ultraviolet

Continuous Penetration Testing (CPT)

Service Description

TABLE OF CONTENTS

1 Continuous Penetration Testing Services

1.1 Document Objective

UltraViolet Cyber (UVC) provides Continuous Penetration Services (“CPT”, “CPT Services” or “Services”) as a core offering. This document (“Service Description”) describes the service features, components, and terms that UVC will provide to customers with a contractual binding Statement of Work (SOW). The specific quantity and type of the Services purchased by Customer (“Client”) will be documented in a SOW between the parties.

1.2 Service Overview

CPT is a proactive security service that focuses on identifying, assessing, and prioritizing vulnerabilities in an organization's applications and supporting IT infrastructure **on an ongoing basis**. A key element of CPT involves monitoring applications and infrastructure with the latest exploits/access vectors, to confirm risks as soon as possible, with scaling in mind.

1.3 Objectives

The primary objectives of CPT are:

- Identify vulnerabilities in the organization's IT systems, networks, and applications.
- Assess the potential impact of identified vulnerabilities to the organization's mission.
- Prioritize the remediation of known vulnerabilities based on an assessment of the overall risk.

1.4 Scope

The scope of the CPT service includes the following as approved by the Client:

- External and/or Internal Network Infrastructure.
- Web Applications, Mobile Applications, and/or APIs.
- Cloud-based Services and Infrastructure

1.5 Methodology

The CPT service follows a structured methodology that includes:

- Goals, Planning, Scoping, & Selectors
- Data Collection via OSINT, Reconnaissance
- Analysis for Access Vectors & Leads
- Monitoring 1-days for Access Vectors
- Manual Penetration Testing for Validation

- Risk Analysis, Reporting, & Retesting

The penetration testing process is performed using a combination of manual techniques and automated tools, following industry best practices such as the OWASP Testing Guide and NIST SP 800-115. UVC actively adjusts the frequency of testing to provide the best possible outcome to the Client (e.g. Critical Findings). By default:

- Data is collected and targets are scanned/probed daily, weekly, and/or monthly.
- Leads are triaged daily (M-F), during core work hours (e.g. MT, or ET), excluding holidays.
- Interactive missions are conducted & new techniques are added monthly and/or quarterly.

1.6 Deliverables

The CPT service provides the following deliverables:

- Leads and Findings accessible via the web portal on-demand.
- Data collected within the data lake is accessible via APIs & CLIs.
- Ongoing progress updates and status reports, via shared approved contact/escalation methods.

2 Service Offering

Continuous Penetration Testing Services use People, Process, & Technology (“PPT”) to strategically improve an organization’s overall security posture by uncovering critical attack chains and collaborating with key stakeholders (e.g. Blue Teams, Engineers, etc.) on the best ways to defend against real-world attacks. The program offering includes:

- **“Assume Breach” Approach** involves treating all applications, services, identities, and networks as potentially compromised. This is covered via our CPTI services.

- **Comprehensive Post-Mortem Evaluations,** where both Red and Blue Teams share lessons from each simulated breach. UVC takes a collaborative approach for all offensive services, and hence this is included in all of UVC’s CPT offerings.

- **ROI** from improvements to an organization's Mean Time To Detection (MTTD), and other crucial performance metrics, via a collaborative efforts focused on countering adversaries.

- **Continuous Automated Red Teaming (CART)** is a technology which enables organizations to proactively identify and address critical security vulnerabilities before they can be exploited by real attackers. This proactive stance is crucial in the constantly evolving cyber threat landscape. By packaging up repeatable red teaming tasks, and automating the testing process, CART can cover a wide range of attack vectors more efficiently and frequently than interactive manual testing.

- **External Attack Surface Management (EASM)** is a technology which enables enhanced visibility into our Client’s IT assets which are directly accessible via the Internet. This means identifying all exposed assets, including unknown, forgotten, or rogue assets on the Internet that could be potential entry points for attackers. These assets are sometimes referred to as “Shadow IT” which may be the result of “Cloud Sprawl”.

