AURORA

CYBER SECURITY SERVICES

About Us

Since 1990, security-conscious companies have turned to Aurora for support of their business-critical applications. Aurora's highly trained sales and engineering teams combine to uniquely position the company as a single source security consulting service provider. A combination of strong solutions offerings and meaningful partner relationship allows Aurora to serve a growing list of clients spanning across three business units:

ENTERPRISE – We specialize in commercial, enterprise & mid-market clients

STATE, LOCAL, EDUCATION – Aurora maintains numerous CMAS Contracts, SLPs and NASPO Agreements frequently used as purchasing vehicles for State, Local and Educational institutions

FEDERAL GOVERNMENT – We are on multiple GWACS including SEWP and STARS II to make it easy for federal customers to work with us

In each of these three business units, we have dedicated resources that focus on:

Security Consulting Services – such as penetration tests, vulnerability assessments, gap analysis and security strategy

Professional Services – our highly trained engineers work with a set of premium partners to bring you leading edge cyber security solutions

OVERVIEW

- We put our **CUSTOMERS' NEEDS FIRST**, educating our customers on the latest technology and product road maps, addressing key business requirements and then working with your team to ensure a successful outcome.

- Our customers rely on Aurora's decades of **EXPERIENCE** in Information Technology to navigate complex Cyber security challenges.

- We focus on a handful of Partners and create **MEANINGFUL RELATIONSHIPS** with them, ensuring that our customers gain the most out of these partnerships.

- We invest heavily in **TRAINING, CERTIFICATIONS, TESTING, RESEARCH, AND IN-HOUSE LABS**. Our highly experienced Sales and Engineering teams have a thorough understanding of security solutions and product interdependencies.

Aurora's expertise is **WELL RECOGNIZED** in both Commercial and Government settings. Our team is equipped with manufacturer and industry certifications for dozens of cyber security disciplines. Public Sector accounts can leverage numerous specialized contract awards and competencies listed on our website.

GSA 8(a)STARS II

SEWP Approved SEWP V Federal Government IT Provider

CMAS Approved Contractor DGS California Multiple CMAS Award Schedules

Certified LSBE County of Los Angeles California 110943

California Small Business 9420

CYBERSECURITY FRAMEWORK CONSULTING SERVICES

AURORA

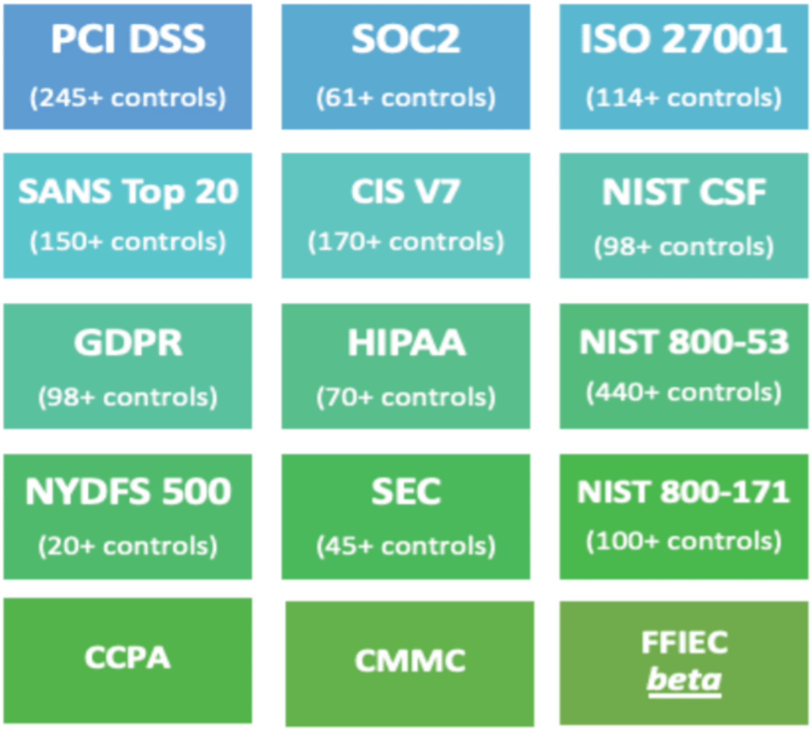
Aurora's Security Consulting Services team provides the expertise and analysis to help you enhance your IT security posture, reduce your information security risk, facilitate compliance requirements and improve your overall operational efficiency.

Aurora provides full lifecycle consulting assessment services to over 15 frameworks & 18 security domains to help your organization easily assess, remediate and deliver cybersecurity and compliance programs on one platform. Aurora's unique value-add is to increase efficiencies by 50% by combining redundant controls when applying multiple frameworks and by centralizing data into a single depository.

Aurora's assessment model has tremendous financial benefits:

- Elimination of spreadsheets and ad hoc processes
- Consolidation of documents into a single repository or link to existing data locations.
- Elimination to maintain framework guidance and policy documentation
- DIY model with Aurora consulting services hybrid model will save on consulting fees

Aurora assessment platform model includes the following frameworks:



PCI DSS (245+ controls)	SOC2 (61+ controls)	ISO 27001 (114+ controls)
SANS Top 20 (150+ controls)	CIS V7 (170+ controls)	NIST CSF (98+ controls)
GDPR (98+ controls)	HIPAA (70+ controls)	NIST 800-53 (440+ controls)
NYDFS 500 (20+ controls)	SEC (45+ controls)	NIST 800-171 (100+ controls)
CCPA	CMMC	FFIEC ***beta***

OVERVIEW

AURORA
SECURITY CONSULTING SERVICES

Aurora's Security Consulting Services team has vast experience in delivering service engagements and assessments for small and large companies in almost all lines of business from financial and healthcare, to manufacturing and high technology, to retail and food service industries. Our team offers a wide range of services. Our range of expertise, experience, proven scope and approach lets us be your partner in many aspects of your cybersecurity management program.

