

RESOLUTION NO. 42-21
CITY OF CENTERVILLE, OHIO

SPONSORED BY COUNCILMEMBER Bill Serr ON
THE 5th DAY OF April, 2021.

**RESOLUTION AUTHORIZING THE CITY MANAGER TO ENTER
INTO AN AGREEMENT FOR MANAGED SWITCHES AND
INSTALLATION WITH SECURE CYBER DEFENSE.**

WHEREAS, the City of Centerville has been improving and updating its information technology (IT) systems in the City; and

WHEREAS, the City of Centerville has been desirous of obtaining professional managed services of network switches; and

WHEREAS, Secure Cyber Defense provides such managed cybersecurity Services, including hardware products; and

WHEREAS, the Ohio Revised Code recognizes exceptions to competitive bidding for professional services and for purchases related to IT that are proprietary or limited to a sole source; and

WHEREAS, the City desires to utilize Secure Cyber Defense for assistance in the carrying out other services, for the City with regards to all of the City's IT requirements; and

WHEREAS, Secure Cyber Defense has unique knowledge of such Technological Services, Professional Services, Products and Software; and has a demonstrated ability to assist in accomplishing the objectives of the City.

**NOW, THEREFORE, BE IT RESOLVED BY THE COUNCIL OF
THE CITY OF CENTERVILLE, MONTGOMERY COUNTY, OHIO, AS
FOLLOWS:**

Section 1. The City hereby agrees to authorize the City Manager to enter into an Agreement with Secure Cyber Defense, a copy of the Agreement attached hereto as Exhibit "A" and incorporated herein on behalf of the City of Centerville.

Section 2. This Resolution shall be in full force and effect at the earliest date allowed by law.

PASSED THIS 5th day of April, 2021.



Mayor of the City of Centerville, Ohio

ATTEST:



Clerk of Council
City of Centerville, Ohio

CERTIFICATE

The undersigned, Clerk of Council of the City of Centerville, Ohio, hereby certifies the foregoing to be a true and correct copy of Resolution No. 42-21, passed by the Council of the City of Centerville, Ohio on the 5th day of April, 2021.



Clerk of Council

Approved as to form, consistency
with existing ordinances, the
charter & constitutional provisions
Department of Law
Scott A. Liberman
Municipal Attorney



SECURECYBER
D E F E N S E

We have prepared a quote for you

Managed Switches & Installation (Rental)

Quote # 001015
Version 1

Prepared for:

City Of Centerville

Larry Rover
lrover@centervilleohio.gov



Hardware & Support

Description	Recurring	Price	Qty	Ext. Recurring	Ext. Price
FortiSwitch-448E-FPOE & Support (Rental) FortiSwitch-448E-FPOE Hardware with FortiSwitch-448E-FPOE FortiCare ** FS-448E-FPOE 24x7 Support (Monthly Recurring - 5 Year Term)	\$120.00	\$0.00	15	\$1,800.00	\$0.00
FortiSwitch-1024D & Support (Rental) Layer 2/3 FortiGate switch controller compatible switch with 24 x SFP / SFP+ slots GE/10 GE capable with dual AC power supplies with FortiCare FS-1024D 24x7 Support (Monthly Recurring - 5 Year Term)	\$275.00	\$0.00	2	\$550.00	\$0.00
SFP+ MMF Transceiver SFP+ MMF Transceiver, SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots (One-Time Cost)	\$0.00	\$150.00	50	\$0.00	\$7,500.00

Subtotal: **\$2,350.00**

Subtotal: **\$7,500.00**

Configuration & Installation

Description	Price	Qty	Ext. Price
Cyber Security Consulting Services Time and Materials Cyber Security Consulting - Configuration and Installation of FortiSwitches. (One-Time Cost)	\$250.00	144	\$36,000.00

Subtotal: **\$36,000.00**



Managed Services

Description	Recurring	Qty	Ext. Recurring
SCD-MGD-FortiSwitch - 17 Switches Managed FortiSwitch - 17 Switches - Includes health monitoring, port level security configuration, moves adds and changes. (Monthly Recurring Cost) <hr/> For any additional switches over 17, cost is standard SCD rate of \$250.00 per switch.	\$150.00	17	\$2,550.00

Subtotal: **\$2,550.00**

Invoicing & Payment Terms

Description	Qty
Customer will be invoiced upon approval of this quote. Payment is due within thirty (30) days from receipt of invoice.	

