SecureWorks®

Statement of Work

SOW-20180103-514154-01

1/3/2018

This Statement of Work ("SOW") is entered into by and between **DELL MARKETING, L.P.**, with its principal place of business located at One Dell Way, Round Rock, Texas 78682 ("Dell") and **City of Grand Junction** with its principal place of business located at **250 N 5th St, Grand Junction, CO 81501-2668**("Customer") as of the SOW Effective Date, which is defined by the latest date in the signature blocks below. Dell and Customer hereafter referred to together as the "parties", and each, a "party". For the purposes of this Statement of Work, services performed hereunder may be performed by Dell, or one of its affiliates, such as SecureWorks, Inc. ("SecureWorks").

1 Scope

Under this SOW, Secureworks will provide Customer with **Incident Management Retained** service ("Service") as such Services are described in detail below.

- **Incident Management Retained Services**

1.1 Incident Management Retained Services

The Incident Management Retained Services that Secureworks offers provides the full spectrum of use cases and capability maturity for Incident Management. Customer agrees to the purchase of a block of hours as set forth in Service Fees and Expenses section below ("Retained Hours") from Secureworks to be utilized for one or more Secureworks proactive or reactive Incident Management Services at Customer's choosing and as further described below with a commitment from Secureworks to a response time for reactive Incident Management Services.

Customer, as needed and as requested, may apply the Retained Hours against one or more Incident Management Services set forth below. Each Incident Management Service requested by Customer and performed by Secureworks shall be referred to hereafter to as "*an Engagement.*"

Secureworks can perform any combination of the following Incident Management Services listed below. (These Services are conducted on a commercially reasonable effort basis, as it relates to the efficacy, usability and completeness of the artifacts available and the time allocated by Customer.)

1.1.1 Initiation of an Engagement

Once Customer initiates a request for incident response ("IR") services ("IR Services") through any of the predefined escalation channels, Secureworks IR personnel will draft and coordinate the exchange of an "Engagement Request for Incident Management Services" document in a form substantially similar to Exhibit B attached hereto. For notifications made into the Secureworks Security Operations Center ("SOC") with a request for Incident Management Services, the SOC will notify IR personnel. IR personnel will make contact with the Customer via designated communication channels as soon as reasonable, but no longer than four (4) hours after being notified by the SOC. During the initial conversation, Customer and IR personnel will determine the appropriate course of action based on the estimated work effort required.

This SOW provides priority access to Secureworks personnel who are available 24/7/365 via a dedicated phone-line or ticket requests to the SOC via the Secureworks customer portal ("Portal"). Preliminary direction and advice can be provided by SOC personnel. If the circumstance is deemed serious and additional expertise is desired, Secureworks IR personnel can be notified to engage with Customer personnel to conduct an in-briefing and begin assessment of the known facts. Estimated work effort required will be provided once Customer engages Secureworks IR personnel with a request for IR Service and the nature and scope of the incident is initially assessed.

Secureworks will assign no less than one Incident Handler ("Incident Handler(s)") and one Senior Delivery Manager ("Delivery Manager") to the IR Engagement.

1.2 Out of Scope

Locations, devices, or personnel that are not specifically listed as in scope are out of scope.

1.3 Location of Services

Incident Management Retained Services

Note: In many cases, remote support can be used while IR personnel are in-transit to Customer's location.

Secureworks' individuals may engage in a combination of onsite and remote work effort. Other IR, Security, and Risk Consulting, ("SRC"), Counter Threat Unit ("CTU") and/or SOC analysts may work at Secureworks facilities in coordination with the primary Engagement personnel. Customer understands and acknowledges that Incident Handlers may be selected for their overall experience in handling Engagements specific to the nature of the incident as well as their availability and geographic proximity to the Customer's location(s).

Onsite Response Supported Locations (United States of America, United Kingdom, Australia, and Japan):

250 N 5th St

Grand Junction, CO 81501-2668

Secureworks reserves the right to limit travel to locations currently considered by Secureworks as unsafe for traveling personnel. Secureworks may also designate certain locations as requiring security escort personnel, at additional Customer expense, where Secureworks believes it to be necessary for the safety of our personnel. Customer will be notified at the time services are requested if additional security is required for a specific location and Customer will be required to authorize the additional expense before travel is arranged.

2 Timeline and Services Schedules

Incident Management Retained Services Timeline

- Proactive Services
  - Onsite work will be performed Monday-Friday, 8 am – 6 pm local time.
  - Remote work may occur Monday-Friday, 8 am – 6 pm local time for the assigned resource.
- Reactive Services
  - After first understanding the nature and scope of the declared cyber incident, Secureworks will schedule available Secureworks Incident Response ("IR") personnel consistent with your response goals, the specified sense of urgency, and in compliance with applicable laws or ordinances, if any.

3 Methodology

3.1 Incident Management Response Services Pre-Planning and Coordination

Upon Secureworks' receipt of this Customer executed SOW; Secureworks will begin establishing workflows to support Customer requests for Incident Management Services. The following actions will be taken by Secureworks personnel and are considered non-billable:

- Distribute contact information to Customer for engaging with Secureworks for IR and digital forensics services. Contact information includes the 24/7/365 IR hotline, the IR Resource Coordinator and IR Senior Managers;
- Provide Customer with artifact acquisition, chain of custody and secure transport instructions;
- Facilitate a Service initiation conference call with the Customer point of contact to review all Services available, clarify escalation channels and verify Customer contact information;
- Provision Customer access to the Portal for IR and forensics service request tickets;
- Coordinate Retained Hour utilization notifications and facilitate non-billable, on-demand meetings to scope proactive and reactive Service Engagements.

3.2 Retained Incident Management Services

3.2.1 Incident Management Briefings and Advisory

Upon Secureworks' receipt of a Customer authorized Engagement request, conference calls or onsite workshops can be arranged to review lessons learned from previous incidents that have occurred, to review the overall status of the Customer's Incident Management program, or provide guidance on topics of interest that fall within the domain of Incident Management.

3.3 Proactive Service Options

3.3.1 Incident Management Workshop

Upon Secureworks' receipt of a Customer authorized Engagement request, an onsite Secureworks consultant ("Consultant") led workshop can be arranged during the Services initiation process to review IR capabilities with Customer key personnel and conduct a tabletop exercise to establish IR processes for engaging with Secureworks for Incident Management Services. This optional workshop allows Secureworks to become familiar with Customer's organizational risk profile, logging and detection capabilities, IR capabilities, and key personnel prior to responding to any active IR support requests. This workshop will support the creation of an information profile on the Customer's environment for Secureworks IR personnel to provide more efficient and tailored Services.