Cyber Security Risk Assessment

HIPAA Security & Compliance

Application Security Assessment

Data Loss Prevention Assessment

PCI DSS Gap Analysis

Penetration Testing

Phishing Simulation Assessment

Security Training Assessment

Vulnerability Assessment

Security Policy Development

Security Code Review

AURORA
PROFESSIONAL SERVICES

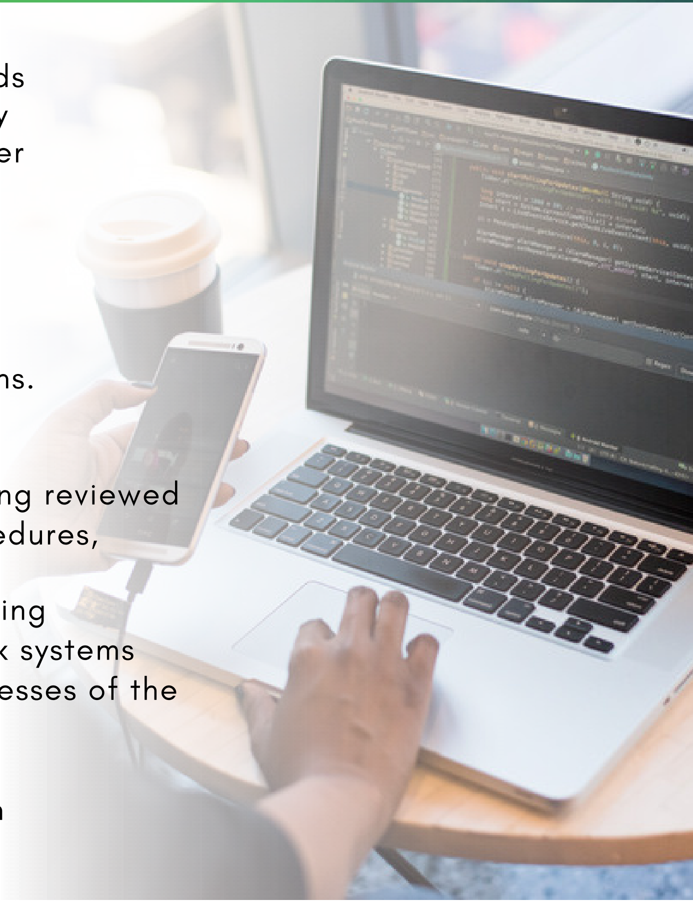
Aurora's Professional Services team constantly strives to attain the highest partnership levels with our technology partners so that we can better leverage support, access new products and roadmaps, strategic management relationships, and better pricing for our customers. This also elevates our engineer's capabilities as they are frequently required to refresh their technical certification and training to meet constantly evolving standards. These requirements include pre-sales knowledge of product features and benefits, POCs (Proof of concepts) and ability to perform demos for our customers.

Symantec. A Division of Broadcom BeyondTrust Windows

aws tenable SOPHOS McAfee

aurorait.com
sales@aurorait.com
888-282-0696

CYBER SECURITY RISK ASSESSMENT



Our solution uses quantitative and qualitative methods to define the current and future state of your security environment in a complete internal and external Cyber Security Risk Assessment. We determine how your organization maps to best practices, along with the steps needed to get to the next level of security, and maintain a robust security environment as change occurs. A Cyber Security Risk Assessment identifies deficiencies and correlates them to practical solutions.

HOW THE PROCESS WORKS

- Define a scope of each process and function being reviewed
- Gather all current documentation (policies, procedures, configuration standards, best practices used)
- Conduct internal and external vulnerability scanning
- Conduct penetration testing against your network systems
- Interview individuals and document how the processes of the business functions
- Compare security practices to best practices
- Prioritize the gaps and create a remediation plan
- Produce a qualitative risk report

KEY VALUE PROPOSITIONS INCLUDE:

- Understand gaps in regulatory compliance requirements
- Understand weaknesses in existing policies, procedures and standards
- Determine weaknesses in access controls, user provisioning, configuration management, vulnerability management processes, and incident handling processes
- Review of network, operating system, application and endpoint vulnerability security measures
- Development of key remediation recommendations

BUSINESS VALUE

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge Transfer

FEATURES AND BENEFITS

- Complete overall network security gap analysis
- Consistent and repeatable testing
- Continuously expanding tests
- Comply with industry-driven regulatory requirements

HIPAA SECURITY & COMPLIANCE

Our HIPAA information security audit is an in-depth appraisal of an organization's adherence to existing policies and industry best practices, and identification of areas of weakness that need to be addressed to meet business needs and/or regulatory and compliance requirements. We will assess existing weaknesses and develop countermeasures in three areas-people, process, and technology-for HIPAA Security Rule requirements.

Aurora provides our clients comparative information and baselines against industry standard practices in addition to the HIPAA mandated review items in the Security Rule. A complete assessment, as required under the HIPAA risk assessment specifications, includes interviews with personnel, system analysis, policy and procedure review, and remediation suggestions. Our cost-effective approach to security and compliance makes it affordable for any size healthcare organization to be in compliance- without cutting any corners. Our comprehensive HIPAA Security assessment service offers an approach based on assessing physical and logical security, and company practices for security confidential data.

HOW THE PROCESS WORKS

- Assess the current state of security
- Develop comprehensive HIPAA Security policy and authorization levels
- Review all relevant security documentation and interview staff
- Perform vulnerability scans locally or remotely over a VPN connection
- Evaluate current practices
- Deliver a recommendations report to close gaps in security practices

KEY VALUE PROPOSITIONS INCLUDE:

- Quickly validate problems and resolution, and prioritize vulnerabilities
- Automated testing provides recommendations for remediation
- Discover key weaknesses, policies and procedures
- Categorize missing controls
- Review network, operating system, application and endpoint security measures

BUSINESS VALUE

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater RO
- Optimized implementation
- Knowledge transfer

FEATURES AND BENEFITS

- Understand gaps in regulatory compliance requirements
- Understand weaknesses in existing policies, procedures and standards
- Determine weaknesses in access controls, user provisioning, configuration management, vulnerability management and incident handling processes
- Review of network, operating system, application and endpoint security measures

aurorait.com
sales@aurorait.com
888-282-0696

APPLICATION SECURITY ASSESSMENT

Our Application Security Assessment is designed to meet best practices for application security. Industry regulations such as PCI, HIPAA and Red Flag require application security testing, Aurora can also assess custom- built web applications and commercial applications.