Managed Switches & Installation (Rental)



Prepared by:

Secure Cyber Defense

Shawn Waldman
(937) 388-4405
swaldman@secdef.com

Prepared for:

City Of Centerville

100 W. Spring Valley Rd.
Centerville, OH 45458
Larry Rover
(937) 428-4722
lrover@centervilleohio.gov

Quote Information:

Quote #: 001015

Version: 1
Delivery Date: 03/25/2021
Expiration Date: 04/23/2021

Quote Summary


Description	Amount
Hardware & Support	\$7,500.00
Configuration & Installation	\$36,000.00
Total: \$43,500.00	

Expenses Summary

Description	Amount
Hardware & Support	\$2,350.00
Managed Services	\$2,550.00
Total: \$4,900.00	

Taxes, shipping, handling and other fees may apply. We reserve the right to cancel orders arising from pricing or other errors. All managed service contracts are a minimum of 1 year unless otherwise noted.

Secure Cyber Defense

Signature: 
Name: Shawn Waldman
Title: CEO
Date: 03/25/2021

City Of Centerville

Signature: _____
Name: Wayne Davis, City Manager
Date: _____

APPROVED AS TO FORM:

Scott A. Liberman, Municipal Attorney



STATEMENT OF WORK

City of Centerville, Ohio
Managed Switches (Rental) – 5 Year Term

This Statement of Work (“Statement of Work” or “SOW”) is entered into and is effective the date of execution, as set forth below (“Effective Date”), by and between Secure Cyber Defense, LLC (“SCD”) and City of Centerville, Ohio (“Customer”). The Appendix(es) to this SOW, if any, shall be deemed to be a part hereof. This SOW is incorporated into and governed by the most recent Master Services Agreement separately executed by and between the parties.

Engagement Resources

The following is a list of contacts for SCD. For questions/requests regarding the implementation of equipment and/or services, please reach out to the Project Manager. For anything other, please contact the corresponding department, as follows:

Role	Phone	Email
Account Manager	937-388-4405, Opt. 3	sales@secdef.com
Accounting	937-388-4405, Opt. 2	accounting@secdef.com
Compliance	937-388-4405, Opt. 3	compliance@secdef.com
Project Manager	937-388-4405, Opt. 1	sgentry@secdef.com
Technical Implementation Lead	937-388-4405, Opt. 1	scdsupport@secdef.com
CIC Service Manager	937-388-4405, Opt. 1	

Implementation/Decommission

The following sections are used to describe the implementation of new or modified services as well as describe any services or components that are being removed/decommissioned, if applicable.

Scope/Deliverables

FortiSwitches

- Unbox FortiSwitches, rack and cable devices
- Installation and configuration 17 FortiSwitches (2 FortiSwitch 1024Ds and 15 FortiSwitch 448E-FPOEs), as listed in Appendix A
- Centralized configuration and management of FortiSwitches via the FortiGates
- Configure 802.1x Dynamic VLAN Assignment(s)
- Creation of new network topology with a redundant core and access layer (access layer redundancy pending fiber connectivity decision(s))
- Migration of existing devices to new switches

Customer Requirements

- Customer will provide access to facility and secure locations within the facility, as needed, during and/or after business hours, in order for SCD engineers to perform onsite work outlined above in this SOW.
- Customer will provide required power and space to install the device.
- Customer will provide any and all network cables, required for installation of the FortiSwitches and/or connections between devices will be provided by Customer
- Customer will provide any and all fiber patch cables required for the SFPs

- Define network devices and their VLANs, based on a network inventory report provided during the course of the project.
- Based on best practices, SCD recommends Customer purchase new network cables to avoid potential issues with existing cabling.

Location

For this engagement, SCD will perform work both onsite as well as remotely. SCD will coordinate and schedule onsite work with the Customer. Travel time, and related travel expenses, for each SCD engineer traveling to and from Customer's installation site will apply and are calculated and included in this SOW.

Managed FortiSwitches

- Includes health monitoring, port level security configuration
- Conduct reasonable moves, adds, changes as requested by the Customer (via Support Ticket). Reasonable requests are minor additions/modifications based on the Customer's current network architecture. Requests for configurations and/or modifications resulting from network architectural changes and/or newly introduced services/solutions are not included in the scope of this SOW and are considered "new work." "New work" is billable and such requests will be quoted for Customer approval.
- Conduct reasonable system configuration and/or modifications, for the purpose of troubleshooting or data collection.