3.3.2 Incident Response Plan and Playbook Reviews

Upon Secureworks' receipt of a Customer authorized Engagement request, Secureworks will conduct a detailed review of Customer's existing IR capabilities. Secureworks will request documentation that supports the effort to understand the Customer's current IR posture and practices in order to provide an analysis of IR capabilities based on Secureworks' breadth of experience, recommendations based on assessment of Customer's environment and relevant standards or regulatory requirements. The documentation requested will consist of items such as process diagrams, policies, procedures, guidelines, and any other pertinent information to help Secureworks understand Customer's current practices and regulatory requirements. As deemed necessary, facilitated workshops and interviews may also be conducted with Customer key stakeholders to rapidly gather a deeper understanding of overall requirements, critical business requirements, and existing response capabilities. It is anticipated that Customer's Engagement point of contact will provide the requested information and access to key stakeholders as rapidly as possible once the Engagement begins. At the close of the Engagement, Customer will receive a risk prioritized findings and recommendations report to improve IR practices.

3.3.3 Incident Response Training Workshops and Exercises

Upon, Secureworks' receipt of a Customer authorized Engagement request, Secureworks will facilitate IR Training Workshops with specific topics customized to improve Customer's IR capabilities. Secureworks will also test Customer's IR plan with facilitated tabletop and functional exercises. Secureworks testing exercises feature tailored threat scenarios relevant to Customer's organization that are intended to proactively highlight gaps or issues with Customer's strategies and plans.

3.3.3.1 Incident Response Training Workshops

The content covered in IR Training Workshops will vary based on the maturity of existing capabilities and desired objectives. Available IR Training Workshop options may include:

- IR Fundamentals
- Evidence Handling and Chain of Custody
- Volatile Data Collection and Analysis
- Forensic Imaging Techniques
- Basic Forensic Analysis
- Malware Analysis for First Responders

3.3.3.2 Incident Response Tabletop Exercises

An IR tabletop exercise involves assembling key IR stakeholders in a single place and walking through a scripted exercise. The facilitator releases information concerning the incident in a controlled manner that will guide the exercise, while each stakeholder describes the role they would play in a real incident. IR tabletop exercises are an efficient way to familiarize staff with IR practices and proactively test existing response plans. IR tabletop exercises are highly effective to validate roles, responsibilities, coordination, and decision-making.

3.3.3.3 Incident Response Functional Exercises

Functional exercises are appropriate after tabletop IR exercises have already been performed and lessons learned from previous tabletop IR exercises have already been adopted. Functional exercises allow Customer's personnel to validate their operational readiness for incidents by performing their duties in a simulated manner. Functional exercises are designed to exercise the roles and responsibilities of specific team members and procedures in one or more functional aspects of a plan. Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Secureworks can coordinate overt and covert IR functional exercises.

An overt functional exercise involves the participants functionally performing each step of the plan as if it were a real incident. All participants are aware that it is an exercise, but attempt to perform actual response activities during the exercise.

A covert functional exercise is where only the Engagement point of contact or their designee is aware that the testing is an exercise. Typically, only organizations that have mature response capabilities undertake covert functional exercises due to the complexity of preparing and coordinating this type of response exercise.

IR training and exercise Engagements include the following major delivery phases:

- One Consultant will review existing IR materials and work with the Customer Engagement point of contact to verify the overall test plan and scenario injects are appropriate;

- At least one Consultant will be scheduled for one day onsite to function as the facilitator and data collector for the exercise. For exercise groups larger than ten people, for exercises that span multiple locations, or for any functional exercises, the facilitator and data collector roles will require at least two Consultants;
- One Consultant will provide Engagement after action reporting and follow-up support.

At the close of a training or response exercise Engagement, Customer will receive an after action report that summarizes the event activities with risk prioritized findings and recommendations to improve IR practices.

3.3.4 Incident Response Plan and Playbook Development

Upon Secureworks' receipt of a Customer authorized Engagement request, Secureworks will assist with developing IR Plan materials at both a strategic and tactical level. At the strategic level, Secureworks will assist with IR plan development, security policy integration, capability development, and governance. From a tactical standpoint, Secureworks will help define IR workflows, roles and responsibilities, as well as detection and response procedures specific to Customer's organization.

Secureworks will request documentation that supports the effort to understand Customer's current posture and practices in order to draft IR materials tailored to Customer's organization. The documentation requested will consist of items such as process diagrams, policies, procedures, guidelines and any other pertinent information necessary to help Secureworks to understand current practices and regulatory requirements. As deemed necessary, facilitated workshops and interviews may also be conducted with Customer key stakeholders to rapidly gather a deeper understanding of overall requirements, critical business requirements, and existing response capabilities. It is anticipated that Customer's Engagement point of contact will provide the requested information and access to key stakeholders as rapidly as possible once the Engagement begins.

Please note that this Engagement requires ample commitment and participation by Customer representatives by actively participating in the development process, providing information in a timely manner and reviewing drafted content to confirm the material is suitable for Customer's organization.

Secureworks will create IR Plans incorporating any previously available content that may include the following sections:

- IR Charter
- Delineation of Roles, Responsibilities, Dependencies and Levels of Authority for Incidents
- Incident Categorization and Severity Definitions
- Procedural Flows and Escalation Procedures for Incident Handling
  - Event Detection Process
  - Triage and Analysis Process
  - Incident Declaration Process
  - IR and Recovery Process
  - Incident Communication Process
- Reporting Procedures, Templates and Forms
- Response Team, Key Vendor and Law Enforcement Contact Information
- Internal and External Notification Requirements
- Employee Awareness and Readiness Training
- Post-Incident Analysis and Improvement Process

- IR Metrics

3.3.5 Compromise Screening Assessment

Upon Secureworks' receipt of a Customer authorized Engagement request, Secureworks will perform compromise screening assessments that may include the analysis of log data, packet captures and forensically acquired images from key devices within Customer's infrastructure.

These artifacts will be analyzed for signs indicative of compromise activity. Artifacts will be analyzed as needed, based on availability and relevance to the assessment scope and required work effort. The data from these artifacts will be screened for threat indicators using a combination of publically available and Secureworks proprietary tools and methods. These proprietary tools and methods will be used to identify patterns of behavior and communications that may indicate unknown compromise activity. Any log data should be provided to Secureworks in a clear text format that enables the application of threat intelligence. The storage size of artifacts to be analyzed will be assumed to be the actual, uncompressed volume of data when estimating level of effort.

As deemed necessary and appropriate, Secureworks may deploy live network traffic analysis appliances on Customer's network to obtain a network-centric view of live traffic with the aim of identifying active connections to known malicious addresses, command and control servers and traffic patterns representative of malware.

To deploy these live network traffic analysis appliances, Secureworks will work with Customer's personnel to select appropriate network locations that will inspect as much "host-to-Internet" traffic as possible so that an appropriate amount of data is collected and analyzed. The live network traffic analysis appliances will only operate in detection mode and not alter or block any traffic during the Engagement.

The design and placement of the live network traffic analysis appliances will be verified in the early stages of the Engagement and may consist of one or more sensor live network traffic analysis appliances. Customer personnel must perform minor network configuration changes to accommodate network traffic analysis. Management and analysis access to the sensors live network traffic analysis appliances will be finalized during the pre-deployment phase. Secureworks will manage and operate the live network traffic analysis appliances for the duration of the Engagement.

