GENERAL SERVICES ADMINISTRATION  
FEDERAL SUPPLY SERVICE  
AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST  

On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order are available through GSA Advantage!, a menu-driven database system. The Internet address for GSA Advantage! is: http://www.gsaadvantage.gov

WORLDWIDE FEDERAL SUPPLY SCHEDULE CONTRACT  
SCHEDULE TITLE: MULTIPLE AWARD SCHEDULE  
LARGE CATEGORY F – INFORMATION TECHNOLOGY  

FSC GROUP: 70  
CONTRACT NUMBER:  
GS-35F-0154X  

PERIOD COVERED BY CONTRACT:  
December 27, 2010 – December 26, 2020  

APTEC, LLC  
301 E Kennedy Blvd, Suite 1750  
Tampa, FL 33602  
Phone: 813-402-1208  
Fax: 813-436-5283  
www.aptecllc.com  

Contractor’s Administration Source:  
Aaron Perry  
aaron@aptecllc.com  

General Services Administration  
Management Services Center Acquisition Division  
Modification # PA-0015  
Dated: 2/13/2020  

Business Size:  
Small Business  

DUNS: 825342202  

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at http://www.fss.gsa.gov.
1a. **TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs)**

- **SIN 611420**: Information Technology Training
- **SIN 54151S**: Information Technology Professional Services
- **OLM**: Order Level Materials

1b. **LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN**: See attached GSA Pricelist

1c. **HOURLY RATES (Services Only)**: See attached GSA pricelist

**MAXIMUM ORDER**:

- **SIN 611420**: $250,000
- **SIN 54151S**: $500,000

*If the “best value” selection places your order over this Maximum Order identified in this catalog/pricelist, you have an opportunity to obtain a better schedule contract price. Before placing your order, contact the aforementioned contractor for a better price. The contractor may (1) offer a new price for this requirement; (2) offer the lowest price available under this contract; or (3) decline the order. A delivery order that exceeds the maximum order may be placed under the Schedule contract in accordance with FAR 8.404*

**MIMINUM ORDER**: $100

**GEOGRAPHIC COVERAGE**: 48 Contiguous States including Washington, DC, Alaska, Hawaii, and Puerto Rico

**POINT(S) OF PRODUCTION**:

- 201 E Kennedy Blvd, Suite 1750
- Tampa, FL 33602

**DISCOUNT FROM LIST PRICES**: Refer to attached Pricelist

**QUANTITY DISCOUNT(S)**:

- **SIN 611420**: None
- **SIN 54151S**: 1% for a single task order at or above $500,000
- **OLM**: None

**PROMPT PAYMENT TERMS**: 0% net 30 days from receipt of invoice or date of acceptance, whichever is later
9a. Government purchase cards *are accepted* at or below the micro-purchase threshold

9b. Government purchase cards *are not accepted* above the micro-purchase threshold

10. **FOREIGN ITEMS:** N/A

11a. **TIME OF DELIVERY:** The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below:

   - SIN 611420: To be negotiated at the task order level
   - SIN 54151S: To be negotiated at the task order level
   - OLM: To be negotiated at the task order level

11b. **EXPEDITED DELIVERY:** To be negotiated at the task order level

11c. **OVERNIGHT AND 2-DAY DELIVERY:** To be negotiated at the task order level

11d. **URGENT REQUIREMENTS:** To be negotiated at the task order level

12. **FOB POINT:** Destination

13a. **ORDERING ADDRESS:**
201 E Kennedy Blvd
Suite 1750
Tampa, FL 33602

13b. **ORDERING PROCEDURES:** For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA’s) are found in FAR 8.405-3

14. **PAYMENT ADDRESS:**
Same as Contractor address

15. **WARRANTY PROVISION:** N/A

16. **EXPORT PACKING CHARGES:** N/A

17. **TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE:** Accepted at or below the micro-purchase threshold

18. **TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR (if applicable):** N/A

19. **TERMS AND CONDITIONS OF INSTALLATION (IF APPLICABLE):** N/A
20. TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE): N/A