Other Customer Requirements

SCD requires that ALL changes to the network or environment be reported and reviewed before implementation for their impact to SCD's security services, including, but not limited to, the addition/removal of devices, which may be subject to additional per device/per license costs, if applicable.

SCD shall not be liable for any changes to the network or environment that have not been communicated and approved by SCD. This could and would include changes to the Customer's firewall and/or other contractor services not under SCD control.

SCD will log changes into the SCD ticket system and said entries will become an official record of change.

Customer acknowledges that a failure to properly communicate any change to or/or within the Customer's network could result in a security breach or incident. SCD requires the opportunity to review any change to determine if any services provided by SCD must be adjusted to accommodate the change.

Changes should be submitted via email to scdsupport@secdef.com.

Project Management

A dedicated Project Manager will be assigned for this engagement, if appropriate. All correspondence, scheduling, information, or issues should be directed to the Project Manager via our project management system. Following approval of this quote and SOW, the assigned Project Manager will reach out and provide you with contact and project ticket information for this engagement.

Project Timeline

The Project Manager will contact all listed resources and schedule a project kickoff call. The purpose of this call is to identify required resources, discuss timeline for equipment delivery, configuration, and installation, as is applicable for this engagement. For the services which you have engaged SCD to perform, estimated timelines for performance of work through to completion may be included in the Scope/Deliverables above. To all extent possible, these estimated timelines will be followed, unless otherwise specified and agreed upon between SCD and Customer. The customer acknowledges that timely access to personnel, equipment, and software is crucial to SCD in completing this SOW.

HWaaS (Hardware Rental)

Hardware-as-a-Service (HWaaS) allows for Customer to, in effect, rent equipment to keep capital expenditures to a minimum. As a result of the agreement between SCD and Fortinet, the equipment will be titled and owned by SCD.

At the end of the five (5) year rental, Customer can continue to rent the device. Device rental will automatically renew for a one (1) year period unless Customer provides written notice of intent to terminate ninety (90) days prior to the termination date of this SOW (12 months from the date of approval/execution hereof). Written notice shall be served by personal delivery or by registered or certified mail, postage prepared, return receipt requested, and addressed to:

Secure Cyber Defense,
Attention: Shawn Waldman
1390 Vanguard Boulevard
Miamisburg, OH 45342

If Customer terminates, the device must be safely and securely returned to SCD within thirty (30) days of the termination date via shipping delivery method with tracking and signature required, at Customer's expense, and addressed to Secure Cyber Defense, Attention: Shawn Waldman, 1390 Vanguard Boulevard, Miamisburg, OH 45342. Customer will provide SCD the tracking information. Under no circumstances should Customer remove the device and/or return the device without notice and acknowledgement by SCD.

At renewal, if device is at End-of-Life and can no longer be supported, SCD will provide equivalent hardware at no additional charge. SCD assumes all hardware support for HWaaS equipment.

SaaS (Software Rental)

If applicable to this engagement, Software-as-a-Service (SaaS) allows for Customer to, in effect, rent solutions/services to keep capital expenditures to a minimum. As a result of the agreement between SCD and solution/service vendor(s), the software/licensing is registered to SCD on behalf of the customer.

At the end of the one (1) year term of this SOW, Customer can continue to utilize the SaaS solution/service. SaaS solutions/services will automatically renew for a one (1) year period unless Customer provides written notice of intent to terminate the solution/service ninety (90) days prior to the termination date of this SOW (12 months from the date of approval/execution hereof). Written notice shall be served by personal delivery or by registered or certified mail, postage prepared, return receipt requested, and addressed to:

Secure Cyber Defense
Attention: Shawn Waldman
1390 Vanguard Boulevard
Miamisburg, OH 45342

If Customer terminates, the SaaS solution/service will be decommissioned at the end of the SOW term. Customers will be responsible for the removal of the solution/service from servers/endpoints.

Location

SCD will perform work from/at the location(s) specified in the Scope/Deliverables above. If not specified, the work will be performed remotely. When travel is required, Customer will be invoiced for travel time and all costs associated with out-of-pocket expenses including, without limitation, meals, lodging, transportation, mileage, and any other applicable business expenses. Such costs will be itemized and invoiced separately.