2.1 Feature Map

The CPT service includes the following features:

Service Features
Analysis Ops
Red Teamer Triages Leads (“Signals”) For Escalation to a Finding
Red Teamer Enhances Findings (“Outcomes”) with Steps to Reproduce
Red Teamer Scores Findings based on Risk using CVSS

Service Features
Red Teamer Enhances Findings with Remediation Recommendations
Interactive Ops
Red Teaming Missions with UVC's Red Team[1]
Collaborative Access to Red Team Subject Matter Experts (SMEs)
CPT External
Continuous Open-Source Intelligence (OSINT)
Continuous External Attack Surface Management (EASM)
Continuous Cloud Resource Enumeration
Continuous Cloud Security Posture Assessments (CSPA)
Continuous Automated Red Teaming (CART)
Automated Findings & Leads Deduplication
Continuous External Network Testing
Continuous External Web Application Testing
CPT Internal
Custom Post-Exploitation Red Team Toolkit
Unique 0-Day(s)/1-Day(s) to Evade, Defeat, and/or Test EDRs
Deep Pivoting between Various Operating Systems (OS) & Architectures
macOS, ARM, ARM64, Windows 11/10, x64, Linux Supported Natively
In-Memory Only Scripting Engines (Python, PowerShell, C#, etc.)
Continuous Internal Reconnaissance & Network Testing[2]
Continuous Internal Web Application Testing *****
Continuous Internal C2 & Exfiltration Analysis *****
Continuous Internal Lateral Movement Analysis *****
Management Ops
Client Service Lead (CSL) from UVC for Project Management & Feedback
Access to Red Team Subject Matter Experts (SMEs)

[1] Quantity and Frequency of Missions is typically stated within the SOW and/or is based on the size purchased.

[2] * We recommend beginning Internal Testing with human-led ops and then enabling automation as we go.

Service Features
Access to a UVC Managing Director and/or other Executives
Reporting Ops
All Findings (“Outcomes”) & Leads (“Signals”) available in the Portal/API
Findings contain a Title, Description, Evidence, References, and more.
Findings contain Steps to Reproduce & Remediation Recommendations
Findings contain a Proof of Concept (PoC) exploit, when applicable.
Findings contain a CVSS Score and ID based on the Risk
Findings also contain the Date Created and the Date Last Updated
Easily export all Findings & Leads with all details to a CSV via the Portal
Export Findings to ITSM via APIs or CSV for Streamlining Remediation
Tailored Reports & Formats Available Upon Request (e.g. PDF, etc.)
Administrative
MFA for Portal Accounts Supported
Access to Raw Scan Data via the APIs, CLIs, etc.
Users - No Additional Charges for Additional User(s)
Findings and/or Leads in near real-time (Outcomes and Signals)
API - REST, Swagger UI, OpenAPI, CLI, etc.
Data Lake - Queries, Exports, Extractions and reporting

[1] * We recommend beginning Internal Testing with human-led ops and then enabling automation as we go.

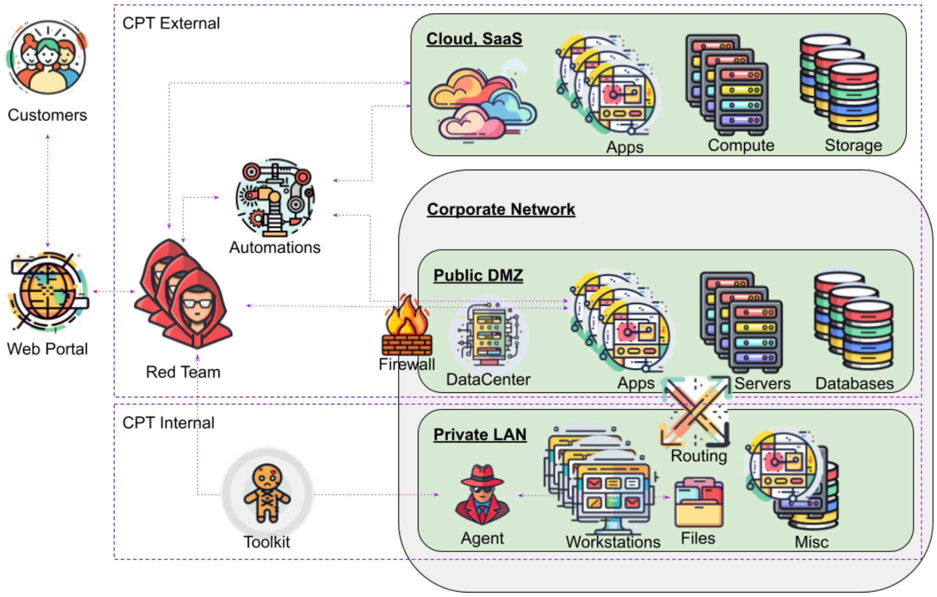
3 Internal vs External Methodology

3.1 Overview

Continuous Penetration Testing (CPT) services are offered in two different categories:

- Continuous Penetration Testing External (CPTE)
- Continuous Penetration Testing Internal (CPTI)

While the types of the systems which will be tested (e.g. Web Applications, Network Services, etc.) may be similar, the approach for testing these systems from both a technology and processes standpoint varies enough that we typically like to approach these two different areas of Information Technology (IT) with solutions tailored for specific interests and concerns.