All security assessments will involve, but are not limited to, the following methodologies:

- Analysis of data access requirements
- Input validation
- Transport mechanism
- Error Condition Handling and Exception Management
- Business Logic, Functional Specification and Implementation
- Site design

HOW THE PROCESS WORKS

- Probe, identify and exploit vulnerabilities in systems within scope, with manual techniques and automated tools
- Attempt to escape out of the network and application boundaries of the systems within scope
- Attempt to gain unauthorized access to systems within scope and systems connected to the web application

KEY VALUE PROPOSITIONS INCLUDE:

- Discovery of key weaknesses in the servers
- Manual and automated testing procedures
- Review of network, operating system, application and end-point security measures
- Development of key remediation recommendations
- Client specified Internet reachable systems

BUSINESS VALUE

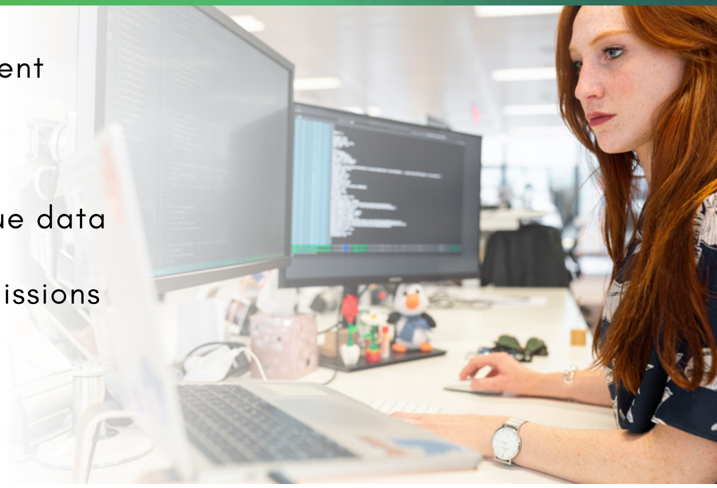
- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge Transfer

FEATURES AND BENEFITS

- Simulates an attacker
- Consistent and repeatable testing
- Continuously expanding vulnerability tests
- Comply with industry-driven regulatory requirement
- Fixed fee

aurorait.com
sales@aurorait.com
888-282-0696

DATA LOSS PREVENTION ASSESSMENT



The Aurora Data Loss Prevention Technical Assessment provides the following:

- Current and ideal state of the customer's data classification and data loss prevention program
- Insight into data aging, access patterns, and true data ownership based on these patterns
- Where sensitive data is being stored, what permissions surround this data, and who is accessing it

Highlights of the Data Loss Prevention Assessment

TECHNICAL REQUIREMENTS WORKSHEET

Aurora and the customer will work together to detail the technical requirements including repositories to be scanned and samples of any documents to be collected. For the assessment, the following guidelines should be followed:

- focus on 1 to 3 file share repositories
- less than 1 TB total data
- Three to four data loss prevention policies

TECHNICAL ASSESSMENT

- The assessment will run for 2 to 4 weeks, depending on the scope of engagement and how much data/usage metrics are required
- The required hardware and software is provided as part of the assessment, and agent installers will be provisioned to be installed on any required repositories

DATA CLASSIFICATION TECHNICAL ASSESSMENT

- At the end of the engagement, Aurora will provide the customer with a report detailing the findings from the engagement
- This includes remediation paths and next steps to minimize risk
- Raw data reports can also be provided to allow for immediate action on high risk repositories

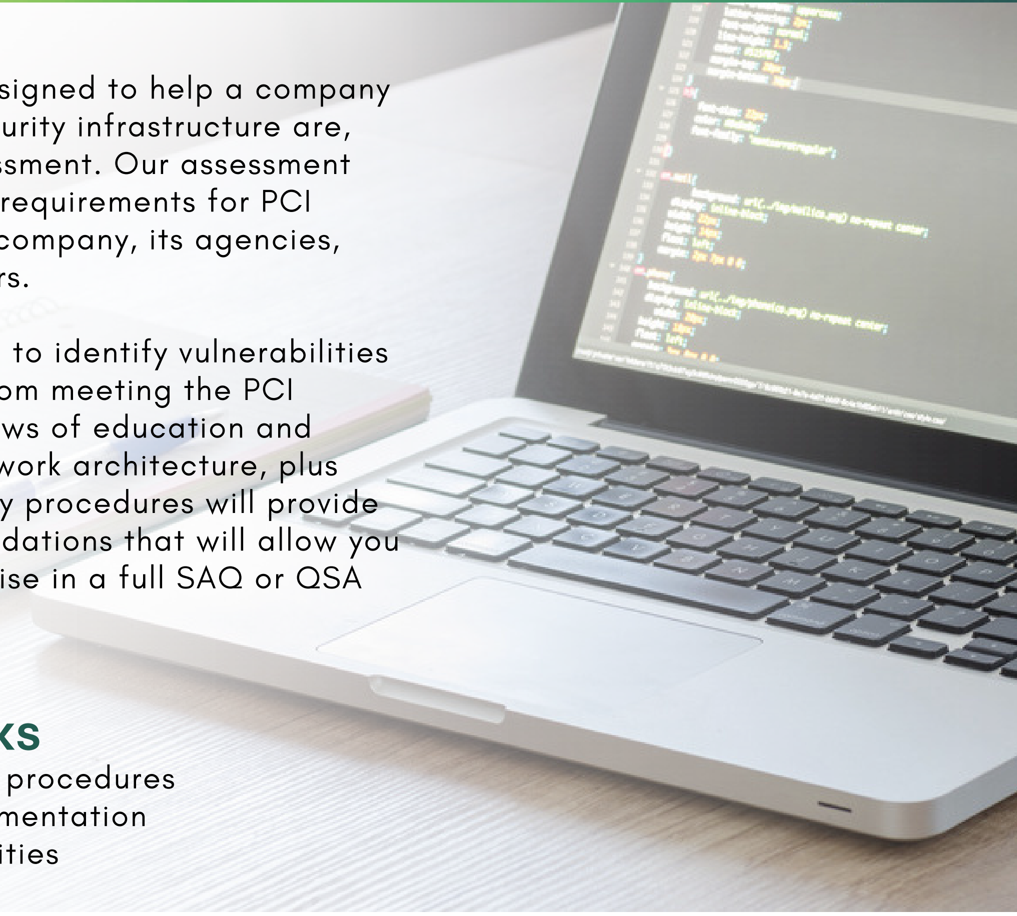
FEATURES

- Recommendations for optimizing the storage environment.
- Classify existing unstructured data by file type, age, use, value to business, etc.
- Achieve greater return on investment.
- Data Classification Report detailing structure, use, and potential exposure

BENEFITS

- Understanding of where unstructured data resides in the physical architecture
- Relate unstructured data to its application(s), from data lifecycle and application criticality perspectives
- Understand how unstructured data is used as information and its importance in achieving the mission of the client

PCI DSS GAP ANALYSIS



Our PCI DSS Gap Analysis is designed to help a company determine where gaps in its security infrastructure are, prior to a full PCI DSS risk assessment. Our assessment services identify and scope the requirements for PCI compliance as it relates to the company, its agencies, merchants and services providers.