20a. TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE): N/A

21. LIST OF SERVICE AND DISTRIBUTION POINTS (IF APPLICABLE): N/A

22. LIST OF PARTICIPATING DEALERS (IF APPLICABLE): N/A

23. PREVENTIVE MAINTENANCE (IF APPLICABLE): N/A

24a. SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants): N/A

24b. Section 508 Compliance for EIT: As applicable

25. DUNS NUMBER: 825342202

26. NOTIFICATION REGARDING REGISTRATION IN SYSTEM FOR AWARD MANAGEMENT (SAM) DATABASE: Active
1. **SCOPE**

   a. The Contractor shall provide training courses normally available to commercial customers, which will permit ordering activity users to make full, efficient use of general purpose commercial IT products. Training is restricted to training courses for those products within the scope of this solicitation.

   b. The Contractor shall provide training at the Contractor's facility and/or at the ordering activity's location, as agreed to by the Contractor and the ordering activity.

2. **ORDER**

   Written orders, EDI orders (GSA Advantage! and FACNET), credit card orders, and orders placed under blanket purchase agreements (BPAs) shall be the basis for the purchase of training courses in accordance with the terms of this contract. Orders shall include the student's name, course title, course date and time, and contracted dollar amount of the course.

3. **TIME OF DELIVERY**

   The Contractor shall conduct training on the date (time, day, month, and year) agreed to by the Contractor and the ordering activity.

4. **CANCELLATION AND RESCHEDULING**

   a. The ordering activity will notify the Contractor at least seventy-two (72) hours before the scheduled training date, if a student will be unable to attend. The Contractor will then permit the ordering activity to either cancel the order or reschedule the training at no additional charge. In the event the training class is rescheduled, the ordering activity will modify its original training order to specify the time and date of the rescheduled training class.

   b. In the event the ordering activity fails to cancel or reschedule a training course within the time frame specified in paragraph a, above, the ordering activity will be liable for the contracted dollar amount of the training course. The Contractor agrees to permit the ordering activity to reschedule a student who fails to attend a training class within ninety (90) days from the original course date, at no additional charge.

   c. The ordering activity reserves the right to substitute one student for another up to the first day of class.
d. In the event the Contractor is unable to conduct training on the date agreed to by the Contractor and the ordering activity, the Contractor must notify the ordering activity at least seventy-two (72) hours before the scheduled training date.

5. FOLLOW-UP SUPPORT

The Contractor agrees to provide each student with unlimited telephone support or online support for a period of one (1) year from the completion of the training course. During this period, the student may contact the Contractor's instructors for refresher assistance and answers to related course curriculum questions.

6. PRICE FOR TRAINING

The price that the ordering activity will be charged will be the ordering activity training price in effect at the time of order placement, or the ordering activity price in effect at the time the training course is conducted, whichever is less.

7. INVOICES AND PAYMENT

Invoices for training shall be submitted by the Contractor after ordering activity completion of the training course. Charges for training must be paid in arrears (31 U.S.C. 3324). PROMPT PAYMENT DISCOUNT, IF APPLICABLE, SHALL BE SHOWN ON THE INVOICE.

8. FORMAT AND CONTENT OF TRAINING

a. The Contractor shall provide written materials (i.e., manuals, handbooks, texts, etc.) normally provided with course offerings, printed and copied two-sided on paper containing 30% postconsumer materials (fiber). Such documentation will become the property of the student upon completion of the training class.

b. **If applicable** For hands-on training courses, there must be a one-to-one assignment of IT equipment to students.

c. The Contractor shall provide each student with a Certificate of Training at the completion of each training course.

d. The Contractor shall provide the following information for each training course offered:
   (1) The course title and a brief description of the course content, to include the course format (e.g., lecture, discussion, hands-on training);
   (2) The length of the course;
   (3) Mandatory and desirable prerequisites for student enrollment;
   (4) The minimum and maximum number of students per class;
   (5) The locations where the course is offered;
(6) Class schedules; and
(7) Price (per student, per class (if applicable)).

e. For those courses conducted at the ordering activity’s location, instructor travel charges (if applicable), including mileage and daily living expenses (e.g., per diem charges) are governed by Pub. L. 99-234 and FAR Part 31.205-46, and are reimbursable by the ordering activity on orders placed under the Multiple Award Schedule, as applicable, in effect on the date(s) the travel is performed. Contractors cannot use GSA city pair contracts. The Industrial Funding Fee does NOT apply to travel and per diem charges.

f. For Online Training Courses, a copy of all training material must be available for electronic download by the students.