Work Hours

Unless otherwise specified in the Scope/Deliverables above, the working hours that apply to this SOW are Monday through Friday from 8am Eastern to 5pm Eastern. It is understood that work after-hours may need to occur for the implementation (Consulting) portion of this SOW (if applicable). For the services and MDR/Monitoring/Alerting portions of this agreement, the hours are 24/7/365.

Miscellaneous

Any proposed addition to the agreement should be submitted in writing via email to sales@secdef.com.

Firmware & Support Services Renewals

If applicable, Purchased Equipment requires that updates to firmware, support services (such as IPS definitions) be licensed and applied to an individual asset. These services will be included at the time of purchase; however, they must be kept up to date and cannot expire for SCD to provide services.

Firmware and support services will automatically renew ninety (90) days prior to expiration and cannot be cancelled if SCD is provides Managed Services for the device. A notice of renewal and cost will be sent to the Customer.

Digital Forensics Services

Secure Cyber Defense will investigate and respond to alarms/alerts and/or cyber threats for the services/solutions which the Customer has subscribed to. If, during investigation of an alarm/alert and/or cyber threat, SCD believes that a compromise has occurred giving rise to a recommendation to the Customer for Digital Forensics and/or if Customer makes a request for Digital Forensics, those services are NOT included in this SOW. The fees for forensic review will be calculated and quoted separately to the Customer on a per incident basis. SCD encourages all our Customers to obtain retainer services from SCD for these types of situations.

Information Security

Secure Cyber Defense’s obligations with respect to Information Security are set forth in Appendix C below.

Term

The term of this SOW shall begin on the effective date hereof and is valid for 12 months. This SOW will automatically renew for an additional 12 months on each anniversary date thereafter unless Customer provides written notice of intent to terminate ninety (90) days prior to the 12-month anniversary/termination date (12 months from the date of execution or renewal hereof). Notwithstanding the foregoing, SCD may not terminate any licenses for which Customer has already paid for until the end of the license term.

Annual Price Increase

Annual price increases can occur for services, maintenance, licensing, HWaaS and/or SaaS, as determined by SCD. Increases may be up to, but will not exceed, a five (5%) percent annual increase per item. Anything over 5% will be submitted to the Customer for review and approval. Price increases, if applicable, will become effective on the 12-month anniversary of the effective date of this SOW (renewal date). Price changes will be reflected accordingly, beginning with the first invoice following the renewal. A Notice of Change will be sent to the Customer if an increase occurs for the applicable item.

Schedule of Services and Fees

Monthly Managed Cyber Security Services			
Description	Qty	Unit Price	Fee
FortiSwitch-448E-FPOE Hardware (Rental) with FortiSwitch-448E-FPOE FortiCare ** FS-448E-FPOE 24x7 Support (Monthly Recurring - 5 Year Term)	15	\$120.00	\$1,800.00
FortiSwitch-1024D Hardware (Rental) Layer 2/3 FortiGate switch controller compatible switch with 24 x SFP / SFP+ slots GE/10 GE capable with dual AC power supplies with FortiCare FS-1024D 24x7 Support (Monthly Recurring - 5 Year Term)	2	\$275.00	\$550.00
SFP+ MMF Transceiver, SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots (One-Time Cost)	50	\$150.00	\$7,550.00
Time and Materials Cyber Security Consulting – Configuration & Installation of Switches (One-Time Cost)	144	250.00	\$36,000.00

Managed FortiSwitches - 17 Switches - Includes health monitoring, port level security configuration, moves adds and changes. (Monthly Recurring Cost)	17	\$150.00	\$2,550.00
For any additional switches, cost is standard SCD rate of \$250.00 per switch.			
Total One-Time Costs:			\$36,000.00
Total Hardware Costs:			\$7,550.00
Total Monthly Recurring Cost (FortiSwitch Rental and Managed Services):			\$4,900.00
Invoicing & Payment Terms:			
Customer will be invoiced upon approval of this quote for Total One-Time and Total Hardware Costs. Payment is due within thirty (30) days from receipt of invoice.			
Customer will be invoiced for Total Monthly Recurring Cost for the hardware rental portion of this quote/SOW the first month following approval of this SOW, for the five (5) year term. Customer will be invoiced for the Managed Services portion of the Total Monthly Recurring Cost once the first device is actively being monitored.			