When any compromise activity is identified, Secureworks can help plan containment and eradication or conduct post-incident forensic analysis. At the close of the assessment, Customer will receive a findings and recommendations report that includes any compromise activity observed and recommendations to improve IR practices.

3.3.6 Incident Management Risk Assessment

Upon Secureworks' receipt of a Customer authorized Engagement request, Secureworks will conduct an operational and technical risk assessment of Customer's incident management capabilities to detect and mitigate malicious threat actors and commonly exploited threat vectors. An operational review will be conducted to assess current IR practices and measure capability maturity relative to Secureworks' breadth of experience for threat scenarios of concern. A technical review can also be performed to validate IR operational practices and identify any gaps in compromise detection capabilities. The Incident Management Risk Assessment can inform any modifications required for IR strategy, plans, playbooks, and testing practices. When any compromise activity is identified during the technical review, Secureworks will help plan containment and eradication or conduct post-incident forensic analysis. At the close of the Engagement, Customer will receive a risk prioritized findings and recommendations report to improve IR practices.

3.4 Reactive Service Options

3.4.1 Digital Forensics and Incident Response Services

Upon Secureworks' receipt of a Customer authorized Engagement request, Secureworks can provide Digital Forensics and Incident Response ("DFIR") Services. Once an incident is declared by Customer and depending on the circumstances of the incident, Secureworks can provide onsite or remote support.

In order to maintain independence during the investigation, Secureworks will not perform remediation activities. This includes the removal or cleaning of any identified malicious code or root kits, or any other similar items. Secureworks can assist in the development of remediation plans to address immediate weaknesses intended to limit the extent of the incident and minimize the potential for additional loss or damage.

3.4.2 Incident Response Services

Secureworks Incident Handler(s) may attempt to establish all or part of the following:

- Provide written and/or verbal guidance for Customer artifact collection.
- Provide chain of custody procedures and documentation.
- Provide guidance and/or recommendations on remediating vulnerabilities discovered.
- Conduct forensic analysis of hard drive(s) from Customer environment that the incident affected.
- Conduct memory analysis of computer systems from Customer environment that the incident may have affected.
- Conduct analysis of mobile devices from Customer's environment that the incident may have affected.
- Analysis of network traffic traversing internal or external boundaries.
- Perform custom searches based on key terms, user names, registry entries, file names, file types, and/or time frame of interest.
- Analysis of network or system log events related to the Customer incident.
- Assessment of any recent vulnerability scans, penetration tests, web application tests, to assist in determining the unauthorized point(s) of entry.
- Conduct analysis of open source and proprietary Threat Intelligence sources that may provide information about threats, vulnerabilities, or risks related to the incident.
- Conduct analysis of malware or other binary files that may be involved in the incident.
- Provide indicators of the incident and threat for use by Customer remediating the incident.
- Provide any evidence discovered that indicates the likeness of the threat of concern.
- Incident summary and recommendations on risk management options.
- Provide media disposition per mutually agreed upon process. Additional costs may apply.

3.4.3 Digital Forensic Analysis Services

Using a variety of forensics tools and methods, Secureworks can acquire, analyze, and recover data stored in the following formats:

- Disk drives
- RAID systems
- Portable storage drives

- Mobile devices
- Other digital media formats for analysis or data recovery

3.4.4 Anti-Phishing Response Services

Secureworks can analyze phishing incidents. This can involve a variety of methodologies, depending on the nature of the incident. The objective is to gain as much information as possible about the incident to facilitate containment. A partial list of techniques includes:

- Networking analysis techniques (traceroute, DNS lookups, ARIN searches, OS fingerprinting, scanning, system enumeration, foot-printing, etc.).
- Application analysis techniques: website code reviews, email analysis, server configuration, etc.
- Research, including IRC, USENET, Websites.
- Analysis of propagation methodologies and magnitudes (i.e., how is the Phishing incident being spread?).
- Severity Assessment, including analysis of the impact of the incident.
- Log review—web logs, server logs, firewall logs, etc.
- Reverse lookup phone numbers used in attacks.
- Notification to mobile phone ISPs.
- Toll free reverse lookup.

No commitments of Customer resources will be made without clear consent from authorized Customer personnel. With guidance and consent from Customer management where needed, Secureworks will coordinate, manage, and facilitate an appropriate selection of countermeasures to have the Phishing site taken offline. These countermeasures will be selected and deployed dependent on the evolving analysis of the particular incident underway. Successful takedown is often dependent on cooperation of third parties such as internet service providers ("ISPs"), hosting providers, and domain registrars, among others. Secureworks does not take offensive measure to takedown phishing sites.

3.4.5 Incident Coordination Services

Secureworks performs incident handling and digital forensic analysis Services, and in addition can provide advisory Services in the analysis and handling of incidents. During IR, Secureworks often collaborates with executive teams, legal, public relations and other Customer key stakeholders. Secureworks' role is to provide these key stakeholders findings and impact assessments derived from IR and forensics work effort. These coordination activities may include:

- Coordinating the Engagement in-brief and regular status meetings.
- Scope definition and management during the course of the Engagement.
- Engagement staff and resource management.
- Engagement status reporting.
- Engagement deliverable reporting.
- Engagement support with the Customer and through the Customer, with other third parties.

3.4.6 Cloud Incident Response Services

Secureworks will provide IR Services for the coordination, analysis, and handling of incidents involving the Customer Cloud Computing architecture. The Service will review evidence of compromise activity that can exist in Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software-as-a- Service (SaaS) Cloud Computing architectures. Secureworks IR personnel can perform investigations to determine nature and extent of suspected intrusions involving Public, Private, and Hybrid Cloud Computing architectures with the Customer and through the Customer when they are end users of Cloud Service Providers (CSPs). Cloud IR Services are highly dependent on prevailing organizational, legal, and technical factors that may complicate investigations involving the Customer Cloud Computing architecture and are conducted on a commercially reasonable effort basis.

3.5 Premium Services

Premium Services are available to assist with incident response work effort or are available as stand-alone Services. Premium Services will be billed at the Premium Services rate in accordance with the Service Fees and Expenses section.

3.5.1 Advanced Malware Analysis and Reverse Engineering Services

Should the Customer identify malicious code of an unknown type, Secureworks can be engaged to reverse engineer the code to better understand the code's capabilities. Secureworks has extensive experience and expertise in malware reverse engineering, but this activity is conducted on a commercially reasonable effort basis because not all code can be successfully reverse-engineered. Secureworks will offer an opinion on the code's potential impact and effect on Customer assets.