Our scanning services allow you to identify vulnerabilities that may block your company from meeting the PCI security requirements. Our reviews of education and training of all stakeholders, network architecture, plus network and application security procedures will provide a solid foundation of recommendations that will allow you to anticipate issues that may arise in a full SAQ or QSA review.

HOW THE PROCESS WORKS

- Identify gaps in operational procedures
- Identify gaps in policy documentation
- Identify technical vulnerabilities

KEY VALUE PROPOSITIONS INCLUDE:

- Quickly validate problems and resolution, prioritize vulnerabilities
- Automated testing provides recommendations for remediation
- Discovery of key weaknesses policies and procedures
- Categorize missing controls
- Review of network, operating system, application and end-point security measures
- Development of key remediation recommendations

BUSINESS VALUE

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge Transfer

FEATURES AND BENEFITS

- Simulates a PCI SAQ assessment
- Consistent and repeatable testing
- Comply with industry-driven regulatory requirement
- Anticipate problems in a full PCI DSS assessment
- Fixed fee

PENETRATION TESTING

Penetration Testing is the first tactical step many companies take to begin the identification process for weaknesses in their IT environment. Our security professionals use proven techniques, methodologies and tools to detect undesirable risks. Aurora will evaluate your technical, administrative and management security controls, and conduct tests against your Internet perimeter using real-world attacks techniques — both automated and manual.

Aurora currently offers 4 types of Penetration Tests:

EXTERNAL PENETRATION TESTING

- Simulates an external or outside attacker.
- Probes, identifies and exploits vulnerabilities in systems within scope
- Attempts to breach the security perimeter of the network boundaries
- Attempts to gain access to systems within scope, upon breach

INTERNAL PENETRATION TESTING

- Simulates an internal attacker, from inside the organization
- Attempts to escape out of the network boundaries
- Attempts to gain unauthorized user access to systems within scope and systems connected to network

WEBSITE APPLICATION PENETRATION TESTING

- Designed to meet best practices and industry regulations for application security such as; PCI, HIPAA and Red Flag
- An assessment looks at the source code, the infrastructure, the operating systems
- and the application functionality
- Attempts to gain unauthorized access to systems connected to the web application

WIRELESS LOCAL AREA NETWORK (WLAN)

- Scalability and features of current systems
- Authentication & encryption controls in use
- Detect rogue wireless Aps
- Penetration testing of the wireless setup

BUSINESS VALUE

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge Transfer

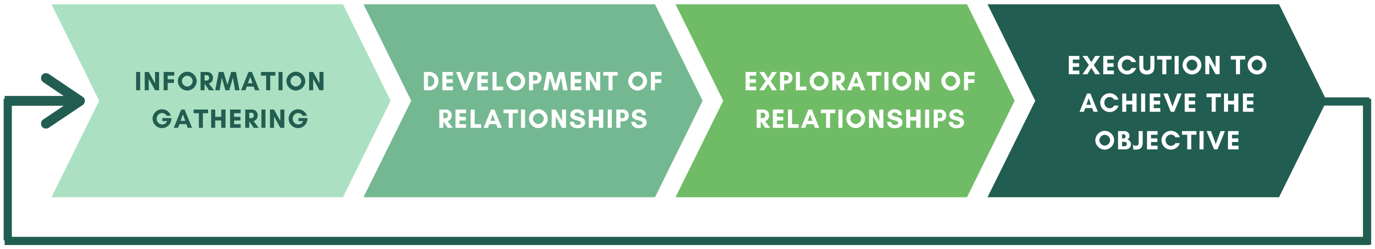
FEATURES AND BENEFITS

- Review of network, operating system, application and endpoint security measures
- Comply with industry-driven regulatory requirement
- Continuously expanding vulnerability tests and remote testing
- Discovery of key weaknesses in the servers
- Manual and automated testing procedures

PHISHING SIMULATION ASSESSMENT

Phishing attacks are designed to deceive individuals into providing sensitive information such as passwords to a malicious third-party, or into performing actions such as downloading malware de- signed to give an attacker remote control over the victim's computer. Disturbingly, these attacks are becoming increasingly sophisticated, to the extent that often neither the individual nor the organization to which they belong is even aware that an incident has occurred until it is too late.

THE SOCIAL ENGINEERING ATTACK CYCLE


INFORMATION GATHERING
DEVELOPMENT OF RELATIONSHIPS
EXPLORATION OF RELATIONSHIPS
EXECUTION TO ACHIEVE THE OBJECTIVE

DO YOU REALLY KNOW YOUR SECURITY POSTURE?

To gauge your current security posture in terms of the risk posed by phishing attacks, ask yourself the following questions:

- As part of your regular security assessments, have you ever performed a controlled phishing attack?
- Would you expect your employees to click on a malicious link within an email? Would they then go on to disclose authentication credentials or attempt to download a malicious payload?
- How many employees in your organization would you expect to perform those actions?
- Which offices and departments within your organization are most likely to be susceptible to a phishing attack?
- Therefore, do you know where your security training budget is best spent for maximum impact and 'quick wins'?
- Have you ever run security awareness campaigns? If so, how effective do you think they were?
- If there were a phishing attack, would there be an internal response, or would it go unnoticed?
- Is the response guaranteed to go as per policy and procedure, or would a real -world attack be likely to cause chaos and confusion?
- If there were a response, would it be sufficient to mitigate the risk posed by the attack?
- Is your organization more or less susceptible to phishing attacks than other organizations with- in the same market sector?