Secure Cyber Defense agrees to provide Customer with services as detailed in the Schedule of Services and Fees above. Customer agrees to pay Secure Cyber Defense the amounts listed at the bottom of the Schedule of Services and Fees titled "Total Monthly Recurring Cost", "Total Hardware Costs", and "Total One-Time Costs".

Invoices will be generated for "Total Monthly Recurring Cost" and emailed to the Billing Contact listed in Appendix B and payment is required within thirty (30) days of the invoice delivery date. The "Total Monthly Recurring Cost" for hardware rental items will commence the month following approval of this SOW, for the 5-year term of the hardware rental. Invoicing for Managed Services will commence once the first device is actively being monitored. Notwithstanding the foregoing, if Customer is not responsive to SCD's requests for a period of thirty (30) days or more, SCD shall have the right to commence invoicing the "Total Monthly Recurring Cost" amount, even though the SOW is not complete.

"Total Hardware Costs" and "Total One-Time Costs," including hardware, software, licensing, Cyber Security Consulting fees and/or Setup (Project) fees, if applicable, are billed immediately upon approval of this SOW, based on the terms set forth in the Schedule of Services above and/or detailed in the Customer quote. Payment for the specified amounts is due within thirty (30) days of invoice delivery.

SCD shall have the right to periodically audit the device and/or service deployment and update pricing accordingly.

A customer is responsible for all costs associated with changes to licensing requirements associated with a device. SCD shall have the right to increase pricing based on such changes to the licensing requirements.

Out-of-Pocket Expenses

If applicable, Customer will be invoiced travel time and for all costs associated with out-of-pocket expenses including, without limitation, meals, lodging, transportation, mileage, and any other applicable business expenses. Such costs will be itemized and invoiced separately.

IN WITNESS WHEREOF, the parties hereto have caused this SOW to be effective as of the day, month and year first written below.

CITY OF CENTERVILLE, OHIO

Signature: _____
Name: Wayne S. Davis
Title: City Manager
Date: _____

APPROVED AS TO FORM:

Scott A. Liberman, Municipal Attorney

SECURE CYBER DEFENSE, LLC

Signature: _____
Name: Shawn Waldman
Title: Chief Executive Officer
Date: _____

Appendix B – Approved Contacts

NAME	TITLE	EMAIL	PHONE	TYPE
Larry Rover	IT Director	lrover@centervilleohio.gov	937-428-4722	Technical POC
Larry Rover	IT Director	lrover@centervilleohio.gov	937-428-4722	Billing POC
Larry Rover	IT Director	lrover@centervilleohio.gov	937-428-4722	Service POC

Appendix C – Information Security

Definitions

“Discover,” with respect to a Security Incident, means knowledge by any member of SCD’s workforce — other than the person responsible for the Security Incident — that the Security Incident has occurred.

“Sensitive Personal Information” means any non-public, individually identifiable information created or received by SCD on Customer’s behalf or received by SCD from Customer — whether in paper, electronic or other form. Sensitive Personal Information includes, but is not limited to, contact information; Social Security number; credit card, debit card, or other financial account number with or without any required security code, access code, or password.

“Required by Law” means that a statute, regulation, court order, or legal process, enforceable in a court of law, mandates the conduct.

“Security Incident” means the unauthorized access to, or use, disclosure, acquisition, modification, or destruction of, Unsecured Sensitive Personal Information when that Unsecured Sensitive Personal Information is held by SCD or its agents or subcontractors.

“Unsecured Sensitive Personal Information” means all Sensitive Personal Information except (1) such information in electronic form that is encrypted in accordance with standards established by the National Institute of Standards and Technology or other industry, standard-setting body, or (2) such information in paper form that has been shredded, burned, or otherwise rendered irrecoverable.

SCD’s Responsibilities with Respect to Sensitive Personal Information

Permitted Use and Disclosure of Sensitive Personal Information. SCD agrees to receive, create, maintain, use, and disclose Sensitive Personal Information only (1) to the extent necessary to provide services to Customer pursuant to the terms of the Customer Services Agreement/Statement of Work, or (2) as Required by Law.