3.5.2 Incident Surveillance Services

In an effort to ascertain additional information about the attack source and methods, Secureworks will attempt to:

- Find specific references to Customer assets affected by the current attack within underground communications.
- Identify specific references to Customer assets in attack tools or malware "kits."
- Research historic proprietary and public data regarding targeted attacks against Customer assets.
- Monitor and analyze underground communications pertaining to the active attack.

Customer will work with Secureworks to provide specific information on the assets to be covered under this project (e.g., names, identifiers, IP address ranges, brands, etc.) for correlation in counterintelligence during the active attack phase.

3.5.3 Targeted Threat Hunting and Response

Upon Secureworks' receipt of a Customer authorized Engagement request, Secureworks can perform a Targeted Threat Hunting and Response assessment, as set forth and described below, in the Customer environment. This service leverages Secureworks' proprietary methodology, expertise, and intelligence related to advanced threat actors and their techniques, tactics and procedures (TTP). Targeted Threat Hunting and Response is specifically designed for customers that need to understand their exposure to targeted threats, and attempts to identify existing adversary presence or tradecraft in the Customer environment. The service will review evidence that may persist in network infrastructure logs, and analyze endpoint systems and other relevant data stored within the organization, to identify indicators of intrusion. When intrusions are identified, Secureworks can help plan and execute threat actor containment and eradication. At the close of the Engagement, Customer will receive a findings and recommendations report that includes any targeted threat activity observed and recommendations to improve IR practices.

The following methods may be used by the Consultants for this Engagement. These method descriptions are provided to describe the techniques that may be used, as agreed upon with the Customer. These methods are not in scope unless identified in the Scope of Work defined in the Engagement request order in a format substantially similar to Exhibit B, but may be added by the methods listed in the **Service Fees and Expenses** section below.

NOTE: This service requires a minimum of 80 hours of Premium Services at the Premium Services Rate as defined in the Service Fees and Expenses section.

3.5.3.1 Pre-Engagement Planning

Prior to the Engagement, the Customer will provide the assigned Secureworks team members with a completed Targeted Threat Hunting and Response Service Questionnaire and the required supporting documentation, including host and network architecture information. Secureworks will work with the customer to identify data necessary to complete the assessment and identify available sources of required data, or formulate a plan to obtain the required data. This information will be thoroughly reviewed to prepare Secureworks consultants for the Engagement.

Additional environment instrumentation (IDS/IPS, etc.) may be required to obtain the necessary data, and in these cases, Secureworks will work with the Customer to identify options they can implement prior to the Engagement. If additional instrumentation is required to effectively perform the Engagement, the project start may be delayed.

As deemed necessary and appropriate, the Engagement may commence with a workshop involving the Customer's IT security staff and the Secureworks consultants to further collect environmental specifics and calibrate Engagement objectives.

3.5.3.2 Log Assessment

The service includes the analysis of log data from key technical elements within the Customer's network. The logs will be analyzed for entries indicative of the operation of malicious software or threat actor activity. Logs will be analyzed as needed, based on availability and relevance to the assessment work.

The data from these logs will be screened for targeted threat and malware indicators using a mixture of publically available and Secureworks proprietary tools. These tools will be used to identify patterns of behavior and communications with suspicious IP addresses that may indicate the presence of malware. Due to the complexity of the search algorithms and the size of the databases behind them, some of this processing work will need to be carried out on Secureworks' owned and operated platforms.

Logs should be provided to Secureworks on disk or other storage media, or alternatively made available in a form that enables them to write code to apply intelligence to the logs. The storage size of logs to be analyzed will be assumed to be the actual, uncompressed volume when estimating the scope of work effort.

3.5.3.3 Network Traffic Analysis

As deemed necessary and appropriate, Secureworks may deploy live network traffic analysis ("Network Traffic Analysis") appliances on Customer's network to obtain a network-centric view of live traffic with the aim of identifying active connections to known malicious addresses, command and control servers, and traffic patterns that are representative of known malware.

To deploy the appliances, Secureworks will work with Customer to select appropriate network locations that will inspect as much "host-to-Internet" traffic as possible so that an appropriate amount of data is collected and analyzed. The live Network Traffic Analysis appliances will only operate in detection mode and not alter or block any traffic during the Engagement. Secureworks will deploy a maximum of two appliances in Customer's network. Additional appliances can be deployed for an additional fee; we will work with Customer to determine if additional appliances are required.

The design and placement of the live network traffic analysis appliances will be verified in the early stages of the Engagement and may consist of one or more sensor live network traffic analysis appliances. Customer personnel must perform minor network configuration changes to accommodate network traffic analysis. Management and analysis access to the sensors live network traffic analysis appliances will be finalized during the pre-deployment phase. Secureworks will manage and operate the live network traffic analysis appliances for the duration of the Engagement.

3.5.3.4 Endpoint Assessment – Malware Hunting

The purpose of the malware hunting portion of the Engagement is to search systems within scope for threat indicators. Based on the results, hosts will be categorized as confirmed compromised, exhibiting suspicious threat indicators or exhibiting no known threat indicators. Secureworks will conduct the following activities for the malware hunting exercise:

- Coordinate with the Customer team to execute the scans using one of several methodologies for connecting to the systems within scope.
- Run sample test scans to ensure the methodology is suitable for the target environment.
- Scan systems for Threat Indicators using a combination of proprietary Secureworks tools, processes, and intelligence.
- Receive scan results into an agreed upon and established repository.
- Review the scan results using threat intelligence, filter logic, and established methodology.
- Refine Threat Indicator set as necessary based on findings from initial scans.
- Investigate any suspicious indicators/systems.
- Working iteratively, we will repeat certain steps above, to categorize the systems according to their level of risk/suspicion.
- Prepare findings for Customer including systems scanned, detected indicators and follow-up actions.

3.5.3.5 Containment and Response

Once sufficient evidence has been collected, the Secureworks team will help define a customized containment and eradication plan. This plan is developed in preparation for rapid execution across the organization during a specified timeframe, locking down systems and adversary access in a swift motion. This plan is also likely to include a strategy to monitor for the adversary's attempts to re-enter Customer systems. All plans and work effort will be developed with the Customer and approved by Customer prior to execution.

4 Deliverables

4.1 Incident Management Retained Services

Presentation of the findings and exact deliverables compiled by Secureworks in the performance of the Services (the "Customer Report" or "Report") are tailored to the type of work performed, and to Customer's needs. The scope of the final Customer Report will be defined during the planning phase, and may include interim or ad-hoc reporting. The Customer Report will focus on the information most relevant to Customer specifically as it relates to Customer's business, operational and risk mitigation goals.

Customer Report format considerations:

- Timing of requested Customer Report.
- Complexity of the incident.
- Customer updates during the analysis, even if the incident and analysis is incomplete and opinion is only provisional.

- The complexity and sufficiency of the evidence that must be analyzed before a logically supportable opinion can be formed.
- The audience for the Customer Report, and their requirements (for example, law enforcement, boards of directors, regulatory agencies, internal executive staff, internal IT staff, etc.).