9. **“NO CHARGE” TRAINING**

The Contractor shall describe any training provided with equipment and/or software provided under this contract, free of charge, in the space provided below. **NONE**
<table>
<thead>
<tr>
<th>SIN</th>
<th>Course Title</th>
<th>Course Length</th>
<th>Course Description</th>
<th>Minimum Participants (if applicable)</th>
<th>Maximum Participants (if applicable)</th>
<th>Location (Customer or Contractor Site or Both)</th>
</tr>
</thead>
<tbody>
<tr>
<td>611420</td>
<td>Introduction to Cyber Security</td>
<td>3 Days</td>
<td>Over the past few years the world has continued to watch as breach after breach has resulted in millions of credit card and personal information records being posted on the Internet. The Internet Storm Center reports an average of over 700,000 detected intrusion attempts daily – and that's only the events they catch. There is no question that Cyber Security is a now a business priority and a prevailing global issue. The challenge lies in where to begin the daunting task of securing your infrastructure, training your end users and preparing your organization to face the year ahead. Introduction to Cyber Security is the foundational training for all users, whether management, IT, end user or programmer. Equip your team with the most up-to-date knowledge of the threats we all face and the hands-on skills to address them. With information gathered from the most trusted sources (CERT, NIST, DHS and others), this course presents an objective, complete, and cutting-edge view of our current environment as well as a vision of the near future of Cyber Security.</td>
<td>7</td>
<td>20</td>
<td>Contractor Site</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Duration</td>
<td>Description</td>
<td>Fee</td>
<td>Class</td>
<td>Both</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----</td>
<td>-------</td>
<td>------</td>
</tr>
<tr>
<td>611420</td>
<td>Understanding Operating Systems</td>
<td>5 Days</td>
<td>This class gives you a firm understanding of the latest operating systems used worldwide as well as advanced information that will help your mastery in our Malware and Exploitation courses. We start by teaching the foundational concepts of operating systems such as kernel structure, process management and resource allocation then progressively expand into other areas, using lab exercises across Windows, Linux and Solaris platforms to reinforce the concepts being introduced. After attending this course students will be fully equipped with the fundamentals of operating system elements and how they are all interconnected. This course is taught as 50% hands-on and 50% classroom instruction.</td>
<td>7</td>
<td>20</td>
<td>Both</td>
</tr>
<tr>
<td>611420</td>
<td>Live System Analysis</td>
<td>5 Days</td>
<td>Discovering exactly how an attacker has infiltrated a system can be difficult. This course teaches students how to correctly create a system baseline and then use it to detect and monitor for unwanted activities when they occur. In this course students will learn useful techniques and tools that can be employed during investigation to reveal the significant indicators of infiltration and compromise. Both Windows and Red Hat Linux Operating Systems are covered in this course. This course is taught as 70% hands-on and 30% classroom instruction.</td>
<td>7</td>
<td>20</td>
<td>Both</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Duration</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>611420</td>
<td>iOS Attack &amp; Defend</td>
<td>5 Days</td>
<td><em>Apple iOS Attack &amp; Defend provides hands-on training in the fundamentals of Software Development and Hacking for the iPhone Operating System from Apple. This course is a laboratory intensive programming course designed for students looking to gain a working knowledge in iPhone Development and Hacking. Through a combination of instructor-led examples and a series of programming assignments and challenges, students will build and enhance their practical knowledge of software development, exploitation and hacking in the iPhone Operating System. Additionally, students will learn how to deploy, execute, and test all developed programs on iPhone emulation software and iPhone hardware devices provided in the class.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>611420</td>
<td>Antdroid Attack &amp; Defend</td>
<td>5 Days</td>
