

# Comprehensive



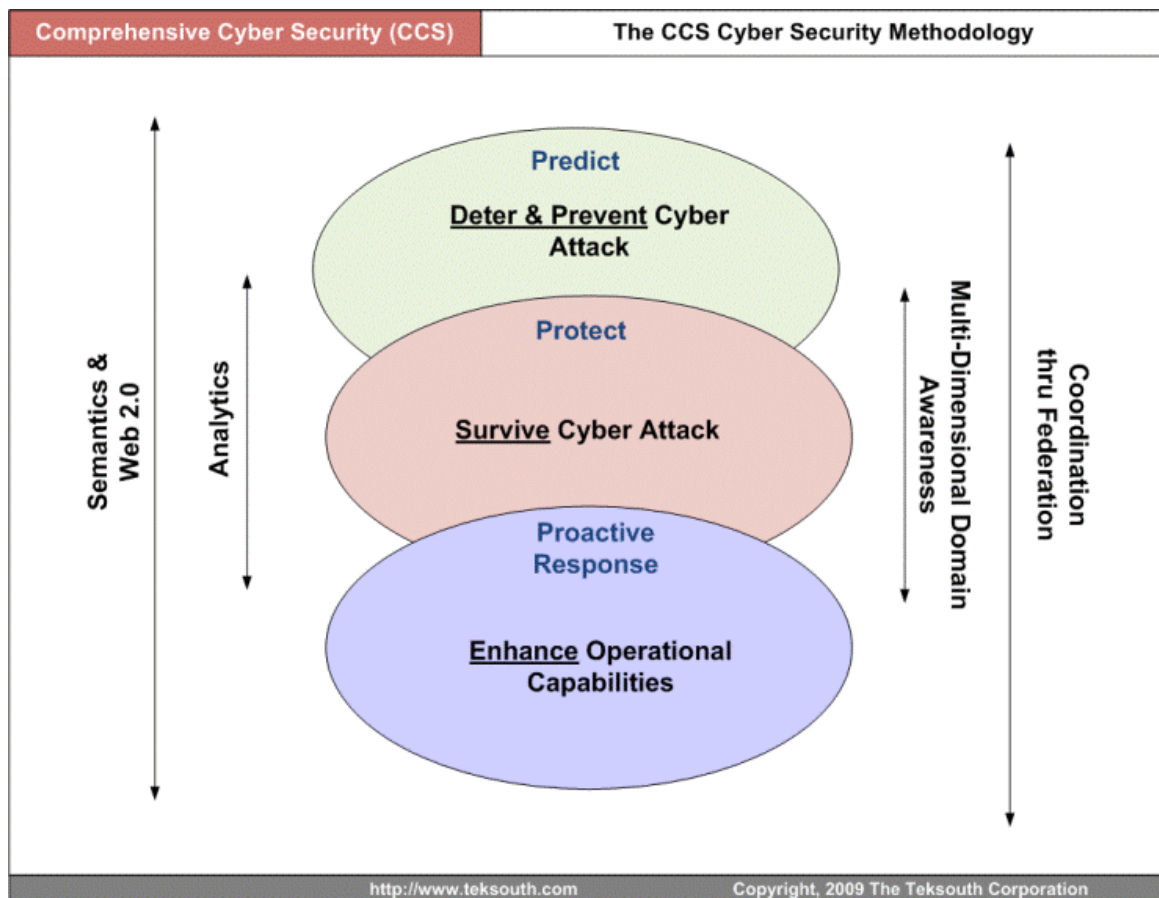
# What is CCS?

CCS is Comprehensive Cyber Security – it is a methodology, a philosophy, a set of related technical solutions and a professional IT consulting practice.

The practice of IT security has for too long been separated among functional “stovepipes,” Cyber Security is a holistic enterprise security endeavor encompassing all IT capabilities and architectures. Cyber Security is also more than a military activity – it encompasses all agencies of government as well as the entire private sector.

Most importantly, CCS represents a major departure from how current Security paradigms are viewed and managed. This paradigm shift is now being reflected in the reorganization of this nation’s Cyber defense organizations and strategies.