Customer Reports may include:

- Regular Status Reporting (written or verbal per Customer request)
  - Summary of activities completed
  - Issues requiring attention and plans for the next work effort period
  - Updates will initially be provided on a daily basis for active incident response Engagements; thereafter, weekly updates may be provided for extended Engagements.
- Incident Response Report that documents the event with the following information where possible
  - Identifying the details of the incident in sequential order
  - Associating a timeline with the incident
  - Identifying any sequential or cascading components of the incident
  - Identifying the specific attack vector used and the specific vulnerability exploited at each stage of the incident
  - Establishing the root cause of the incident
  - Assessment of impact
  - Identify areas of improvement to existing information security practices
- Chain of Custody Documents
- Engagement Findings Report
- Incident Response Plan Materials

Within three (3) weeks of completing an Engagement, Secureworks will issue a draft formal Report to Customer's designated point of contact. Customer shall have three (3) weeks from delivery of such draft formal Report to provide comments concerning the nature and scope of the Engagement to be included in the final Report (the "Report Review Period"). If there are no comments received from Customer before the expiration of the Report Review Period, the Report shall be deemed final and Secureworks will finalize for distribution. If no changes are required, we encourage you to accept the formal report prior to the three week waiting period to expedite final delivery.

5 Service Fees and Expenses

5.1 Service Fees

As designated by Dell quote

5.2 Premium Services

Retained Hourly Rate for Premium Service Options: $500

Retained hours at the Standard Retainer Rate may be applied to Premium Services based on a factor to convert those hours to the nearest half hour increment; additional Premium Service hours at the Premium Services Rate may be required and added as needed, with Customer approval, to successfully accomplish the goal.

5.2.1 Endpoint Assessment – Malware Hunting

The Targeted Threat Hunting Endpoint Assessment service requires the deployment and support of additional host software that is billed monthly at a rate of $.50 per endpoint.

5.3 Billing for Services

Incident Management Retained Services

- Retained Hours will be tracked in quarter hour increments.
- Secureworks will keep Customer informed of the balance of Customer Retained Hours.
- Each service request will be scoped, and a minimum commitment of hours will be established prior to service initiation. Those minimum committed hours will be decremented from Customer Retained Hours.
- Hours spent delivering Premium Services are billed at the Premium Services rate.
- Any distinction, variation, or designation of work that will be categorized as a "Premium Service" will be mutually understood and agreed upon before assignment or work is performed
- A monthly fee of $0.50 per endpoint applies in addition to Service Fees should Secureworks and Customer agree that malware detection and analysis on endpoint devices be applicable.
- Malware analysis or reverse engineering work effort associated with Incident Response or Digital Forensic Analysis Services will be billed at the Standard Services rate. Stand-alone requests for malware analysis or reverse engineering services will be billed at the Premium Services rate.
- As deemed necessary and appropriate by Secureworks and Customer, Secureworks will deploy a maximum of two network traffic analysis appliances at Customer site during the course of IR service delivery at no cost. As deemed necessary and appropriate by Secureworks and Customer, Secureworks will charge the following one-time fees in addition to Service Fees for each additional network traffic analysis appliance deployed at Customer site during the course of IR service delivery: $3,100 USD per one (1) gigabit Ethernet copper appliance; $7,200 USD per ten (10) gigabit Ethernet copper appliance; and $7,500 USD per ten (10) gigabit Ethernet fiber appliance.
- Includes hours spent on delivering work, reporting, project management and all other work performed in this Engagement. Customer will not be invoiced for time spent traveling an onsite response supported location.
- Reasonable out of pocket expenses for dedicated hardware, software and shipping costs as necessary for the Engagement as well as travel, food and lodging will be invoiced separately at actual costs.
- The determination of whether Secureworks IR personnel are used for an incident will be made jointly by Customer and IR personnel during the initial contact call before any IR Services work effort is initiated.
- Any unused Retained Hours at the end of the SOW Term will be forfeited.

All Retained Hours are non-refundable and non-transferable for other Secureworks services, except those listed in this SOW.

- This is a fixed work effort contract; not a fixed price contract. Additional blocks of hours may be retained in advance of exhaustion of contracted hours at the contracted rate above by the parties by executing a change order or an additional statement of work for such additional hours.
- Customer may authorize continued work effort for active cyber incident response services beyond the committed hours in 40-hour increments, via email to irservices@Secureworks.com, to ensure

continuous delivery of services. Additional hours must be authorized prior to the exhaustion of existing hours. Customer will only be billed for actual accrued hours.

- Customer will be invoiced immediately for committed hours and monthly for additional work activity against this SOW that are authorized via email.
- Secureworks reserves the right to bill any cyber incident declared within fourteen (14) calendar days from the SOW Effective Date at the current Emergency Cyber Incident Response Services rate of $385 per hour.

5.4 Out-of-Pocket Expenses

The Service fees outlined above include all incidental out-of-pocket expenses such as report preparation and reproduction, faxes, copying, etc.

The following out-of-pocket expenses are NOT included in the Service fees: those related to transportation, meals and lodging to travel to perform the Services. Customer agrees to reimburse Secureworks for all reasonable and actual out-of-pocket expenses incurred for travel to the Customer location in the performance of the Services hereunder.

Customer acknowledges and agrees that IR by Secureworks requiring last minute air transportation will result in much higher costs than ordinary business travel as a result of the requirement to purchase tickets with little if any advance notice. Forensic work MAY also require additional costs associated with required media storage, specific equipment or licensing, depending on the size of the incident, image acquisition needs or the complexity of the incident. Such expenses will be added, at cost, to Customer's invoice.

6 Service Scheduling

6.1 Scheduling of Proactive Services

Proactive Services outlined above require a minimum of four (4) weeks advance notification in order to schedule. This allows Secureworks to schedule the appropriate resources to meet the specific Engagement requirements and ensure completion of the Engagement before the expiration of the SOW Term. The Secureworks IR Resource Coordinator is available to facilitate non-billable, on-demand meetings with IR personnel to scope Proactive Services Engagements. An email confirmation of an agreed upon schedule, sent by Secureworks, confirmed and returned by email by Customer, shall constitute formal acceptance of such schedule. Once scheduling of any onsite work at Customer's facility has been mutually agreed to, any changes by Customer to the onsite work within two (2) weeks of the onsite work to be performed will incur a $2,000 re-scheduling fee. This re-scheduling fee does not apply to work that does not require travel by Secureworks.

6.2 Scheduling of Reactive Services

Customer has 24/7/365 access to Secureworks SOC personnel and the Portal for the initial communication channel. Additional communication channels include the email addresses and phone numbers of the Secureworks IR Resource Coordinator and Senior Managers.

In the case of a Cyber Incident declared within fourteen (14) days of SOW Effective Date, Customer understands that Secureworks IR resources will be scheduled on a reasonable effort basis.