<td><em>AndroidTMAttack and Defend provides an Instructor-led platform hands on course in the fundamentals of Software Development for this new Operating System from Google. This course is a laboratory intensive, programming course designed for students looking to gain a working knowledge in Android Development. Through a combination of Instructor-led examples and a series of programming assignments and challenges, the students will build and enhance their practical knowledge of software development in the Android Operating System. Additionally students will also deploy, execute, and test all developed programs on Android emulation software and Android hardware devices provided in the class.</em></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>611420</td>
<td>Behavioral Malware Analysis</td>
<td>5 Days</td>
<td>The sharp skills and attention to detail needed by both analysts and responders can only come from dedicated study and experience. In this course students will learn first-hand the impact and severity of today’s malware by executing and observing real-world samples. Students will gain the skills to set up a controlled sandbox environment and use system monitoring tools to quickly and safely analyze malware samples and their malicious effects on the system. From simple Keyloggers and packed or encrypted trojans to massive botnets, this class introduces students to a wide variety of current malware types. This class is taught as 70% hands-on and 30% classroom instruction, and culminates in a capstone examination exercise.</td>
<td>7</td>
<td>20</td>
<td>Both</td>
</tr>
<tr>
<td>611420</td>
<td>Assembly for Reverse Engineers</td>
<td>5 Days</td>
<td>Many who are employed as analysts or programmers have not had the time to learn the Assembly language - a skill that will save them precious time when effective analysis is needed most. Designed for Malware Analysts and Code Developers alike, Assembly for Reverse Engineers will equip students with the know-how to effectively read Assembly, understand statements and reverse engineer machine code back to its higher-level equivalent. Discover how a compiler transforms high-level code into machine code, learn common Assembly statements you’ll see used in the real world, and then be introduced to writing your own code during this week-long, lab-intensive course. This class is taught as 70% hands-on and 30% classroom instruction, and culminates in a capstone examination exercise.</td>
<td>7</td>
<td>20</td>
<td>Both</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Duration</td>
<td>Description</td>
<td>Fee</td>
<td>Subsidy</td>
<td>Coverage</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>611420</td>
<td>Malware Reverse Engineering</td>
<td>5 Days</td>
<td>Mastering the dynamic analysis process learned in our Basic Malware Analysis course is the first step in becoming an effective malware analyst, but dynamic analysis only reveals the non-obscured activities of a piece of malicious code. In order to understand any type of malware’s true actions and the author’s intent, the analyst must also learn the art of static analysis using debugging and disassembly techniques. During this 5-day class, students will use debuggers (including OllyDbg, x64dbg and the IDA Pro debugger) and the IDA Pro Disassembler in a controlled environment to identify exactly what a malware specimen is designed to do. Students will learn how to patch a specimen to make sections inactive or crack the program to allow full access to areas that have been hidden or encrypted by the malware developer. This class is taught as 70% hands-on and 30% classroom instruction, and culminates in a capstone examination exercise.</td>
<td>7</td>
<td>20</td>
<td>Both</td>
</tr>
<tr>
<td>611420</td>
<td>Hacking with Python</td>
<td>5 Days</td>
<td>Once you've graduated from our Introduction to Python Scripting course and venture down the path of an Elite Operator, you'll find your way to our latest programming course, Hacking With Python. The Python scripting language has been on an incredible rise as we merge scripting and object oriented programming together in today's rapid development environment. To survive as an Information Assurance Analyst today, you must have a good scripting background. This course teaches you how to use Python to build powerful scripts to push the limits of system security. Designed to be used for Gray Hat Hacking, the course will detail code that can be used to ethically hack into applications and networks to test security. This course</td>
<td>7</td>
<td>20</td>
<td>Both</td>
</tr>
</tbody>
</table>
is also designed with the Reverse Engineer in mind since automated Malware Analysis is almost essential in this chaotic network warfare world we live in. Python is quickly becoming the adopted language of choice to automate analysis tasks with IDA and OllyDbg. The world's best hackers are using Python to do their handiwork – shouldn't you?

