

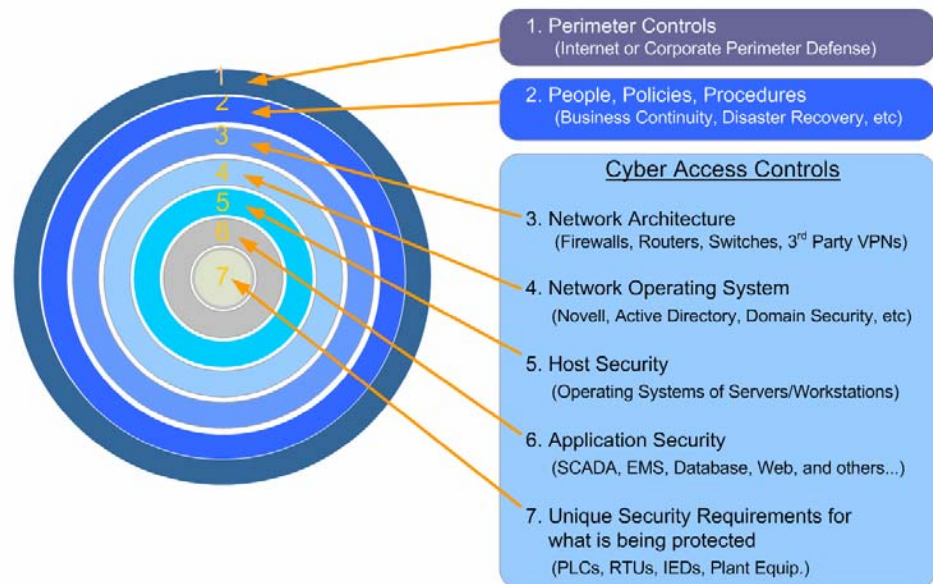


## Enterprise Security Consulting: SCADA Security Services

Securing SCADA (Supervisory Control and Data Acquisition) Systems, DCS (Distributed Control Systems), EMS (Energy Management Systems), Process Control Systems, Telecom systems, Network Management Systems, and any real-time, high-availability environment requires experienced security professionals who have years of SCADA and security experience. Our focus and dedication to the Energy, Utility, Transportation, and Critical Infrastructure sectors ensures our team has relevant experience, understands the unique needs of these industries, and can make a large impact in securing these systems without adversely impacting operations.

### 7-Layer Defense-in-Depth Approach

At the core of all of our security services is an appreciation for the various security layers that play a role in securing mission-critical real-time control systems. Each of these layers of defense represents categories of system components that must all be secured and hardened to the highest level so that each system can compensate for inherent deficiencies in the layers below it.



Each of our SCADA Security Service offerings either expose vulnerabilities in these systems, or exploit weaknesses in current defenses to show how an adversary could gain access to, and potentially take control of these environments.

- Network Architecture Review and Documentation
- Vulnerability Assessment Services
- Penetration Testing Services
- Red Team Testing
- Emergency Response and Disaster Recovery Consulting
- NERC Compliance Gap Analysis
- Critical Infrastructure Protection Training
- Cyber Forensics

## **Network Architecture Review and Documentation**

The first step in building a road map for security and regulation compliance is determining what systems are in place in our client's environments and how they are integrated. Our team can quickly document the architecture in a logical network diagram, complete with security zones for each unique environment, based on interviews with key staff on-site, or by referencing existing network maps and diagrams. Often, simply visually seeing all of the various environments, and how they are interconnected, can help point out high-level system vulnerabilities prior to running any tools on the network. This is also a critical step involved in achieving NERC compliance for those organizations in the Electric Power sector.

## **Vulnerability Assessment Services**

When faced with a possible risk in a critical infrastructure environment such as SCADA or other real-time environments, it is possible that the mitigation could turn out to be more disastrous than the risk itself, due to unforeseen system impacts. Sometimes systems, applications, or code may be so proprietary or vendor-dependent that our clients are not able to apply the necessary patches or countermeasures. Our ability to help our clients accurately identify and understand their current vulnerabilities and risks in the security of their physical, IT, and SCADA controls is based on the methodologies that we developed over a history of conducting these assessments for similar market sectors. Knowing what to look for when conducting a Vulnerability Assessment project, and making sure to cover all of the components or layers involved in securing Critical Infrastructure, is key to the success of these projects. The results and final deliverable are provided in a full report, complete with usable database data, charts and graphs, counter measure options, and business cost analysis.

## **Penetration Testing Services**

The only way to know for sure if a hacker or intruder can actually get into your network and/or facility is to actually test the vulnerabilities found in an assessment with penetration testing. Our team utilizes specialized, goal-oriented testing (such as individual systems of interest) to gain privileged access by pre-conditional means using a safe "hacker" and/or intruder methodology. This usually provides "proof of concept" of specific system vulnerabilities. Our security testers and analysts will use the same proven techniques and methodology that hackers use to gain unauthorized entry to networks and computer systems and our intrusion specialists use the same proven techniques and methodology that could be used by real world thieves, intruders, or even terrorists. The results will be provided to you in a full report complete with usable database data, charts and graphs, countermeasure options, while at the same time, posing absolutely no actual risk to your network, computer systems, physical security controls, or personnel. Penetration Testing can be done in collaboration with the client staff or covertly.