SECURITY TRAINING ASSESSMENT

People are often the weakest link and the most under-invested component of organization's security strategy. Our security training fills this gap by providing interactive on-demand and instructor-led education that is accessible 24x7. Training is role-focused and can be customized to your security requirements and environment.

LIST OF COURSES

SECURITY AWARENESS (30-45 MINUTES EACH)

AWARE-01	Security Awareness Training
AWARE-02	PCI DSS Security Training
AWARE-03	HIPAA/HiTech Security Training
AWARE-04	Advanced Security Awareness Training for IT

APPLICATION SECURITY (2-3 HOURS EACH)

APPSEC-01	Introduction to Application Security – OWASP Top 10
APPSEC-02	Application Security Emerging Threats
APPSEC-03	Security Testing for QA / Ethical Hacking
APPSEC-04	Mobile Apps (IOS / Android) Security Top 10
APPSEC-05	Security for Technical Management / Threat Modeling
APPSEC-06	Cloud Security / AWS Best Practices

SECURITY FOR DEVELOPERS (3-4 HOURS EACH)

DEV-01	Security Training for Developers
DEV-02	Security Training for Developers – .NET
DEV-03	Security Training for Developers – JAVA / J2EE
DEV-04	Security Training for Developers – IOS
DEV-05	Security Training for Developers – Android

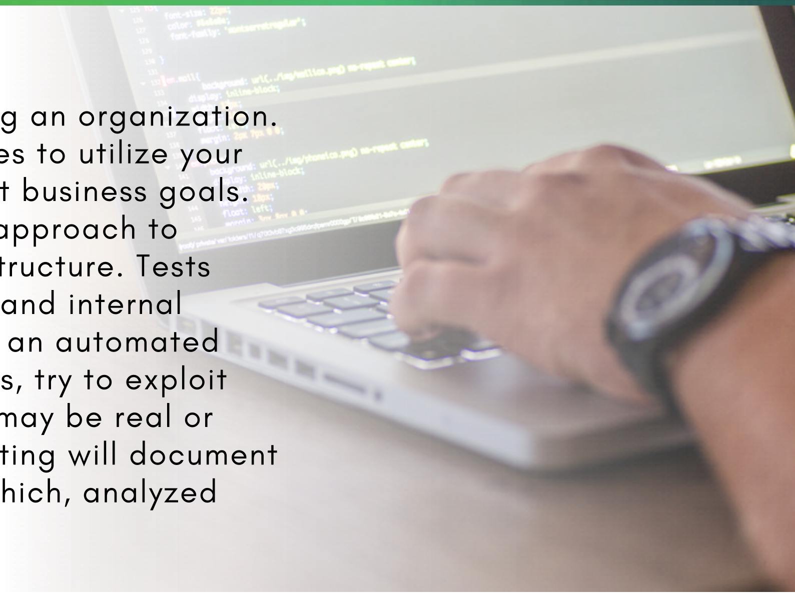
DATABASE SECURITY (1-2 HOURS EACH)

DATAB-01	Oracle Database Security
DATAB-02	SQL Server Data- base Security

FEATURES AND BENEFITS

- Delivered on-demand, instructor-led or hybrid
- Interactive engaging content with quiz and learning games
- SCORM Compliant
- Customized to your role and company policy standards
- Repeat multiple times reinforce key concepts
- Monthly student activity and progress reports
- Meet PCI DSS, HIPAA and other compliance requirements
- Deliverables include all content & training completion certificates

VULNERABILITY ASSESSMENT



Vulnerability analysis is the frontline in securing an organization. Aurora can develop custom-built methodologies to utilize your personnel and financial resources to help meet business goals. Vulnerability scanning is a necessary tactical approach to securing all the "low-hanging" risk in an infrastructure. Tests will be conducted against Internet perimeters and internal systems using real world attacks techniques in an automated manner. We analyze all potential vulnerabilities, try to exploit them to leverage access and determine what may be real or what may be "false" positives. Our exploit testing will document the security exposure of any in scope assets which, analyzed collectively, may lead to unauthorized access.

HOW THE PROCESS WORKS

- Remote testing of internal networked devices via a VPN connection
- Architecture review
- Automated external scanning
- Automated internal security scanning
- Recommendations matrix as final delivery report
- Fixed fee

KEY VALUE PROPOSITIONS INCLUDE:

- Discovery of key weaknesses in the servers
- Methodology development
- Analysis of remediation process and solution development
- Development of key remediation recommendations
- Policy development to maintain proper vulnerability remediation procedure

BUSINESS VALUE

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge transfer

FEATURES AND BENEFITS

- Review of network, operating system, and application security
- Determine weaknesses in access controls, vulnerability management processes, incident handling processes
- Understand weaknesses in existing policies, procedures

SECURITY POLICY DEVELOPMENT

Our complete set of security policies can be developed including the infrastructure, third-party, asset classification, accountability, personnel security, physical and environmental security, communications security, operations security, user education and awareness, access control, system development life cycle, business continuity, disaster recovery, and regulatory compliance.

HOW THE PROCESS WORKS

- Gap analysis of current policies and operating environment with policies developed accordingly
- Policies mapped towards industry's best standards
- Policies and procedures that can evaluated include:
  - Disaster Recovery/Business Continuity Plan (BCP)
  - Incident Response and Notification
  - Account Administration (administrative & user)
  - Virus and Malicious
  - Code Protection
  - Network Security
  - Security Control over Network Servers (web, databases, etc.)
  - Information System Logging and Monitoring
  - Configuration and Control Over Routers and Gateways

KEY VALUE PROPOSITIONS INCLUDE:

- Quickly validate problems and resolution, prioritize vulnerabilities
- Automated testing provides recommendations for remediation
- Development of key remediation recommendations

BUSINESS VALUE

- Cost effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge transfer

FEATURES AND BENEFITS

- Develop policies to meet gaps (except BCP)
- 7 policies reviewed and/or developed
- Fixed Fee

SECURITY CODE REVIEW

Security code review provides insight into the "real risk" associated with insecure code. When used together with automated tools and manual penetration testing, code reviews. When used together with automated tools and manual penetration testing, code review can significantly increase the cost effectiveness of an application security verification effort. Aurora combines automated and manual code analysis techniques in a multi-step process of familiarization, prioritization and analysis to understand the context and make a relevant risk estimate that accounts for both the likelihood of attack and business impact of a breach.