Confidentiality of Sensitive Personal Information. SCD will not disclose Sensitive Personal Information to any third party except as permitted by this Agreement. Disclosure of Sensitive Personal Information to employees of SCD will be limited to those who have a need to know such information to carry out SCD obligations under this Agreement. The confidentiality and other obligations set forth in this Section will continue indefinitely for as long as the Sensitive Personal Information remains in SCD’s possession.

SCD’s Safeguards for Sensitive Personal Information. SCD shall maintain reasonable and appropriate measures to protect against foreseeable risks to the security, confidentiality, and integrity of Sensitive Personal Information.

Reporting Security Incidents. SCD shall promptly report to Customer any Security Incident discovered by SCD, regardless of whether the Security Incident results from the actions of SCD or its agents or subcontractors.

Data Ownership. SCD acknowledges that SCD has no ownership rights with respect to any Sensitive Personal Information.

SCD Agents and Subcontractors. SCD shall obtain reasonable assurances, in writing, from any agent or subcontractor to whom SCD discloses Sensitive Personal Information. Such assurances by the agent or subcontractor will include at least the following: that the agent or subcontractor will comply with the same restrictions and conditions on the use and disclosure of Sensitive Personal Information that this Agreement imposes on SCD; (ii) will implement reasonable and appropriate physical, technical and administrative safeguards to protect Sensitive Personal Information; and (iii) will

notify SCD of any breach of the confidentiality of the Sensitive Personal Information or of any impermissible use or disclosure of the Sensitive Personal Information.

Demands to Produce Sensitive Personal Information Directed To SCD. To the extent permitted by law, SCD shall (1) notify Customer of any judicial or administrative order, subpoena, civil discovery request or other legal process requiring or requesting that SCD produce Sensitive Personal Information, and (2) permit Customer adequate time to exercise its legal options to prohibit or limit disclosure of Sensitive Personal Information before SCD produces any Sensitive Personal Information.

Destruction of Sensitive Personal Information. Promptly after termination of the Customer Services Agreement/Statement of Work, SCD shall, at Customer's written direction, return, destroy, or transfer to a third party designated by an authorized Customer representative in writing, all Sensitive Personal Information.

SCD Retention of Sensitive Personal Information. If after termination of the Customer Services Agreement/Statement of Work, SCD promptly delivers to Customer written notice explaining the conditions which make return, destruction, or transfer of Sensitive Personal Information as required by paragraph I, above, infeasible, then Customer may excuse SCD from complying, in whole or in part, with paragraph I, above. If Customer does excuse compliance with paragraph I, in whole or in part, SCD agrees that, with respect to the Sensitive Personal Information for which compliance with paragraph I has been excused, SCD shall extend the protections of this Agreement to the retained Sensitive Personal Information and limit further uses and disclosures of the retained Sensitive Personal Information to those purposes which make return or destruction infeasible, for as long as SCD maintains such Sensitive Personal Information.

Survival. SCD's obligations and duties under this Agreement with respect to Sensitive Personal Information received by SCD or created by SCD while performing under the Customer Services Agreement/Statement of Work, or on SCD's behalf, shall survive the termination of the Customer Services Agreement/Statement of Work and of this Addendum and shall continue for as long as that Sensitive Personal Information remains in the possession of SCD or of its agents or subcontractors.

No Third-Party Beneficiaries. No third party shall be considered a third-party beneficiary under this Addendum, nor shall any third party have any rights because of this Addendum.

Construction; Effect of Addendum. In the event of a conflict between the provisions of this Addendum and the Agreement, the provisions of this Addendum will prevail regarding Sensitive Personal Information.

SCHEDULE OF SUPPORT SERVICES

Secure Cyber Defense Support/Helpdesk

This Schedule of Secure Cyber Defense Support Services provides the basis for managing helpdesk and support provided by Secure Cyber Defense, LLC (SCD), along with our commitment to providing valued and timely services to our Customers. This schedule establishes a shared set of expectations regarding the operation and support of Secure Cyber Defense services provided to your organization. SCD does not guarantee or warrant its service until after completing a full investigation of the problem. All terms and conditions of SCD's Master Service Agreement apply.

For any questions regarding this Schedule of Support Services, please consult with your Sales Engineer, or contact SCD at 937.388.4405, sales@secdef.com.

