Scope of Work for CREST Pen Testing

This Scope of Work ("SOW") governs your organization's ("you" or "Customer") use of Kaseya's internal and external network penetration testing ("Pen Testing") that is performed by Kaseya through its subsidiary Vonahi ("Kaseya") in its capacity as an organization accredited by CREST ("CREST Member Company") pursuant to the CREST Code of Conduct and conducted in accordance with a methodology that has been reviewed by CREST ("CREST Pen Test").

This SOW and the Kaseya CREST Pen Test services, products and SaaS platform (collectively, the "CREST PEN TEST") are governed by, the Kaseya Master Agreement accessible here. The Kaseya Master Agreement and this SOW are collectively are referred to as the "Agreement." Capitalized terms not defined in this SOW have the meaning given to them in the Kaseya Master Agreement. By purchasing or using the Services, you agree to be bound by the Agreement (i.e., the Kaseya Master Agreement and this SOW). If you do not agree to the Agreement, neither you, nor any client for whom you purchase CREST Pen Test(s) ("Client") may access or use the CREST Pen Test, including the relevant SaaS platform.

Should you wish to understand more about what it means to be a CREST Member Company, or to purchase a CREST Pen Test, please review the CREST Code of Conduct which is accessible here. Further, the Crest Code of Ethics is accessible here

Testing Methodologies

With respect to CREST Pen Tests, Kaseya performs a periodic review of its testing methodologies to ensure that its activities, techniques, and tactics are up-to-date and include tasks that help allow for the discovery of the latest security threats. Certain details of this testing methodology are defined below, and all CREST Pen Tests will follow this methodology.

Internal and External Network Testing

A CREST Pen Test is a network penetration test. We do not provide or perform any application layer testing or other penetration testing services. Our network penetration testing services follow a structured methodology to assess the security posture of your network infrastructure. This includes the following actions and techniques that we employ:

- Host Discovery: Utilizing automated techniques to identify active hosts within your network environment.
- Vulnerability Scanning: Employing tools and techniques to identify potential vulnerabilities present on the identified hosts.
- Enumeration: Conducting enumeration of network resources, services, and configurations to gather additional information necessary for testing purposes.
- Exploitation: Limited exploitation of identified vulnerabilities is performed solely for the purpose of verifying their existence and severity.
- Post-Exploitation & Lateral Movement / Escalating Privileges: Demonstrating potential impacts, such as lateral movement within the network or escalating privileges, in scenarios where initial exploitation is successful.

Actions and Techniques We Do Not Employ:

- Denial of Service (DoS) Attacks: We do not engage in any actions leading to disruption or degradation of services.
- Data Manipulation or Destruction: We do not attempt to modify or delete data beyond what is necessary for testing purposes.
- Unauthorized Access: We do not attempt to access systems or data beyond the scope of the agreed-upon testing parameters.

- Interference with Production Systems: We do not take any actions with the intention of interfering with the normal operation of production systems.

Tools List

Below is a list of common tools that are leveraged by Kaseya during the penetration test as well as a brief description of their function.

ENTERPRISE ASSESSMENT AND PENETRATION TESTING TOOLS	
Nessus	Commercial vulnerability scanner developed by Tenable.
Gobuster	Directory enumeration and brute force tool.
Curl	Command-line tool used to communicate with network and application services, as well as performing brute force attacks and enumeration.
COMPREHENSIVE CONFIGURATION REVIEW TOOLS	
Nipper	Commercial network device configuration review utility, developed by Titania.
Nessus	Commercial vulnerability scanned from Tenable with capabilities to perform configuration reviews.
PASSWORD CRACKING TOOLS	
John the Ripper	Multi-purpose command-line cracking tool.
Rainbow Crack	Pre-computed hash cracking tool.
Ncrack	High-speed network authentication cracker developed by Nmap.
HashCat	GPU accelerated password cracking suite.
EXPLOIT FRAMEWORK	
Metasploit	Commercial and open source exploitation framework used for discovering and validating security exploits.
PowerSploit	A collection of Microsoft PowerShell modules that can be used by penetration testers to perform discovery and validation of security exploits.
Empire	PowerShell and Python-based post-exploitation agent.
INFORMATION DISCOVERY AND ENUMERATION	
Bloodhound	Used to expedite information gathering about the target Active Directory environment. Information gathered is used to assist with privilege escalation.
Leprechaun	Leprechaun is a tool used to map out the internal network infrastructure after obtaining elevated privileges. Results allow the platform to identify potentially valuable targets.
Nmap	Command-line tool used to perform discovery and enumeration of hosts and services.

SSLScan	Command-line tool used to enumerate information about SSL/TLS services supported on a remote service.
FOCA	Application used to extract metadata information from files, such as .pdf, .docx, .xlsx, etc.
URLCrazy	Command-line tool used to identify potentially registered sub domain names based on a provided domain.
Dnsmap	Command-line tool used to enumerate DNS information about a particular domain name provided.
Arping	Command-line tool used to discover information about systems residing on the local subnet, such as connectivity validation.
Whois	Tool used to identify registration information about a particular domain or IP address.
Shodan	Search engine used to identify information about Internet-connected devices.
Sublist3r	Subdomain enumeration tool using both dictionary wordlists as well as search engine data.
Wireshark	Packet analyzer tool used to inspect network traffic.