From a technology standpoint, one of the greatest obstacles we face when looking at an organization's **external** internet facing applications and services, is discovering where they are located. We address this within our solution primarily three (3) different ways:

1. Microservices based Attack Surface Management (ASM) solution for target discovery.
2. Custom Open-Source Intelligence (OSINT) sources for deep discovery of assets.
3. Read-Only Enumeration of Public Resources within Cloud Providers (e.g. AWS, etc.).

On the **internal** side, two of the greatest obstacles we face is establishing comms within tightly controlled networks and pivoting between agents to gain access to deep network segments via the Internet. Our bespoke toolkit is designed from the ground up to overcome these obstacles.

3.2 Continuous Penetration Testing External (CPTE)

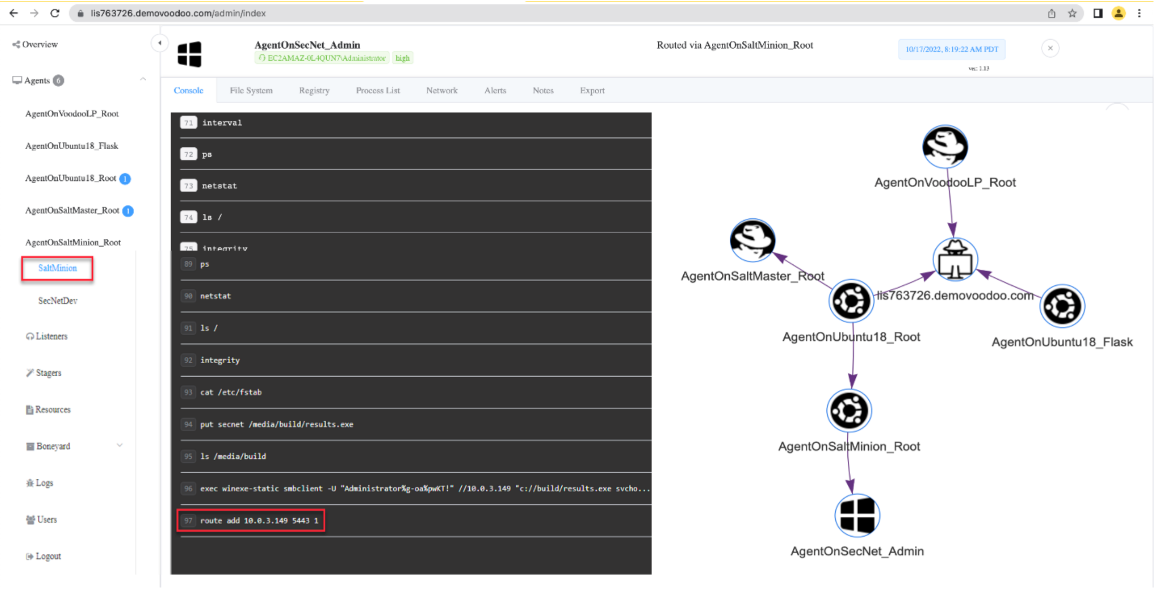
CPTe is a subset of CPT focused on an organization's Internet facing applications (e.g. Web, APIs, etc.) and supporting IT infrastructure (e.g. Cloud, etc.). The primary capabilities leveraged with CPTE are:

- **External Attack Surface Management (EASM)** is a technology which enables enhanced visibility into our Client's IT assets which are directly accessible via the Internet. This means identifying all exposed assets, including unknown, forgotten, or rogue assets on the Internet that could be potential entry points for attackers. These assets are sometimes referred to as "Shadow IT" which may be the result of "Cloud Sprawl".
- **Cloud Resource Enumeration** is a technology whereby the Customer provides read only access to their Cloud environments, and then UVC will enumerate the resources and automatically add them to the scope of the engagement on a set schedule (e.g. daily).
- **Continuous Automated Red Teaming (CART)** is a technology which enables organizations to proactively identify and address critical security vulnerabilities before they can be exploited by real attackers. This proactive stance is crucial in the constantly evolving cyber threat landscape. By packaging up repeatable red teaming tasks, and automating the testing process, CART can cover a wide range of attack vectors more efficiently and frequently than interactive manual testing.
- **New Access Vectors R&D,** involves monitoring for new 0-day/1-day access vectors being released publicly and then rapidly checking the Client's assets for any critical or high impact findings. Often reconnaissance is further expedited by our preexisting knowledge of the Client's assets (e.g. applications, services, networks, etc.) via data stored proactively within UVC's data lake.
- **Scaling Novel Access Vectors,** involves codifying the novel techniques we discover on our various Red Teaming Missions, and then scaling the check for those access vectors across all of our Client's assets. This enables the Client to benefit from not only the time our experts spend interactively manually testing the Client's assets, but also the time and resources we expended testing any of our Client's assets. This has many benefits for the Client, including gaining more diverse perspectives, being more cost effective, faster discover of critical access vectors, and more.
- **High Fidelity & Validated Outcomes,** involves UVC's trained experts reviewing "Signals" within our systems before they are escalated to be a formal "Outcome". In this manor Client's can focus on only the "Outcomes" within the portal, that we have an extremely high confidence are exploitable, and typically have a Proof of Concept (PoC) exploit with steps to reproduce the exploit ready for the Client to review.

3.3 Continuous Penetration Testing Internal (CPTI)

CPTi is a subset of CPT focused on your organization’s internal applications (e.g. Web, APIs, etc.) and supporting IT infrastructure (e.g. Cloud, etc.). The primary capabilities leveraged with CPTI are:

- **Post-Exploitation Platform (aka “Voodoo”)** is a technology which enables testers to pivot off an endpoint within the targeted network, leveraging the user’s access to a trusted LAN/network and credentials to move deeper into the targeted information systems, in a concerted effort towards researching the goals set for the mission.



```
71 interval
72 ps
73 netstat
74 ls /
75 integrity
89 ps
90 netstat
91 ls /
92 integrity
93 cat /etc/fstab
94 put secnet /media/build/results.exe
95 ls /media/build
96 exec winexe-static smbclient -U "Administrator%g-oa%pwKT!" //10.0.3.149 "c://build/results.exe svcho...
97 route add 10.0.3.149 5443 1
```

- **Insider Emulation** is a scenario where frequently, attackers leverage access from the outside (e.g. Internet) to become a virtual insider threats. They compromise a corporate endpoint (e.g. via Phishing) and then masquerading as an employee within trusted information systems and local networks.
- **Defense-In-Depth** involves focusing on the internal attack surfaces which enables an organization to identify attack paths that would otherwise remain unknown until a breach occurs. These attack paths are often highly complex but once laid out in a network map type topology, organizations can begin to more easily understand the core weakness in current security designs and work towards implementing additional security controls to effectively prevent attackers from gaining access to the most critical assets within the organization.

4 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.

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

4.1 Prepare – Onboarding and Scope

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

UVC Responsibilities	Customer Responsibilities
▪ Define the scope of the services and customer footprint available for testing ▪ If necessary, assist with configuring and providing API access to scan and detection data ▪ Identify a points of contact to engage with Customer	▪ Unless as otherwise agreed in writing, provide the reasonably requested inventory and topology information in a timely manner ▪ Review and approve scope and Activation date(s) ▪ Identify points of contact to engage with UVC

Output: Project scope

4.2 Prepare - Service Activation

Summary: With Customer's assistance, UVC will connect the CPT Components via APIs or with sufficient information to perform ongoing assessments and analysis. UVC will perform tests to confirm that the CPT Components meet technical readiness requirements.

UVC Responsibilities	Customer Responsibilities
▪ Provide Customer with general guidance on activities required to allow activation of services ▪ Provide access to the customer portal and activate agreed upon services ▪ Provide notification to Customer that activation is complete	▪ Configure APIs and implement requirements as described in the UVC documentation ▪ Assist UVC in establishing and validating connectivity between the CPT Components if necessary

▪ Provide a documentation to Customer to describe necessary steps to configure the CPT Components	▪ Disclose and/or validate all discovered or presented information required to perform the CPT Service

Output: N/A

4.3 Execute - Continuous External Attack Surface Management (EASM)

Summary: UVC will help identify, validate, and exploit or prove-out likelihood and impact of findings.

UVC Responsibilities	**Customer Responsibilities**
▪ Create Findings details within the portal from detections ▪ Manage Findings by classifying, prioritizing, and providing context around detections ▪ Notify relevant parties about Findings ▪ Make recommendations to resolve/remediate Findings	▪ Review Findings ▪ Advise or approve actions within the adversary emulation process

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

4.4 Execute - Active Testing

Summary: UVC will perform active testing against Customer's assets in accordance with the approved SOW and testing scope.