<p>| 611420 | Hacker Methodologies for Security Professionals | 5 Days | Mainstream media coverage of hacker groups and their exploits have left the public thinking that all of cyber security is black magic. While many attacks involve some advanced networking and coding techniques, the majority of compromises are carried out by much less sophisticated attackers. The majority of these individuals have learned the process of compromising servers and networks in the same way that all of us have learned technology; by researching online. The days of creating and compiling your own exploit code are long since past. Most attackers are using “point and pwn” utilities like Armitage, Cain &amp; Able, and the Social Engineers Toolkit (SET) to cause havoc for organizations worldwide. We believes that to emulate the various cyber threat vectors, it is critical to understand what most attacks have in common: their methodology. Bringing together decades of experience in government, commercial and academic cyber security training and consulting, our instructors have developed and implemented multiple threat emulation methodologies. While methodologies change over time to account for new technologies and techniques, the concepts involved remain constant. This course provides a flexible methodology for use in emulating external and internal network intrusion threat vectors. | 7 | 20 | Both |</p>
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Duration</th>
<th>Description</th>
<th>7</th>
<th>20</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>611420</td>
<td>Network Traffic Analysis</td>
<td>5 Days</td>
<td>The preponderance of network traffic, particularly HTTP, was an expected outcome of the pivotal role that the Internet has come to play in our daily lives. The sheer volume of traffic and complexity of protocols creates a very diverse and ever-changing landscape within which the network analyst must navigate. Network Traffic Analysis will teach students to differentiate between normal and abnormal network traffic, understand how packets flow through a network and enable them to attribute conversations and actions taken over a network segment to specific hosts or users. This course focuses on research, filtering and comparative analysis to identify and attribute the different types of activity on a network. You'll learn to follow conversations across a wide range of protocols and through redirection, as well as how to develop custom filters for non-dissected protocols. After attending this course, students will be able to hone in on the key events in a traffic capture and reconstruct the event timeline. This class is taught as 70% hands-on and 30% classroom instruction, and culminates in a capstone team-based CTF challenge.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>611420</td>
<td>Python for Network Defenders</td>
<td>5 Days</td>
<td>This introductory course gives a great foundation on how to use Python. The course is focused on using Python from a security analyst perspective showing its usefulness around reverse engineering and intrusion analysis.</td>
<td>7</td>
<td>20</td>
<td>Both</td>
</tr>
<tr>
<td>611420</td>
<td>Malicious Network Traffic Analysis</td>
<td>5 Days</td>
<td>There are a tremendous number of network-based attacks occurring every day, and that number is increasing rapidly. To defend against these attacks, they must be understood at the packet level. This course teaches you how to analyze, detect, and understand the network-based attacks that have</td>
<td>7</td>
<td>20</td>
<td>Both</td>
</tr>
</tbody>
</table>
become pervasive on today’s Internet. By learning to identify statistical patterns and isolate events of interest, students will gain the skills needed to perform critical, real-time analysis in a production environment. Malicious Network Traffic Analysis employs several traffic analysis tools including Wireshark and RSA’s Netwitness Investigator alongside custom tools developed by networking experts to show you how to detect these network attacks and be prepared to handle them. This class is taught as 70% hands-on and 30% classroom instruction, and culminates in a capstone examination exercise.