HOW THE PROCESS WORKS

- Identify and remediate code level vulnerabilities
- Conduct security due diligence of key applications and 3rd party software
- Meet regulatory requirements (PCI DSS 1.2, clause 6.3.7)
- Educate developers on secure coding best practices
- Enforces security as development priority

KEY VALUE PROPOSITIONS INCLUDE:

- Minimize the risk and likelihood of a network breach
- Secure Code training for developers
- Increased cost effectiveness of applications security

BUSINESS VALUE

- Cost-effective compliance
- Prioritized and simplified recommendations
- Achieve greater return on investment
- Optimized implementation
- Knowledge transfer

FEATURES AND BENEFITS

- Review of network, coding and application security
- Determine weaknesses and vulnerabilities with code analysis
- Achieve government mandated compliance requirements

AURORA PROFESSIONAL SERVICES

AURORA
PROFESSIONAL SERVICES

Aurora's Professional Services team has vast experience in delivering service engagements and assessments for small and large companies in almost all lines of business from financial and healthcare, to manufacturing and high technology, to retail and food service industries. Our team offers a wide range of services from **CYBERSECURITY CONSULTING & ASSESSMENTS**, **IMPLEMENTATION**, and **REMEDIATION** services. Our range of expertise, experience, proven scope and approach lets us be your partner in many aspects of your **CYBERSECURITY MATURITY PROGRAM**.

Our areas of expertise continue to grow as we naturally adapt to the changing customer needs, threat intelligence, emerging technologies, and shifting market strategies and consolidations. We have SMEs (Subject Matter Experts) on Data Loss Preventions (DLP), Data Classification, Endpoint Security, CASB, Vulnerability Management, EDR, Policy Orchestration, Encryption, Identity Access Management, Datacenter and Infrastructure services (Windows, Azure, AWS, GCP,VDI, VMWare).

We constantly strive to attain the highest partnership levels with our technology partners so that we can better leverage support, access new products and roadmaps, strategic management relationships, and better pricing for our customers. This also elevates our engineer's capabilities as they are frequently required to refresh their technical certification and training to meet constantly evolving standards. These requirements include pre-sales knowledge of product features and benefits, POCs (Proof of concepts) and ability to perform demos for our customers.

During all engagements, we work closely with the client's staff, sharing information and educating the staff when possible. We want to partner with our clients rather than be a point solution provider. Security is a long process that cannot be solved by any one engagement. The results of all engagements are tailored to the client's requests, needs and business goals, with constant communication every step of the way, and we can speak to any level of the organization from CEO and CFO to technicians and sales staff.

SYMANTEC PARTNER SOLUTIONS

AURORA
PROFESSIONAL SERVICES

Symantec.
A Division of Broadcom

Aurora is an established premier partner of Broadcom/Symantec with deep knowledge and experience within the Symantec security portfolio. With recognized expertise in multiple Symantec solution sets and a high level of customer satisfaction, Aurora has established itself as a proven IT strategic security partner with their clients.

Our highly skilled staff of professional service engineers have solution expertise in the following areas: **Data Loss Prevention (DLP), Encryption, Validation & ID Protection (VIP), Endpoint Protection (SEP), Symantec Encryption Management Server (SEMS), Symantec Endpoint Security (SES), Symantec Endpoint Encryption (SEE) and Symantec Cloud SOC (CASB).**

Aurora's goal is to ensure that Symantec broad security solution sets are appropriately aligned with organization’s key initiatives to maximize their return on investment. Our areas of expertise continue to grow as we naturally adapt to the changing customer needs, threat intelligence, emerging technologies, and shifting market strategies and consolidations. We have SMEs (Subject Matter Experts) on Data Loss Preventions (DLP), Data Classification, Endpoint Security, CASB, Vulnerability Management, EDR, Policy Orchestration, Encryption, Identity Access Management, Datacenter and Infrastructure services (Windows, Azure, AWS, GCP,VDI, VMWare).

INFORMATION SECURITY

Data Loss Prevention (DLP)
Secure Access Cloud
CloudSoc (CASB)
Encryption
Control Compliance Suite

IDENTITY SECURITY

VIP
MPKI (Digicert)

ENDPOINT SECURITY

End-user Endpoint Security
Server Security
Endpoint Management

NETWORK SECURITY

Messaging Gateway
Encrypted Traffic Management
Advanced Threat Protection

PARTNER LEVEL: PREMIER

BROADCOM
CA AUTHORIZED PARTNER
Premier
SYMANTEC

Symantec.
Symantec KNIGHTS

EXPERIENCE:

- 10 years of DLP experience
- Over 10 years of endpoint experience
- Experience with fortune 500, healthcare, public sector, higher education, and federal customers

AURORA FACTS:

- Geography Covered: National
- 23 Years in Business
- Customer Segments:
  - Enterprise
  - SLED
  - Healthcare
  - Federal

aurorait.com
sales@aurorait.com
888-282-0696

MCAFEE PARTNER SOLUTIONS

Aurora has been a long-standing professional services partner of McAfee for over a decade, with clients in various vertical industries ranging from education, healthcare, commercial, communications, and financial industries. Aurora's professional services and solution architects are highly qualified and experienced across the McAfee solution portfolio.

Our highly skilled staff of professional service engineers have solution expertise in the following areas: MVISION, Cloud Security, Endpoint Security, Cloud Access Security Broker (CASB), Endpoint Detection & Response, Data Protection & Encryption, ePolicy Orchestrator and Web Gateway.

With Aurora service expertise and years as a managed service specialized partner they have established themselves as a trusted McAfee security adviser in the industry.