Hours of Operation Support Contact Information	
General Business Hours	Monday – Friday, 8:00 a.m. to 5:00 p.m.
Critical Urgent	Monday – Sunday, 24/7
Contact SCD Support:	scdsupport@secdef.com 937.388.4405, Opt. 1

Problem Management - Response times are based on the General Business Hours, defined below, except for calls designated as Priority 1 or Priority 2. For after hours (before 8 a.m. after 5 p.m.) Priority 1 or 2 calls, customer will contact SCD by phone and a Cyber Security Analyst will respond as outlined below with follow-up attempted within 15 minutes.				
IMPACT LEVEL	BUSINESS IMPACT	OPERATIONAL HOURS	INITIAL RESPONSE TIME	RESOLUTION TIME*
PRIORITY 1* Critical Phone Only	<ul style="list-style-type: none"> Severe impact to organization Total loss of services Work around not available 	24/7	1 hour	6 hours**
PRIORITY 2* Urgent Phone Only	<ul style="list-style-type: none"> High impact to organization Degraded or partial loss of services Work around may/may not be available 	24/7	2 hours	12 hours**
PRIORITY 3 Medium	<ul style="list-style-type: none"> Moderate impact to organization Services not functioning properly Work around may/may not be available 	M-F 8 a.m. - 5 p.m.	4 hours <small>Ticket assigned and scheduled w/in 4 business hours.</small>	2 business days*
PRIORITY 4 Low	<ul style="list-style-type: none"> Minimal impact to services Does not impede operations/function Customer experience able to be improved 	M-F 8 a.m. - 5 p.m.	6 hours <small>Ticket assigned and scheduled w/in 6 business hours</small>	3 business days*
PRIORITY 5 Change	<ul style="list-style-type: none"> Change and/or request related to Services currently provided by SCD 	M-F 8 a.m. - 5 p.m.	8 hours <small>Ticket assigned and scheduled w/in 8 business hours.</small>	5 business days*
PRIORITY 6 New Request	<ul style="list-style-type: none"> Request for new services not currently provided by SCD 	M-F 8 a.m. - 5 p.m.	Transfer to Sales 2 business days	TBD
PRIORITY 7 Question	<ul style="list-style-type: none"> Non-support questions regarding existing and/or new services 	M-F 8 a.m. - 5 p.m.	8 hours <small>Ticket assigned and scheduled w/in 8 business hours.</small>	TBD

*Priority de-escalation of a helpdesk ticket may occur in certain circumstances. These include, but are not limited to: 1) the Cyber Security Analyst performs support tasks and resolves the urgent portion of a helpdesk support ticket - the ticket will be de-escalated to the appropriate priority level for any remaining tasks to be performed; and (2) if an issue is determined to be that of a third-party solution provider (and not a Secure Cyber Defense solution), such as Internet services are down - the helpdesk ticket will be de-escalated to the appropriate level for any remaining tasks to be performed.

**Resolution times are set based on our commitment to provide timely support. Resolution times may, however, be exceeded due to Customer availability, vendor availability, technical complexity, and/or other issues. Throughout the support ticket, analysts will maintain communication including, but not limited to status updates, progress made, and resolution(s) implemented.