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Duration</th>
<th>Seats Available</th>
<th>Class Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>611420</td>
<td>Cyber Threats Detection and Mitigation</td>
<td>5 Days</td>
<td>7</td>
<td>Both</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Duration</td>
<td>Description</td>
<td>Min.</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>611420</td>
<td>Advanced Network Traffic Analysis</td>
<td>5 Days</td>
<td>Understanding how traffic flows within your network is the first step in becoming a true network analyst, but what happened to the traffic before it arrived at your ingress router and what happens to it when it leaves your network for its destination? Advanced Network Traffic Analysis will take you above and beyond normal LAN-based operations and broaden your analyst skills with insight into global-reaching network attacks such as BGP route poisoning and redirection. Students will learn to map network topology through an understanding of network traffic such as SNMP, BGP, VOIP, VPN and more. Upon completion of this course, they will be able to discover infrastructure devices including firewalls, routers, switches and access points, and servers providing DNS, web, mail, database, file storage and authentication services (including Active Directory, LDAP, RADIUS and TACACS+). This class is taught as 70% hands-on and 30% classroom instruction, and culminates in a capstone team-based CTF challenge.</td>
<td>7</td>
</tr>
<tr>
<td>611420</td>
<td>Windows System Analysis</td>
<td>5 Days</td>
<td>Windows System Analysis teaches students how to identify abnormal activity and investigate a running system that may have been compromised. In this course, students will learn the most useful commands, tools, and techniques that can be employed during investigation to reveal the significant indicators of infiltration, as well as how to create a system baseline to be used for future analysis. This course is focused primarily on the Windows 10 operating system, using many tools and techniques that also apply to Windows 7 and recent versions of Windows Server. It also serves as a great starting point from which to learn behavioral malware analysis.</td>
<td>7</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Duration</td>
<td>Description</td>
<td>Days</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>611420</td>
<td>Linux Kernel Internals</td>
<td>5 Days</td>
<td><em>Linux Kernel Internals</em> teaches students all the fundamental requirements necessary to understand and start developing for the Linux kernel. Attendees will go deep into the internals of the Linux operating system and begin to develop kernel modules for the latest popular distributions. From kernel module implementation to memory and process management, including I/O, debugging, file systems, and kernel security mechanisms, this course is all-encompassing.</td>
<td>7</td>
</tr>
<tr>
<td>611420</td>
<td>Advanced Linux Kernel Internals</td>
<td>5 Days</td>
<td>This advanced course builds on the skills acquired in our Linux Kernel Internals class and dives deeper into the security mechanisms used in modern Linux Kernel versions. We explore the vulnerabilities that exist at the kernel level, how they can be exploited and how the kernel can be patched and extended to defeat these exploits. This expert-level course is taught as 80% hands-on and 20% classroom instruction.</td>
<td>7</td>
</tr>
<tr>
<td>611420</td>
<td>Linux &amp; C++ Reverse Engineering</td>
<td>5 Days</td>
<td>This course enables the skilled malware analyst to branch into the less mainstream (but equally important) areas of reversing C++ binaries and Linux binaries. After a review of assembly, including a deeper dive into the differences between x86 and x64 architectures, students will learn about C++ calling conventions, classes, objects, and exception handling and how these affect reverse engineering and malware analysis. The course then turns to the Linux operating system, covering topics such as kernel structure and the Linux Application Binary Interface (ABI) in preparation for statically analyzing and debugging Linux executables and malware.</td>
<td>7</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Duration</td>
<td>Description</td>
<td>Credits</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>611420</td>
<td>Windows Rootkit Reverse Engineering</td>
<td>5 Days</td>
<td>This course takes students into advanced and specialist malware analysis topics surrounding rootkit analysis. Students will learn about the Windows kernel, automated and manual unpacking, live kernel debugging with IDA and WinDbg, and reverse engineering drivers. This is a heavily lab-intensive course that requires students to have a solid background in programming, reverse engineering, and malware analysis prior to attending.</td>
<td>7</td>
</tr>
<tr>
<td>611420</td>
<td>Introduction to C Programming</td>
<td>5 Days</td>
<td>C is one of the oldest and yet most widely used high-level programming languages in the world today. This course covers the fundamental principles of programming in this essential language. Suitable for beginners, it starts with the basics of programming languages, program structure, and programming concepts before progressing to topics such as variables and scope, arithmetic operators, control flow, basic I/O, and using libraries. By the end of this course, students should be able to write, compile, and execute C programs that perform a variety of functions involving file and user I/O, data structures, algorithmic data manipulation, memory management, and more. This course also serves as a platform from which to learn more advanced static malware analysis techniques, such as disassembly.</td>
<td>7</td>
</tr>
<tr>
<td>611420</td>
<td>Introduction to System Programming in C</td>
<td>5 Days</td>
<td>This course takes those with entry-level competency in C programming to a more advanced level. It will enable them to build programs that involve complex data structures and types, manage interaction between processes and threads, perform pointer arithmetic and manipulation, dynamically allocate and manage memory, and read/write binary data to/from file systems and network sockets. This course also</td>
<td>7</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course Title</td>