6.3 Events that require onsite Incident Handling

6.3.1 Within scope for Onsite Response Supported Locations

Secureworks shall use commercially reasonable efforts to have an incident handler arrive onsite (i.e., "onsite presence"), within thirty-six (36) hours for onsite response supported location travel after the mutual determination by Customer and IR personnel that onsite IR is required.

6.3.2 Within scope for In-Transit Response Supported Locations

In the case that visa and work permits are not required for travel to the country in question, Secureworks shall use commercially reasonable efforts to have an incident handler board a plane or other appropriate form of transportation within forty-eight (48) hours for in-transit response supported location travel after the mutual determination by Customer and IR personnel that onsite IR is required.

Customer acknowledges and agrees that it is impossible and unrealistic for Secureworks to anticipate every contingency in connection with emergency on site IR and, notwithstanding its commercially reasonable efforts, that there may be unforeseen circumstances or contingencies outside the reasonable control of Secureworks that could make compliance with the foregoing unrealistic or impossible, regardless of cost, including but not limited to: holidays, acts of war or terrorism, weather, flight availability, visa and passport requirements, restrictions of importation of encrypted technologies, handler schedules, unanticipated levels of contemporaneous emergency incident responses and other similar or dissimilar circumstances or events.

6.4 Service Scheduling and Services Hold Terms

Once the Services Term has entered the final quarter or has expired, Secureworks will implement the following restrictions on services. Secureworks has no obligation to provide Services beyond the Services Term.

6.4.1 60 Days Prior to Services Term Expiration

The following Proactive Services require a minimum of four (4) weeks advance notification in order to schedule the appropriate resources to meet the specific Engagement requirements and must be scheduled more than 60 days prior to the expiration of the Services Term to ensure completion of the Engagement before the expiration of the Services Term:

- Compromise screening assessment services
- Incident management risk assessment services
- Incident response plan and playbook development services
- Incident response plan and playbook review services
- Incident response tabletop exercises services
- Incident response functional exercises services
- Incident response training workshop services
- Incident management workshop services
- Incident management briefings and advisory services

6.4.2 At Services Term Expiration

No Proactive IR services will be available to the Customer.

7 Customer Obligations

Customer acknowledges that Secureworks' ability to perform the Services hereunder is contingent upon the following:

- Customer resources are scheduled and available.
- For onsite Services to be performed, Customer has provided suitable workspace and necessary accesses for Secureworks' staff and equipment.
- Access to Customer computer systems, devices and network as necessary to perform the Services is made available to Secureworks.
- If Customer does not own such network resources, including IP addresses, hosts, facilities, or web applications, it will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Secureworks, to permit Secureworks to provide the Service.
- Replies to all document requests and other information are timely and in accordance with the delivery dates established in the planning phase.
- Customer scheduled downtime allows adequate time for Secureworks' performance of the Services.
- Until this SOW is fully executed by both parties, Customer understands that the fees proposed herein are only valid for 90 days from the date received.

Incident Management Retained Services

- Customer's contracted third parties involved in an Engagement will be cooperative and forthcoming with required information. Such cooperation includes but is not limited to the following:
  - Actions taken during the course of the investigation
  - Findings reports from any other investigative firms
  - Providing Secureworks copies of original evidence files and or images where sound forensic processes were employed
- Customer acknowledges that they are the best informed as to their contractual privileges and responsibilities with respect to contracted third party services such as cloud or hosted environments and will provide Secureworks with authoritative positions regarding permissions to operate in third party environments for the purposes of this SOW.
- Customer accepts responsibility for obtaining any and all necessary third party authorizations required to perform services in cloud, hosted, co-location or other environments not owned by Customer.

8 SOW Term

The term of this SOW shall commence on the SOW Effective Date and terminate on the earlier to occur of (i) the date which is one (1) year thereafter, or (ii) the completion of the Services (the "SOW Term").

The term of the Services for the Incident Management Retainer shall commence on the SOW Effective Date and terminate on the earlier to occur of (i) the SOW term, or (ii) the completion of any outstanding time and materials billing (the "Services Term").

To the extent that Customer authorizes continued work effort for active cyber incident response services pursuant to the Service Fees and Expenses section, and such continued work effort extends beyond the SOW Term and/or Services Term, the SOW Term and Services Term shall be extended to the completion of such continued work effort (the "Extended Term"). During such Extended Term, the terms and conditions of this SOW and the MSA shall be in full force and effect.

Upon completion of the Services, the Customer designated contact will receive an email confirmation from Secureworks. Unless otherwise notified in writing to the contrary by the Customer designated contact within thirty (30) days of such email confirmation, the Services and this SOW shall be deemed complete.

9 Disclaimers

9.1 Onsite Services

Notwithstanding Secureworks employees' placement at the Customer location, Secureworks retains the right to control the work of such employees. For international travel, onsite Services may require additional documentation, such as Visas, visitor invitations, etc., which may affect timing of the Services and reimbursable expenses.

9.2 Security Services

Should this SOW include security scanning, testing, assessment, forensics, or remediation Services ("Security Services"), Customer understands that Secureworks may use various methods and software tools to probe network resources for security-related information and to detect actual or potential security flaws and vulnerabilities. Customer hereby authorizes Secureworks to perform such Security Services (and all such tasks and tests reasonably contemplated by or reasonably necessary to perform the Security Services or otherwise approved by Customer from time to time) on network resources with the internet protocol ("IP") Addresses identified by Customer. Customer represents that, if Customer does not own such network resources, it will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Secureworks, to permit Secureworks to provide the Security Services. Secureworks shall perform the Security Services during a timeframe mutually agreed upon with Customer. The Security Services, such as penetration testing or vulnerability assessments, may also entail buffer overflows, fat pings, operating system specific exploits, and attacks specific to custom coded applications but will exclude intentional and deliberate denial of service ("DoS") attacks. Furthermore, Customer acknowledges that the Security Services described herein could possibly result in service interruptions or degradation regarding the Customer systems and accepts those risks and consequences. Customer hereby consents and authorizes Secureworks to provide any or all the Security Services with respect to the Customer systems. Customer further acknowledges it is Customer's responsibility to restore network computer systems to a secure configuration after Secureworks' testing.

9.3 Compliance Services

Should this SOW include compliance testing, assessment, or other similar compliance advisory Services ("Compliance Services"), Customer understands that, although Secureworks' Compliance Services may discuss or relate to legal issues, Secureworks does not provide legal advice or services, none of such Compliance Services shall be deemed, construed as, or constitute legal advice and that Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries or reports provided by Secureworks in connection with any Compliance Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer legal or regulatory compliance.

