedule of activities that causes service levels to fall outside of measured and defined Service Level obligations set forth in this SLA;
- d) Any delays or faults caused by Client, third party equipment, software, services, support, or vendors not under the control of UVC (e.g., Carrier cycle time);
- e) Periods of maintenance where updates, patches, etc. are installed and configured (i.e. Maintenance Windows);
- f) A Force Majeure Event;

- g) Any UVC or third-party hardware dispatch and replacement, which may be covered under a separate agreement;
- h) The PT Components being past the End of Support (EOS) date or not covered by support and maintenance.
- i) Software defects that require installation of major software updates or reinstallation of the software on the UVC equipment
- j) Changes in the PT Components or network that were not validated or approved by UVC or delays by Client in implementing Changes requested by UVC or otherwise agreed between Client and UVC;
- k) Failure to implement UVC's recommendations necessary to remediate Incidents; l) Failure by Client to provide a required response necessary for UVC to meet the Service Levels (Please note: Incident Tickets will be on "hold" for any period of time UVC is delayed in receiving required information from the Client, the End User, or applicable third-party service providers);
- l) Any conditions existing prior to UVC management of the PT Components, including any incident, problem, error or other event subject to an open support ticket from a legacy or other third-party service provider; and/or
- m) Changes to the PT Components that were not approved by UVC.

6.3 Security Audit

If there are repeated Security Incidents that UVC reasonably believes can be prevented through the proper use of the PT Components and Services, UVC may conduct, at its own expense and discretion, a review of Client's security environment. Client will reasonably cooperate with this review. Following any such review, Client will make commercially reasonable efforts to implement any reasonable UVC recommendations. If Client fails to do so, this SLA will not apply.

6.4 Governance and Escalation

UVC and Client will hold regular meetings to review and assess Service Level Performance, address any Client concerns, and work in good faith to resolve any disputes between the Parties with respect to Service Level Performance.