<td>Duration</td>
<td>Description</td>
<td>Fee</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----</td>
</tr>
</tbody>
</table>
| 611420      | Introduction to C++ Programming    | 5 Days   | This course introduces the student to the core concepts of object-oriented programming and equips them to implement these concepts in the C++ programming language. Starting with the foundations of classes, objects, inheritance, and polymorphism, the course covers a wide range of techniques and is designed for those who are new to object-oriented programming. This course also serves as a platform from which to learn more advanced static malware analysis techniques for binaries created in object-oriented languages.
|             |                                    |          |                                                                                                                                                                                                            | 7   | 20      | Both |
| 611420      | Python for Reverse Engineers       | 5 Days   | Scripting and automation can vastly improve the accuracy and efficiency of analytic tasks, especially in the fields of malware analysis reverse engineering. This course is designed to take those with prior programming experience in other languages, through the basics of Python to the point where they can successfully use it to accelerate, automate and optimize reverse engineering tasks. Lab exercises for this course will start with performing basic functions such as producing output and performing calculations, progress through more complex structure and the use of file I/O, modules and libraries, and culminate with performing malware analysis and reverse engineering tasks using Python, including the use of IDAPython.
<p>|             |                                    |          |                                                                                                                                                                                                            | 7   | 20      | Both |
| 611420 | Introduction to Cyber Risk Management | 1 Day | This is a one-day, seminar-style program that covers the cyber fundamentals leaders need to operate their business securely, embrace disruption safely, and effectively communicate cyber risks within their organizations. Designed with busy executives in mind, this program dissects the most important issues in cyber risk management and arms attendees with the tools needed to engage in strategic cyber conversations at the executive level. | 7 | 100 | Both |</p>
<table>
<thead>
<tr>
<th>SIN(s)</th>
<th>Course Title</th>
<th>Location (Customer or Contractor Site or Both)</th>
<th>Course Length</th>
<th>Minimum Participants</th>
<th>Maximum Participants</th>
<th>PRICE TO GSA (including IFF)</th>
<th>QUANTITY/VOLUME DISCOUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>611420</td>
<td>Introduction to Cyber Security</td>
<td>Contractor Site</td>
<td>3 Days</td>
<td>7</td>
<td>20</td>
<td>$2,167.36</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Understanding Operating Systems</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Live System Analysis</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>iOS Attack &amp; Defend</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Antdroid Attack &amp; Defend</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Behavioral Malware Analysis</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Assembly for Reverse Engineers</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Malware Reverse Engineering</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Hacking with Python</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Hacker Methodologies for Security Professionals</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Network Traffic Analysis</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Python for Network Defenders</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>SIN(s)</td>
<td>Course Title</td>
<td>Location (Customer or Contractor Site or Both)</td>
<td>Course Length</td>
<td>Minimum Participants</td>
<td>Maximum Participants</td>
<td>PRICE TO GSA (including IFF)</td>
<td>QUANTITY/VOLUME DISCOUNT</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>---------------</td>
<td>----------------------</td>
<td>----------------------</td>
<td>-----------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>611420</td>
<td>Malicious Network Traffic Analysis</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Cyber Threats Detection and Mitigation</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Advanced Network Traffic Analysis</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$3,450.98</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Windows System Analysis</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$4,443.32</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Linux Kernel Internals</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$4,443.32</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Advanced Linux Kernel Internals</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$4,443.32</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Linux &amp; C++ Reverse Engineering</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$4,443.32</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Windows Rootkit Reverse Engineering</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$4,443.32</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Introduction to C Programming</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$4,443.32</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Introduction to System Programming in C</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$4,443.32</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Introduction to C++ Programming</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$4,443.32</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Python for Reverse Engineers</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$4,443.32</td>
<td>None</td>
</tr>
<tr>
<td>611420</td>
<td>Introduction to Cyber Risk Management</td>
<td>Both</td>
<td>5 Days</td>
<td>7</td>
<td>20</td>
<td>$1,179.95</td>
<td>None</td>
</tr>
</tbody>
</table>
1. SCOPE