9.4 Payment Card Industry (PCI) Compliance Services

Should this SOW include PCI compliance auditing, testing, assessment, or other similar PCI compliance advisory Consulting Services ("PCI Compliance Services"), Customer understands that Secureworks' PCI Compliance Services do not constitute any guarantee or assurance that security of Customer systems, networks, and assets cannot be breached or are not at risk. These PCI Compliance Services are an assessment, as of a particular date, of whether Customer systems, networks and assets, and any compensating controls meet the applicable PCI standards. Mere compliance with PCI standards may not be sufficient to eliminate all risks of a security breach of Customer systems, networks, and assets. Furthermore, Secureworks is not responsible for updating its reports and assessments, or enquiring as to the occurrence or absence of such, in light of subsequent changes to Customer systems, networks, and assets after the date that the final Report is created, absent a separately signed statement of work expressly requiring the same.

9.5 Record Retention

Secureworks will retain a copy of the Customer Reports and supporting Customer Data in accordance with Secureworks' record retention policy, which provides such retention for a period commensurate with such Customer Reports and supporting Customer Data usefulness and Secureworks' legal and regulatory requirements and Secureworks' directives.

Unless Customer gives Secureworks written notice to the contrary prior thereto, then thirty (30) days after delivery of its final report, Secureworks shall have the right, in its sole discretion, to dispose of all acquired hard drive images and other report backup information acquired in connection with its performance of its obligations under this SOW.

9.6 Post Engagement Activities

Upon the "Engagement Conclusion" defined as the earlier to occur of (i) acceptance by Customer of the final Customer Report, or (ii) thirty (30) days after the delivery of the final Customer Report, Secureworks will commence with the appropriate media sanitization and/or destruction procedures of the Customer acquired images, hard drives or other media obtained by Secureworks in the performance of the Services hereunder (the "Incident Media"), unless prior to such commencement, Customer has specified in writing to Secureworks any special requirements for Secureworks to return such Incident Media (at Customer's sole expense). Upon Customer's request, Secureworks will provide options for the transfer to Customer of Incident Media and the related costs thereto. If so requested, Secureworks will provide a confirmation letter to Customer addressing completion and scope of these post incident activities, in Secureworks' standard form. Unless agreed to otherwise by the parties, Secureworks shall, in its sole discretion, dispose of the Incident Media on or after the Engagement conclusion and only maintain a copy of the final Customer Report and associated deliverables.

9.7 Legal Proceedings

If Customer knows or has reason to believe that Secureworks or its employees performing Services under this SOW have or will become subject to any order or process of a court, administrative agency or governmental proceeding (e.g., subpoena to provide testimony or documents, search warrant, or discovery request), which will require Secureworks or such employees to respond to such order or process and/or to testify at such proceeding, Customer will (i) promptly notify Secureworks, unless otherwise prohibited by such order or process, (ii) use commercially reasonable efforts to reduce the burdens associated with the response, and (iii) reimburse Secureworks for (a) its employees' time spent as to such response at the hourly rate reflected in this SOW, (b) its reasonable and actual attorney's fees as to such response, and (c) its reasonable and actual travel expenses incurred as to such response. Nothing in this paragraph shall apply to any legal actions or proceedings between Customer and Secureworks as to the Services or this SOW.

9.8 Endpoint Assessment – Malware Hunting

Unless otherwise agreed upon in writing, within thirty (30) days following the expiration or termination of this SOW (the "Thirty Day Period"), Customer shall uninstall any and all copies of the software agent used for Malware Hunting. During the Thirty Day Period, (i) Customer shall not use the software agent, and (ii) the license and use restrictions that apply to the software agent remain in effect notwithstanding the expiration of termination of the Service. Customer will install Secureworks' proprietary software agent if Endpoint Assessment Services are in scope. Customer (i) will use the Endpoint Assessment software agent for its internal security purposes, and (ii) will not, for itself, any Affiliate of Customer or any third party: (a) decipher, decompile, disassemble, reconstruct, translate, reverse engineer, or discover any source code of the software agent; and (b) will not remove any language or designation indicating the confidential nature thereof or the proprietary rights of Secureworks from the software agent. Customer will uninstall the software agent as described in this SOW.

9.9 Payment Card Industry Forensic Investigator (PFI) Services

Customer is not entitled to PCI Forensic Investigator services under this SOW. If PCI Forensic Investigator services are required, a separate SOW must be scoped and executed for PCI Forensic Investigator services.

This SOW is agreed to by the parties. Any terms and conditions attached to a purchase order submitted by Customer in connection with this SOW are null and void.

	Dell Marketing L.P.		City of Grand Junction 250 N 5th St Grand Junction, CO 81501-2668
By:	Teri L Miller	By:	Scott Hockins
Printed:	Teri L. Miller	Printed:	Scott Hockins
Title:	chief Accounting Officer	Title:	Purchasing Supervisor
Date:	2/5/2018	Date:	1/31/2018

SFDC: 0063600000PkpPiAAJ

Exhibit A - Supplemental Terms and Conditions

1. Rights in Data and Works

Customer agrees that SecureWorks is the owner of all right, title and interest in all computer programs, including any source code, object code, enhancements and modifications, all files, including input and output materials, all documentation related to such computer programs and files, all media upon which any such computer programs, files and documentation are located (including tapes, disks and other storage media) and related material developed in connection with the performance of any Services provided by SecureWorks before or after the date set forth above; provided however, that such related material shall not include information or data belonging or pertaining to Customer of affiliated entities, or it's parties. In no way limiting the foregoing, Customer agrees that all copyrights and other proprietary rights in computer programs, files, documentation, and related materials developed by SecureWorks in connection with this SOW are owned by SecureWorks and Customer hereby assigns to SecureWorks all right, title and interest in such copyrights and other proprietary rights.

2. Customer Reports

Customer agrees that any written summaries, analyses or reports provided by SecureWorks in connection with the Services ("Customer Reports") are solely for the use of Customer and its officers, directors and employees (collectively with the Customer, the "Customer Entities"). Aside from Customer Entities, Customer Reports may be provided only to parties who are under contract with the Customer to provide products or services to the systems of the Customer, provided that such parties shall keep the contents of Customer Reports confidential and shall not disclose this report or the information herein to others. The provision of any Customer Report or any information therein to the parties other than Customer Entities shall not entitle such parties to rely on any Customer Report or the contents thereof in any manner or for any purpose whatsoever, and SecureWorks specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary or punitive) arising from or related to provision of such any such Customer Report to such parties.

3. Warranties

a. **Warranties.** SecureWorks warrants that all Services provided under this SOW will be performed in a workmanlike manner by its subcontractor and in compliance with the requirements and specifications included in the applicable Statement of Work.

SecureWorks further represents and warrants that it (or its subcontractor) is under no present obligations or restrictions, which will conflict with or prevent it from performing any of the Services, called for by this SOW.

CUSTOMER'S EXCLUSIVE REMEDY FOR BREACH OF ANY WARRANTY HEREUNDER SHALL BE LIMITED TO REPERFORMANCE OF THE SERVICE OR RETURN OF THE PURCHASE PRICE.

b. **Disclaimer of Any Other Warranties.** EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS SOW, THE SERVICES AND SERVICE PRODUCTS PROVIDED BY SECUREWORKS HEREUNDER ARE PROVIDED "AS IS" WITHOUT ANY WARRANTY AS TO THEIR PERFORMANCE, ACCURACY, OR FREEDOM FROM ERROR, OR AS TO ANY RESULTS GENERATED THROUGH THEIR USE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE.