MVISION CLOUD

Unified Cloud Edge
CASB
Next-gen SWG
Data Protection
Container Security
Workload Protection
Intrusion Prevention

MVISION ENDPOINT

Endpoint Security
Endpoint Detection & Response
Mobile Security
Data Loss Prevention

MVISION PLATFORM

MVISION ePO
MVISION Insights

PARTNER LEVEL: GOLD

EXPERIENCE:

- 10 years of McAfee PO
- Over 10 years of endpoint experience
- Experience with fortune 500, healthcare, public sector, higher education, and federal customers

AURORA FACTS:

- Geography Covered: National
- 23 Years in Business
- Customer Segments:
  - Enterprise
  - SLED
  - Healthcare
  - Federal

aurorait.com
sales@aurorait.com
888-282-0696

TENABLE PARTNER SOLUTIONS

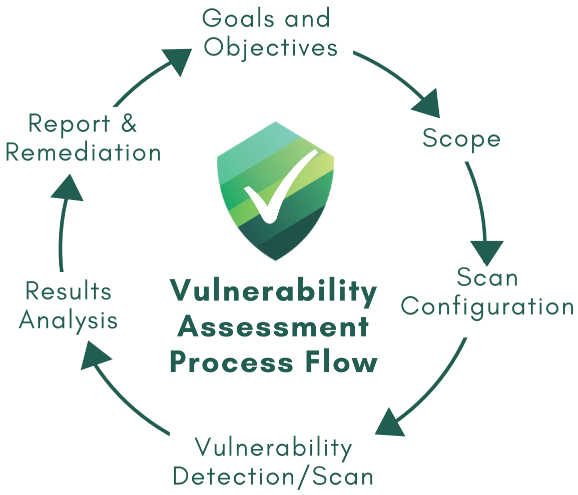
AURORA PROFESSIONAL SERVICES

tenable

Allow Aurora to lighten your organizations vulnerability management operational load. Aurora is offering Vulnerability Management MSSP through tenable IO & SC. With many years of experience in the health care, government and the private sector, we are confident in our ability to reduce the attack surface of your environment. Through custom reporting, detailed configuration and granular vulnerability analysis, we provide a unique vulnerability management platform to each of our customers.

TENABLE PRODUCTS

- Tenable Security Center
  - Tenable IO
  - Web App Scanning
  - Lumin
- Container Security
- Tenable Nessus Pro



OUR SERVICES

- Manage On-premise Tenable SC
- Health Check
- Best Practice Configuration
- Policy Review
- Compliance Standard Review
- Quarterly Business Review
- Patch Management strategy
- Upgrade/Update Tenable SC
- Training of staff
- Weekly, Monthly, Quarterly scans
- Ad-hoc scans
- Custom Reporting Matrix
- Strategic Remediation Plan Service Options

Aurora provides services for customers who have Tenable products already implemented and configured in their environment. As well as customers who have yet to implement a vulnerability management system.

PARTNER LEVEL: GOLD

tenable network security GOLD PARTNER

EXPERIENCE:

- Over 5+ years of Vulnerability Management experience
- HIPAA, PII and PCI Experience

Tenable Certifications:

Tenable SC/IO Pre-Sales Engineer
Tenable SC/IO Pre-Sales Integrator
Tenable SC/IO Pre-Sales Architect

AURORA FACTS:

- Geography Covered: National
- 23 Years in Business
- Customer Segments:
  - Enterprise
  - SLED
  - Healthcare
  - Federal

aurorait.com
sales@aurorait.com
888-282-0696

BEYOND TRUST PARTNER SOLUTIONS

AURORA
PROFESSIONAL SERVICES

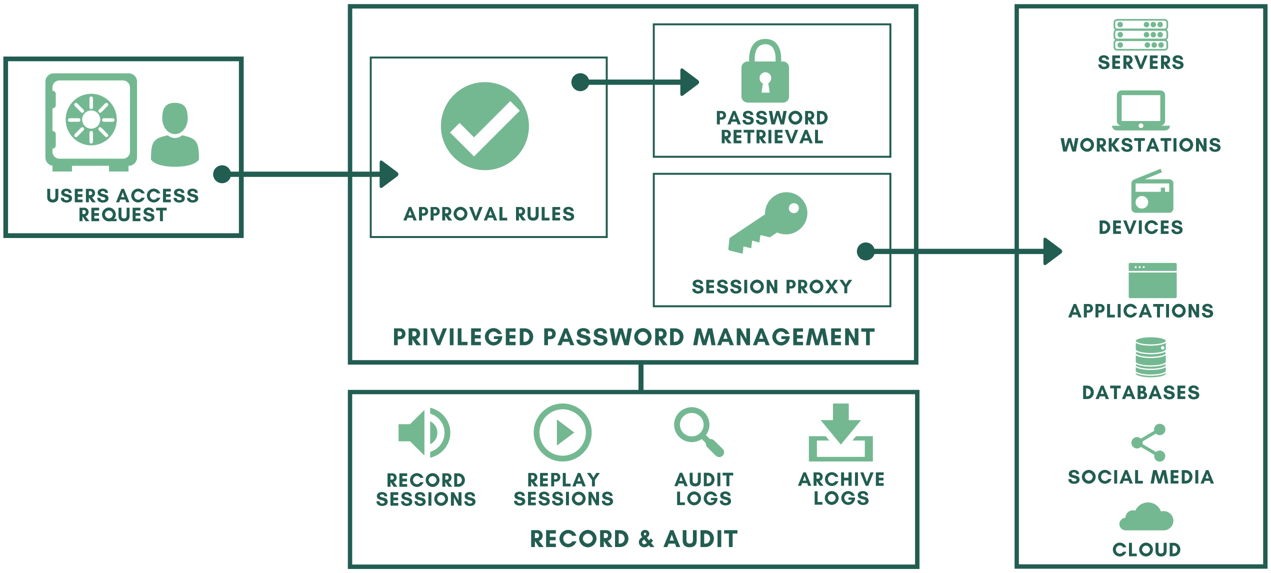
BeyondTrust

Aurora is an established partner of Beyond Trust with a deep knowledge and experience within the Beyond Trust Security Portfolio. Our highly trained engineers can implement full integration of Beyond Trust Privileged Access Management (PAM) solution access Active Directory environment for Desktops and/or Servers. The Aurora team can also mass deploy Beyond Trust Agents as needed for endpoints.