a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services apply exclusively to IT/IAM Professional Services within the scope of this Information Technology Schedule.

b. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)

a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.

b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.

c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity’s mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDER

a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.

b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

4. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of IT/IAM Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

5. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.
(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6. INSPECTION OF SERVICES


7. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data – General, may apply.

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT/IAM Professional Services.

9. INDEPENDENT CONTRACTOR

All IT/IAM Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.
b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

11. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for IT/IAM Professional services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

12. PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31 (FEB 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition. As prescribed in 16.601(e)(3), insert the following provision:

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

(b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—

(1) The offeror;

(2) Subcontractors; and/or

(3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES
Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

14. INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

16. DESCRIPTION OF IT/IAM PROFESSIONAL SERVICES AND PRICING

a. The Contractor shall provide a description of each type of IT/IAM Service offered under Special Item Numbers 132-51 IT/IAM Professional Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all IT/IAM Professional Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.

The following is an example of the manner in which the description of a commercial job title should be presented:

EXAMPLE: Commercial Job Title: System Engineer

Minimum/General Experience: Three (3) years of technical experience which applies to systems analysis and design techniques for complex computer systems. Requires competence in all phases of systems analysis techniques, concepts and methods; also requires knowledge of available hardware, system software, input/output devices, structure and management practices.

Functional Responsibility: Guides users in formulating requirements, advises alternative approaches, conducts feasibility studies.

Minimum Education: Bachelor’s Degree in Computer Science
Labor Category Descriptions

Solution Architect

**Functional Responsibility:** The Solution Architect is responsible for the design of the solution, business / technical requirements and for ensuring that the development and implementation of the solution is performed within the bounds of the labor contract between APTEC and the client. This role also performs project management activities to ensure the overall APTEC delivery team meets the schedule and budget of the project, communicates regularly with the customer on all project-related issues, and is the project-specific supervisor of the rest of the APTEC project delivery team, which may include Senior Consultants and Senior Developers.

**Minimum Experience:** A minimum of twelve (12) years of related experience.


Senior IT Consultant

**Functional Responsibility:** The Senior IT Consultant is responsible for solution implementation according to the bounds of the labor contract, activities include solution configuration according to design specifications, solution test planning and testing, solution bug fixing, and solution documentation and readiness for production deployment and actual production deployment/support activities. Also responsible for training the customer's technical and support staff on all relevant aspects of the solution to facilitate full knowledge transfer in accordance with the terms of the contract.

**Minimum Experience:** A minimum of eight (8) years of related experience.


Senior Developer

**Functional Responsibility:** The Senior Developer is responsible for all solution development activities, including custom API development/integration according to design specifications in
the appropriate programming languages, development of user interfaces and development of auditing and reporting systems, database integration and development of SQL code. This position is also responsible for supporting the solution quality assurance and user acceptance testing cycles, providing code-based bug fixes, client knowledge transfer and training on the solution and all appropriate solution documentation in the area of application development and solution integration.

**Minimum Experience:** A minimum of eight (8) years of related experience.

### Hourly Rates for Work Performed at the Customer Location

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Price w/ IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Solution Architect</td>
<td>$204.59</td>
</tr>
<tr>
<td>54151S</td>
<td>Senior IT Consultant</td>
<td>$168.79</td>
</tr>
<tr>
<td>54151S</td>
<td>Senior Developer</td>
<td>$153.44</td>
</tr>
</tbody>
</table>

*Hourly Rates are for Work Performed at the Customer Location*