Documentation and Communication

Kaseya has policies and procedures in place focused on maintaining proper communication during the CREST Pen Testing engagement (“Platform Information”). That Pen Test Information is housed in Kaseya’s Pen Test platform and includes security issues identified, progress made, upcoming tasks, and date of completion. The Platform Information will also include certain deliverable reports that are tailored to executives and technical contacts, as described below (the “Reports”).

All communication regarding the penetration test is delivered via vPenTest. That communication uses encryption during data transmission as well as storage. Sensitive data is also obfuscated before it is stored where possible for reporting purposes.

You have the ability to add points of contact within your organization, or other organizations including any applicable Client organization, to the Platform. **Please note, all contacts will see all Platform Information**. Kaseya will not communicate any information regarding the Pen Testing outside the contacts listed on the Product platform.

Prior to the test kicking off, acknowledgment of the penetration testing methodology is required. The penetration testing methodology informs users of the types of activities that are performed during each test, including password attacks, relay attacks, and other types of activities that would typically generate alerts.

The following Reports and other Platform Information can be expected:

- **(Optional) Real-Time Status Updates** – You and your contacts will have the ability to track the progress of the overall engagement in real-time, including real time reporting of identified threats. This dashboard will convey what issues have been identified, including their recommended remediation strategies, evidence, and expected time for completion.
    ○

- **Executive Summary Report** – An executive summary report will be included in the final deliverable package. This Report contains a high-level summary of the Pen Test findings identified as well as a remediation roadmap.

- **Technical Report** – The technical report will consist of the specific details identified during testing. Throughout testing, the Platform collects log information as well as captures screenshots to demonstrate proof of validation of identified vulnerabilities. The technical report also includes recommendations with regard to how to remediate the identified Pen Test findings.

Assumptions and Exclusions

General Assumptions

This engagement will be conducted with the assistance and cooperation of you and the contacts in the platform. As part of the engagement, each party agrees to the following:

1. Kaseya

A. The work is to be performed consecutively until project completion, according to the allowed testing times provided by you.

B. All Platform Information, including archived information is considered as sensitive and confidential and will be protected based on the confidentiality provisions of the Kaseya Master Agreement.

C. We will notify you of any delays in services as soon as reasonably possible through the Platform in order to determine ways to manage any impact (e.g. cost, modifications, etc.).

D. All Reports will be presented to you in the Platform for review and comments within **5 business days** of the completion of the CREST Pen Test. For a period of ninety (90) days after Reports are delivered, you may submit questions/comments and requests via the platform to our support team for review.

E. Kaseya implements controls with the goal of preventing or detecting and acting upon the introduction of unauthorized or malicious software during the testing process.

F. Kaseya is not responsible for providing services or performing tasks not specifically set forth in this SOW.

2. Your Cooperation and Obligations

A. During the project scheduling and testing, you will provide the start date of the test, the type of test to be performed (internal or external), the allowed time of testing, and the IPs to be tested. This data will be protected as Confidential Information under the Kaseya Master Agreement.

B. You will provide a primary point of contact within the organization to help Kaseya coordinate access to the required project materials and personnel.

C. You will provide the necessary information in the platform to perform the requested services within a timely manner.

D. Kaseya will be reliant on the information provided in the platform to complete the Pen Testing.

E. You control the amount of time Platform Information is stored in the Platform through the “Auto-Purge Data” option, **up to 365 days**. All data will be purged based on this policy, and you understand Kaseya reserves the right to purge all Platform Data that is older than one (1) year.

Complaint Handling

Complaint Process

Kaseya follows the complaint handling process described in the CREST Code of Conduct. Pursuant to that process, you have the right to lodge complaints regarding the CREST Pen Test (or about Kaseya as a CREST Member Company) with CREST. The CREST Code of Conduct, along with its complaint handling process, is accessible here. .

Contacting CREST

If you believe that Kaseya's CREST Pen Testing process does not meet the requirements of CREST, and should you wish to notify CREST of the general nature of their complaint or the incident, you may email governance@crest approved.org. CREST documentation states that upon receipt of a potential complaint, CREST will register the relevant details and, based on the nature of the potential complaint or incident, will determine if any other individuals need to be involved in the investigation.

Quality Policy Statement

Our Quality Policy is defined and strongly driven by the following management principles and behaviors:

- Build a mutually profitable relationship with our customers, ensuring their long-term success, through the understanding of their needs and the needs of their customers as well
- Achieve our commitments for quality, cost, and schedule
  Enhance the systematic research and use of best practices for network penetration testing
- Drive continual improvement and innovation based upon efficient business processes, well-defined measurements, best practices, and customer surveys
- Comply with all applicable statutory, regulatory, and contractual requirements
- Develop staff competencies, creativity, empowerment and accountability through appropriate development programs and show strong management involvement and commitment

Vonahi strives to be the best provider of network penetration testing in the industry. Through the use of these guiding principles, everyone in Vonahi is accountable for fully satisfying our customers by meeting or exceeding their needs and expectations with best-in-class solutions and services. Our goal is 100% customer satisfaction 100% of the time.