CONTACTING SECURE CYBER DEFENSE SUPPORT		
IMPACT LEVEL	CONTACT SUPPORT INSTRUCTIONS	EXAMPLES OF PRIORITY RELATED ISSUES (include, but not limited to)
PRIORITY 1 Critical	<ul style="list-style-type: none"> • CONTACT SECURE CYBER DEFENSE BY PHONE – 937.388.4405 ➤ Dispatcher or after-hours on-call Cyber Security Analyst will create the ticket and commence investigation. 	<ul style="list-style-type: none"> • Organization Interruption of Service • Suspected External Security Incident • Suspected Internal Security Incident • SCD Security Device/Core Service Not Operational, i.e., Firewall
PRIORITY 2 Urgent	<ul style="list-style-type: none"> • CONTACT SECURE CYBER DEFENSE BY PHONE – 937.388.4405 ➤ Dispatcher or after-hours on-call Cyber Security Analyst will create the ticket and commence investigation. 	<ul style="list-style-type: none"> • Department/Group Interruption of Service • Suspected External Security Incident • Suspected Internal Security Incident • SCD Security Device/Core Service Not Operational, i.e., Firewall
PRIORITY 3 Medium	<ul style="list-style-type: none"> • Customer Portal/Support Page • Submit Ticket online for Support. ➤ Ticket will be assigned and scheduled ➤ Customer will receive notification within the initial response time-period. 	<ul style="list-style-type: none"> • Virus/Malware Infection • Email Issue • Unauthorized Access • White/Blacklist additions/exceptions • VPN Access • Increased Server/Service Activity
PRIORITY 4 Low	<ul style="list-style-type: none"> • Customer Portal/Support Page • Submit Ticket online for Support. ➤ Ticket will be assigned and scheduled ➤ Customer will receive notification within the initial response time-period. 	<ul style="list-style-type: none"> • Email Trace (FortiMail Users) • SCD Service Install Issues • SCD Service Update Issues • False Alarms • Password Change
PRIORITY 5 Change	<ul style="list-style-type: none"> • Customer Portal/Support Page • Submit Ticket online for Support. ➤ Ticket will be assigned and scheduled ➤ Customer will receive notification within the initial response time-period. 	<ul style="list-style-type: none"> • Additional Licensing for any SCD Product • Additional FortiTokens Request • Add New Users to Security Awareness Training
PRIORITY 6 New Request	<ul style="list-style-type: none"> • Customer Portal/Support Page • Submit Ticket online for Support. ➤ Ticket will be assigned and scheduled ➤ Customer will receive notification within the initial response time-period. 	<ul style="list-style-type: none"> • Addition of New Service/Product - not currently provided under existing Customer contract
PRIORITY 7 Question	<ul style="list-style-type: none"> • Customer Portal/Support Page • Submit Ticket online for Support. ➤ Ticket will be assigned and scheduled ➤ Customer will receive notification within the initial response time-period. 	<ul style="list-style-type: none"> • For non-support questions related to existing and/or new cyber security services • General questions regarding services • Billing questions



SECURE CYBER DEFENSE – an Advanced Fortinet Partner

The Secure Cyber Defense Story

From the start, Secure Cyber Defense saw a need for an MSSP totally dedicated to cybersecurity.

Today, Secure Cyber Defense is focused on providing the most current threat intelligence, incident response, and data protection services. Utilizing a blend of technology, a dedicated 24/7/365 cyber intelligence center, and a team of certified cyber analysts, we provide customized solutions to address the ever-changing threat landscape.

24/7/365 Cyber Intelligence Center at Your Service

Our cyber intelligence center sets itself apart by taking in and analyzing multiple intelligence feeds from federal and local law enforcement and weather data systems to further inform our proprietary threat intelligence database and managed response playbooks. Consider us your always-on threat-detection and response service.

We excel working with clients in:

- Manufacturing
- Education (K-12 and Higher Ed)
- Financial Services
- Healthcare
- Government (State & Local)
- Defense and Aerospace
- General Business



Fortinet Supported Products

FortiGate
FortiMail
FortiEDR
FortiAnalyzer
FortiSIEM
FortiSOAR
FortiSwitch
FortiAP
FortiManager
SD-WAN

Value-Added Services

24/7/365 Threat Monitoring
& Response
SOC Service & Response
Digital Forensics/Incident
Response
Incident Response Planning
& Triage
Compliance Consulting (DFARS
& CMMC)
Cybersecurity as a Service
Offerings





The Secure Cyber Defense Difference

Our goal is to understand our client's business and goals first so we can develop solutions that deliver the data security solution that's right for them. Our mission is not to be just another MSSP which is why we also offer:

- A fully staffed 24/7/365 Cyber Intelligence Center
- Integration of federal and local law enforcement threat intelligence feeds
- Incident Response and Digital Forensic teams
- Certified incident response and planning analysts

The importance of an experienced team

We understand data security means trusting us with your most sensitive information. We take this role seriously by training and hiring an experienced team

- SANS GCFA Certified Analysts
- Fortinet NSE 4 Certifications
- Former military and federal and local law enforcement officers

Our Customer-First Approach

While we may be cybersecurity experts, we recognize that building a trusting relationship is important, particularly when the unexpected happens. This means offering weekly insights on the latest threats and educating our customer on new technology and security approaches. That's why we believe being **Cyber Aware means being Cyber Prepared.**



SECURECYBER
D E F E N S E

Contact us at
937-388-4405 or
info@secdef.com

Twitter: @secdefllc

LinkedIn:
secure-cyber-defense-llc

Youtube: **Secure Cyber
Defense**