4. Limitation of Liability

a. **Consequential Damages.** The parties will not be liable to each other for indirect, special, incidental, exemplary, punitive or consequential damages (including, without limitation, lost profits, revenue, anticipated savings, or damages for loss of data or other business information) arising from or related to this SOW or any Statement of Work, regardless of the cause of action and even if the other party has been notified of the possibility of such damages.

b. **Limitation of Liability.** Under no circumstances will either party's aggregate liability to the other party for any claim exceed the amounts paid by Customer under the Statement of Work that is the source of such liability.

5. Confidentiality

Each party shall protect Confidential Information (as defined below) of the other party with at least the same degree of care it uses to protect its own confidential information, but not less than a reasonable degree of care. Neither party shall use, disclose, provide, or permit any person to obtain any such Confidential Information of the other party in any form, except for employees, agents, or independent contractors whose access is required to carry out the purposes of this SOW and who have agreed to be subject to the same restrictions as set forth herein. Violations of any provision of this Section shall be the basis for the immediate termination of this SOW. Customer's obligation as to the confidentiality shall survive termination of this SOW. "Confidential Information" means all information relating to the business or affairs of SecureWorks and the Services, including but not limited to, technical or non-technical data, software (whether in object or source code form), formulas, tools, patterns, plans, compilations, programs, devices, methods, techniques, drawings, processes, financial data. Further, Confidential Information includes information that a reasonable person would determine to be proprietary or confidential when taking into consideration its nature and the circumstances under which it is disclosed.

1 Exhibit B: SAMPLE Engagement Request for Incident Management Services

This Engagement Request documents the Incident Management Services requested by Customer that will be provided by Secureworks as a part of the Incident Management Services SOW entered into between Secureworks and Customer. This Engagement Request will be drafted by Secureworks IR personnel when a request for an Engagement is initiated by Customer through any of the defined escalation channels. Secureworks IR personnel will distribute this form to Customer via email for review and authorization to trigger Retained Hour utilization and commencement of the Engagement. This Engagement Request must be returned by an authorized representative of Customer via email prior to commencement of the Engagement set forth below.

1) Engagement Codename:

2) Engagement Contact Information:

Customer	
Engagement Address	
Point of Contact Name	
Point of Contact Email Address	
Point of Contact Primary Telephone Number	
Point of Contact Secondary Telephone Number	

Secureworks	
Primary Consultant Name	
Primary Consultant Email Address	
Primary Consultant Telephone Number	
Senior Manager Name	
Senior Manager Email Address	
Senior Manager Telephone Number	
Practice Director Name	
Practice Director Email Address	
Practice Director Telephone Number	

3) Engagement Schedule:

4) The Incident Management Services to be rendered hereunder shall commence on <MM/DD/YYYY> and are estimated be completed no later than <MM/DD/YYYY>.

5) Incident Management Services Scope of Work:

6) Incident Management Services Deliverables:

7) Incident Management Services Billable Retainer Hours Estimate*:

8) Customer Responsibilities:

9) Estimated Timeline for Requested Incident Management Services:

Time Interval	Work Effort
Week 1	
Week 2	
Week 3	
Week 4	

* The Retained Hours necessary for the completion of an Engagement may vary depending on the Customer requests and the complexity of the circumstances for such Service chosen.

2 Exhibit B: Endpoint Sensor Software Installation, Management, Maintenance and Limitation of Liability

The installation and maintenance of endpoint sensor software are the sole responsibility of the Customer.

Secureworks will not be liable for any losses, costs, or damages relating to the installation of the End Point user software. Secureworks strongly recommends that the Customer install and evaluate Endpoint Sensor software in a test environment and deploy it in small batches in accordance with the Customer's change management policies to insure there are no issues before rolling it out to the entire target endpoint population.

Secureworks will not be liable for any impact that may be incurred from installing Endpoint Sensor software on an unsupported operating system or custom built image.

Secureworks will not be liable for any impact that may be incurred from the Customer's failure to comply with the Endpoint Sensor software updating process.

Secureworks will not be liable for any losses, costs, or damages relating to the installation of the End Point user software on any endpoints not owned by the Customer.

The Software may come bundled or otherwise be distributed with open source or other third party software, which is subject to the terms and conditions of the specific license under which it is distributed. Open source software is provided by Secureworks "as is" without any warranty, express, implied, or otherwise, including, but not limited to, the implied warranty of merchantability, fitness for particular purpose and non-infringement. Notwithstanding anything to the contrary, as it relates to any and all claims arising out of or in connection with open source software, Secureworks shall have no liability for any direct, indirect, incidental, punitive, special or consequential damages, however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise,) arising in any way out of the use of open source software, even if advised of the possibility of such damages. Under certain open source software licenses, you are entitled to obtain the corresponding source files. Secureworks will provide the corresponding source files at the Customer's request.

Unless otherwise agreed upon in writing, upon expirations or termination of this SOW Customer shall uninstall any and all copies of the software agent used for Malware Hunting, including all of the end point sensor software from its environment.

Secureworks will not be liable for any losses, costs, or damages relating to the failure of Customer to remove the End Point user software from any endpoints upon expiration or termination of this SOW.

9.9.1.1 Endpoint Sensor Operating System Support

Red Cloak has support for only the following Windows operating system versions:

- Windows XP 32-bit SP2 and later
- Windows XP 64-bit SP1 and later
- Windows 2003 (32-bit and 64-bit) SP1 and later
- Windows 2003R2 (32-bit and 64-bit) and later
- Windows Vista (32-bit and 64-bit) SP0 and later
- Windows 2008 (32-bit and 64-bit) SP0 and later
- Windows 2008R2 64-blt and later
- Windows 7 (32-bit and 64-bit) SP0 and later
- Windows 8 (32-bit and 64-bit) SP0 and later
- Windows 10
- Windows 2012 (32-bit and 64-bit) SP0 and later
- Windows XP Embedded SP 3 and later
- Windows Embedded POSReady 2009
- Windows Embedded POSReady 7
- Windows Server 2012
- Windows Server 2016

Red Cloak is tested and verified on all operating systems listed as supported by Secureworks. In cases where Red Cloak supports an operating system that is no longer supported by the operating system vendor, troubleshooting and remediation of performance and other issues that arise may be limited and could be deemed out of scope for the service at Secureworks' discretion.

9.9.1.2 Endpoint Sensor Operating Systems Not Supported

Red Cloak is known not to run on the following operating system versions:

- Windows ME
- Windows 2000
- Windows 98
- Windows 95
- Windows NT

Any other Windows version not listed in the supported list above, to include non-English language packs. Red Cloak is also known not to run on operating systems utilizing Itanium processors.