## **Red Team Testing**

While the Penetration Testing Services mentioned in the previous section can occur anywhere in the network environment, the Red Team Test is an all-out attempt to gain physical or cyber access to a critical infrastructure system from the outside, with little or no information about the target. Since critical infrastructure assets are targets for determined attackers, owners and operators of these assets should consider going beyond a structured vulnerability assessment project, and actually test their physical and cyber defenses against a focused and determined attacker. During a Red Team Test, a highly skilled team of security professionals use adversary techniques commonly used by hackers, cyber terrorists, and motivated criminals to gain

either physical or cyber access of a critical infrastructure system. Subverting a combination of physical, electronic, and cyber access controls is typically achieved through a combination of physical access subversion techniques, specialized electronic devices, social engineering, and cyber tools, with the goal of discovering as much information about a particular system as possible prior to being detected or caught. Ground Rules for these types of projects are negotiated and documented prior to project start, and our teams operate under the restraint that they can “do no harm” to any physical, electronic, or cyber systems during the Red Team Test. To get the best value from a Red Team Test, the test should be performed in a very covert manner, and no one on the inside of the IT or security teams should be alerted that this type of test is underway. Usually, the project sponsor is the only one at the client location that is aware that this test is being performed.

## **Emergency Response and Disaster Recovery Planning**

With all of the recent natural and man-made disasters that have impacted our nation’s critical infrastructure, having an Emergency Response plan in place is essential to ensure that core mission critical goals can be met while responding to unplanned events. Emergency Response planning, when coupled with Disaster Recovery planning, outlines a road map for your organization to quickly recover and restore critical operational functions after an unexpected event. These events can include potential natural, environmental, technological, and man-made threats. We use the NIST 800-30 methodology to identify most likely threat sources and create threat-pairs based on impact and risk to operations. For each risk that poses a significant impact to operations, we identify the need for a specific Emergency Response to that risk. These individual response plans are merged into a unified Emergency Response Plan that includes clear instructions for the Incident Response team to follow. The planning process is a key element that forces managers and their staff to explore viable options that can be employed in the event of an emergency or disaster. These contingencies can ultimately help to save lives, reduce property loss, as well as lessen an organization’s potential liability. The Disaster Recovery Planning work helps identify those systems that are most required for operations to continue, and what, how, and when those critical systems should be backed-up so that they can be quickly restored from tape, CD, DVD, or over-the-wire from a hot off-site location. Our team identifies each critical system (hardware, software, and network devices), and the acceptable downtime for each system. The Disaster Recovery Plan can then be tailored so that the most critical systems are restored first, thus reducing the impact to operations.

## **NERC Compliance Gap Analysis**

If your organization is responsible for planning, operating, and using the bulk electric system, then you must comply with NERC (North American Electric Reliability Council) reliability standards. To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets, NERC created and published the Urgent Action Standard 1200 that encompasses 16 topics from Cyber Security Policy (1201) through Recovery Planning (1216). The NERC Standards Drafting Team has passed Draft 3 of the new CIP Standards (CIP-002-1 through CIP-009-1), and is currently working on Draft 4. How well does your organization currently comply with either the 1200 standards or the new CIP standards? We can conduct a NERC Compliance Gap Analysis of your organization to provide very specific feedback to those areas that you will need to focus on in order to become either Substantially Compliant (SC) or Auditably Compliant (AC).

## Critical Infrastructure Protection Training

The PCIP (Professional of Critical Infrastructure Protection) certification is different than other security certifications in that it is tailored specifically to Critical Infrastructure environments. Professionals carrying the PCIP designation will have demonstrated the necessary knowledge and professional skills required for designing, maintaining, and managing security architectures as well as the extended skills required for critical infrastructure, SCADA, or other high availability environments. These skills range from security architecture design & management to highly advanced technical skills such as those used by hackers to circumvent security measures as well as countermeasure techniques all specific to these critical infrastructure, SCADA, and high availability environments. This new Critical Infrastructure Protection training and certification is made possible through the Critical Infrastructure Institute. ([www.ci-institute.org](http://www.ci-institute.org)).

## Cyber Forensics

When critical assets and systems come under attack, security professionals must be able to gather electronic evidence and utilize that evidence to bring to justice those who are responsible. Cyber forensics is the process of extracting information and data both volatile and from computer storage media and guaranteeing its accuracy and reliability. Since electronic evidence is fragile and can easily be modified, finding this data, collecting it, preserving it, and presenting it properly in a court of law is the real challenge. Additionally, cyber thieves, criminals, dishonest and even honest employees hide, wipe, disguise, cloak, encrypt and destroy evidence from storage media using a variety of freeware, shareware and commercially available utility programs. Often times such attacks are the results of multiple instances or can be just the “tip of the iceberg” of something larger. Improper handling of forensics data can destroy an entire case or bring an investigation to a halt. All data should be left completely alone except by a trained cyber forensic expert. Our team leverages the combined capabilities in Cyber Forensics and expertise with SCADA and mission-critical real-time systems to provide a uniquely qualified team of professionals who can assist in those critical moments after a cyber incident.

## Next Steps

Contact Counterpane's Professional Services group at [ps@counterpane.com](mailto:ps@counterpane.com) or 888.710.8175. We will assemble a Statement of Work with full scope and pricing detail, customized to your specific project.

### *Contact Us*

(888) 710-8175

[ps@counterpane.com](mailto:ps@counterpane.com)

[www.counterpane.com](http://www.counterpane.com)

1090A La Avenida  
Mountain View  
CA 94043  
U.S.A.