UVC Responsibilities	**Customer Responsibilities**
▪ Create Findings with details within the portal from detections ▪ Manage Findings by classifying, prioritizing, and providing remediation recommendations ▪ Work with Customer to create Red Team objectives ▪ Notify relevant parties about Findings	▪ Contact UVC to deconflict in the event that Red team activity is detected ▪ Contact UVC if Customer believes scanning activity has affected business operations ▪ Review and take action on Findings ▪ Advise or approve actions within the scope of adversary emulation

- Customize Red Team activities to match Customer's environment and goals	

Output: Reports with recommendations to resolve Findings

4.5 Prosper – Reporting and Advisement

Summary: UVC Incident Response will host a service review meeting on a regularly established cadence. The operational review will provide reports on current threat patterns, detection volumes, and trending events and other relevant incident information.

UVC Responsibilities	Customer Responsibilities
▪ Provide recommendations on how to improve services, processes, and/or technologies based on data outputs from services and business intelligence tools ▪ Provide recommendations on improving defensive coverage ▪ Identify gaps between procured services and Customer goals. If applicable, highlight opportunities where other services can support Customer goals	▪ Participate in established meeting cadence ▪ Designate appropriate persons to review recommendations

Output: Status Reports

5 Services Terms

5.1 Scope of Additional Services

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

5.2 Portal Access

Customer will receive login credentials and ability to create five (5) sub accounts into the customer 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. Users will be able to request new penetration testing quotes, view historical penetration testing reports with attestation, view historical quotes, and view current penetration testing activities ongoing.

5.3 Continuous Open-Source Intelligence (OSINT)

UVC will utilize a variety of tactics employed by adversarial actors to identify and assess your attack surface. This can range from public facing IP Addresses, Domains, Sub-domains, Cloud instances, as well as any publicly available information. 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.

5.4 Continuous 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 Customer. Gathering information on users, public email addresses/phone numbers, GitHub repository information or secrets, Known Risks, etc.

5.5 Findings View

Within the customer 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 CPT services. This will provide MITRE ATT&CK mappings, criticality ratings, descriptions, along with potential remediation action and/or detection capabilities.

5.6 Quarterly Meetings

Each quarter your Custom Success Lead and a member of UVC will meet with you and your team to go over all findings which have occurred over the previous quarter as well as shed light on current threats to your sector or environment and how to protect or detect them.

5.7 Continuous External Analysis

UVC's platform will continuously simulate the adversary and known TTPs against your external attack surface. If we identify IMMINENT RISK, we will notify you within timeframes commensurate with the SLA for the risk categorization and proceed with the attack simulation depending on approvals.

Using information gleaned from EASM, CSPM, CART and applying UVCGMA rules against it to produce findings. These findings will be validated by UVC experts.

5.8 Continuous Cloud Analysis

UVC's platform will continuously simulate the adversary and known TTPs against your cloud attack surface. If we identify an IMMINENT RISK, we will notify you within timeframes commensurate with the SLA for the risk categorization and proceed with the attack simulation depending on approvals.

Using information gleaned from EASM, CSPM, CART and applying UVCGMA rules against it to produce findings. These findings will be validated by UVC experts.

5.9 Continuous Internal Analysis

UVC's platform will continuously simulate the adversary and known TTPs against your internal attack surface using our proprietary post exploitation toolkit VooDoo. If we identify an IMMINENT RISK, we will notify you within timeframes commensurate with the SLA for the risk categorization and proceed with the attack simulation depending on approvals. Using VooDoo on a host or host(s) and applying UVCGMA rules against data derived from it to produce findings. These findings will be validated by UVC experts.

5.10 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.

5.11 UVC Red Team

Reserved for the most astute organizations, UVC will perform red team exercises against your internal network emulating nation state level adversaries. We will work and move stealthily from pre to post exploitation, moving laterally, to achieve predefined mission objectives. Our "Iron sharpens Iron" approach to red teaming will work with your cyber defenders to ensure these exercises improve your ability to detect and defend.

5.12 Reporting

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

5.13 UVC Recommendations

To the extent that Customer fails to implement any reasonable UVC recommendations or requirements with respect to the CPT 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 Customer.

5.14 Services Management and Governance

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

UVC and Customer will implement a governance function with the following goals: discuss alignment of the services to Customer'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 Customer will make available appropriate members of its IT, business, and leadership organization for the governance meetings, as applicable.