Beyond Trust products that we can sell and service include:

ENDPOINT PRIVILEGE MANAGEMENT

- Windows and Mac
- Unix and Linux
- Active Directory Bridge



PARTNER LEVEL: PREMIER

EXPERIENCE:

BeyondTrust
— CERTIFIED —
Implementation Engineer
Privilege Management
for Desktops

AURORA FACTS:

- Geography Covered: National
- 23 Years in Business
- Customer Segments:
  - Enterprise
  - SLED
  - Healthcare
  - Federal

aurorait.com
sales@aurorait.com
888-282-0696

SOPHOS PARTNER SOLUTIONS

AURORA
PROFESSIONAL SERVICES

SOPHOS

Sophos Endpoint Protection for Desktops, Servers, & Mobile Devices and Sophos XG Firewall

Sophos Endpoint Protection is a leader in endpoint protection. What sets Sophos apart from its competitors is the ability to protect your devices from ransomware. Sophos is unique because they use cryptoguard. This has the ability to do smart machine learning for ransomware to protect files. If your files do get encrypted, it has automatic file recovery built in.

Aurora IT has experienced professionals with Sophos implementation that can help you deploy and configure Sophos Endpoint Protection in your environment.

SOPHOS ENDPOINT PROTECTION INTERCEPTX ADVANCED AND/OR WITH EDR (ENDPOINT DETECTION AND RESPONSE)

- Desktops
- Servers
- Active Directory integration
- Create Endpoint Protection Policies as needed

MOBILE DEVICE MANAGEMENT

- Apple Devices
- Android Devices

SOPHOS XG FIREWALL

- Configure your internal network
- Configure Synchronized Security to work in conjunction with Sophos Endpoint Protection for a more rounded security posture protecting what is on the Network as well as on your end- points

PARTNER LEVEL: GOLD

Sophos Gold Partner

EXPERIENCE:

- Sophos Central Endpoints and Servers for InterceptX Advanced with EDR including Active Directory integration
- Sophos XG Firewall solution on hosted on AzureSophos Certified Engineer

AURORA FACTS:

- Geography Covered: National
- 23 Years in Business
- Customer Segments:
  - Enterprise
  - SLED
  - Healthcare
  - Federal

INFRASTRUCTURE AND DATACENTER SERVICES

AURORA
PROFESSIONAL SERVICES

aws

Professional Services for Amazon Web Services (AWS)
Aurora has highly skilled professions in AWS. We can help you save on costs and move your current datacenter from On-Premise to AWS Cloud Infrastructure. Below are what we can help you implement:

AWS INFRASTRUCTURE

- Build out your servers in the cloud to host your applications.
- Configure AWS Database connectivity for hosted applications
- Configure S3 buckets for storage

AWS AD CONNECTOR

- Build out a Domain Controller on AWS and use AWS AD
- Connector to connect your On-Premise AD to AWS Domain Controller

AWS WORKSPACES

- Desktop-as-a-Service setup which would allow your remote users to use their own Laptops or Home Desktops, and access the Desktop hosted on AWS via a client

AWS APPSTREAM

- Install applications on AWS Appstream to be accessible via an Internet Browser
- This can also be accessible via Appstream 2.0 client from anywhere

AURORA FACTS:

- Geography Covered: National
- 23 Years in Business
- Customer Segments:
  - Enterprise
  - SLED
  - Healthcare
  - Federal

EXPERIENCE:

- On-premise Active Directory integration with AWS directory and AD connector
- Experience with Virtual Desktops in AWS (Workspaces)
- Experience with EC2 instances for server infrastructure and connectivity for multiple applications and use cases (External to host web, applications, and or database services
- Transit Gateway solution to allow connectivity and communication between multiple VPCs within the native or external accounts
- AppStream 2.0 - accessing your application via a browse or desktop client. Also SAML integration with your AD infrastructure

INFRASTRUCTURE AND DATACENTER SERVICES

AURORA
PROFESSIONAL SERVICES

Windows

Microsoft Windows Server On-Prem and Cloud Services

Aurora has highly skilled professionals in Microsoft Server Infrastructure that can help you configure your On-Premise and/or Cloud Datacenter. These include but not limited to setting up:

CLOUD

- Azure Active Directory standalone or Hybrid
  - Hybrid - Syncing On-premise Active Directory to your Cloud Azure Active Director
- Microsoft Office 365 for your Emails
  - New Build or Migrating from Microsoft Exchange Server On-Prem to Office 365
  - Migrating from other email systems, like GSuite, to Office 365
    Hybrid integration for On-Prem Exchange with Office 365
- Microsoft 365 Data Loss Prevention (DLP) with Azure Information Protection (AIP)
  - Utilize Keywords and Regex for DLP policy use on Exchange Online, Sharepoint Online,OneDrive, Microsoft Teams, and Windows Endpoints
  - Utilize Exact Data Matching (EDM) for DLP Policy use on Exchange Online, Sharepoint Online, OneDrive, Microsoft Teams and Windows Endpoints
  - Utilize AIP to classify documents so that when shared, they are encrypted, blocked or allowed based on DLP Policy
- Microsoft Intune (with integration to SCCM)
  - Register devices with Intune and manage them with Security Policies which utilize SCCM for patch management
- Microsoft Azure
  - Build Windows Servers and host applications on servers in the Cloud
- Virtual Desktop/s hosted in Azure

ON-PREMISE

- Active Directory and GPOs for security and automations
  - New Build, Migrations, Upgrades
- Microsoft Exchange Server for your Mail system
  - New Build, Migrations, Upgrades
- Windows Server Update Services (WSUS) for Patch Management
  - Internet Information Services (IIS) for hosted Web Sites
- Microsoft SQL Server Build with or without Clustered Services for backend Microsoft SQL Databases
- System Center Configuration Management (SCCM) Buildout and Training in Administering
- File Shares with Distributed File System Replication (DFSR)
- DHCP and DNS

AURORA FACTS:

- Geography Covered: National
- 23 Years in Business
- Customer Segments:
  - Enterprise
  - SLED
  - Healthcare
  - Federal

EXPERIENCE:

- Over 20 years as a Windows Systems Engineer / Sr. Systems Administrator
- Over 20 years on Windows Servers
- Over 20 years on Desktop Systems
- 8 years on Microsoft Azure and Office 365
- Over 15 years on SCCM
- Over 15 years on Microsoft Exchange
- Over 20 years on WSUS / Active Directory / GPO / DNS / DHCP
- Over 15 years Scripting with Powershell and Batch