5.15 Security Assessment

While performing CPT, UVC 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 Customer may be contacted for immediate resolution.

Customer 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 as a result of 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 Customer'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.

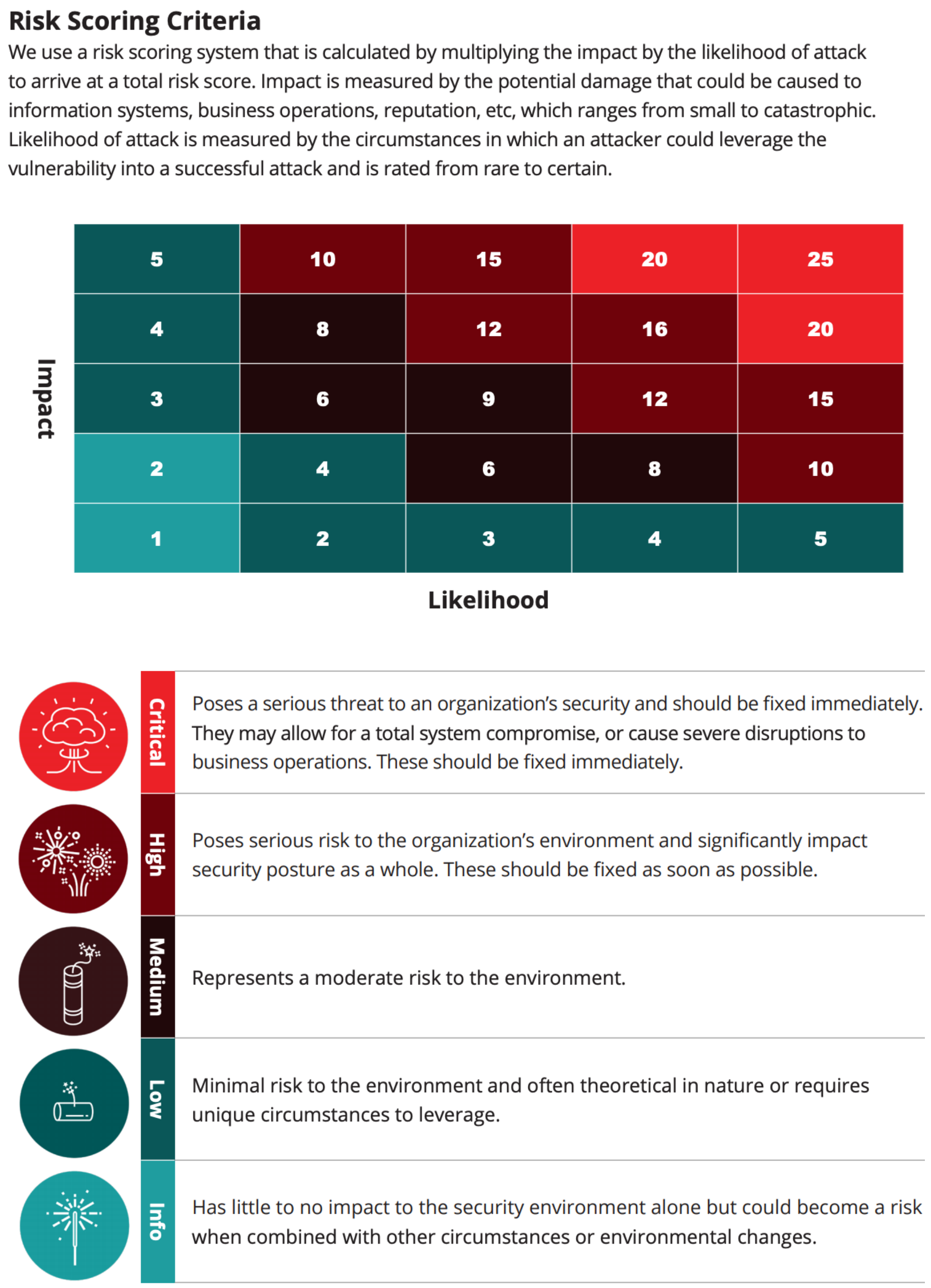
Targeted and exploited machines can be implanted (e.g. install additional covert software) with tools to perform additional network reconnaissance. These tools are extremely covert and, in most cases, do not impact end users.

At the conclusion of the service, all targeted systems will be completely cleaned of any tools used or introduced during the engagement.

While CPT 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.

5.16 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. A ticket may be left open after containment or restoration for a prescribed period while remediation efforts are being assessed.