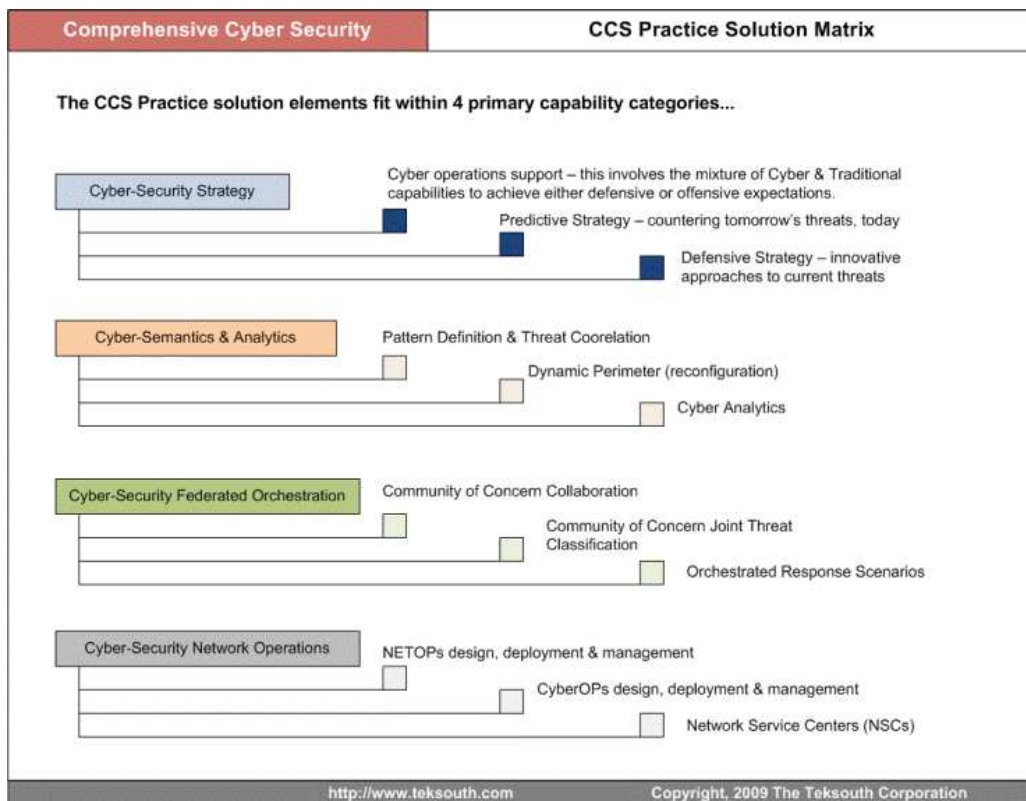
The previous paradigm for network security or Information Assurance (IA) was reactive, slow and disjointed. The future requires predictive anticipation, real-time response and complex federated management and collaboration. Our CCS solutions practice has been created to address this emerging paradigm – Utilizing the CCS practice we provide clients with both solutions engineering and implementation support for state of the art Cyber Security initiatives.



# The CCS Practice

The CCS Practice takes a holistic approach to managing all aspects of Cyber Security within a continuous and connected “Cyber Lifecycle.” Each of the following CCS Practice capabilities can be applied individually or used together for enterprise Cyber Security management and oversight.

- ❖ **Practice Capability 1 – Cyber Security Strategy & Methodology.** This provides process and lifecycle management and governance as well as dynamic, directed strategy.
- ❖ **Practice Capability 2 – Cyber Semantics & Analytics.** This capability represents the foundation for our unique technical solutions. Understanding activity patterns allows us to determine intent and respond properly to a wide variety of Cyber events.
- ❖ **Practice Capability 3 – Cyber-Security Federation & Collaboration.** Cyberspace is a community of organizations and individuals – its very nature contradicts the notion that enclaves can be effectively isolated from the larger whole.
- ❖ **Practice Capability 4 – Cyber Network Operations (NETOPS).** This is where we blend current architectures, capabilities and processes into a new approach for cyber management as well as supporting a new paradigm for Cyber Operations.



# The Cyber Challenge

Network defense and management for the past two decades has focused primarily upon reactionary responses to security breaches or “exploits.” Determining whether an attack has occurred is a forensic rather than a proactive activity.

Continuation of a reactive defense paradigm allows our adversaries to enjoy a more or less permanent offensive advantage and leaves us vulnerable to novel attacks not previously experienced and accommodated within our current defensive structures. In other words, Situation Awareness without predictive and dynamic responsive capabilities will continue to leave us relatively unprepared for the scenarios we are likely to face in the near future.

Another facet of the problem relates to the nature of Network Defense and attack as a collaborative activity. Network attack is and already has been collaborative in nature for more than a decade; however most network defense implementations are still highly segmented. This also provides a significant advantage in information sharing and freedom of action to Cyber adversaries.

This becomes particularly important when we consider the relative complexity required to support federated defensive collaboration as opposed to the relative simplicity required to mount a coordinated, distributed attack. The natural advantage again resides with our adversaries. This advantage is both technical and economic in nature, which is why Cyber attack represents perhaps the lowest cost option for asymmetric operations (i.e. the relation of the cost of organizing an attack versus the potential cost of damage inflicted).

Over the past decade, Computer and Network defense has consisted of ever-increasing levels of perimeter controls and sensors as well as identification and sharing of specific exploit “signatures.” The exploits represent specific attacks at the OS, application or network level and their signatures are derived from incident histories. While this represented a major breakthrough when it was first introduced nearly a decade ago, the incident focused perspective of network defense may now be hurting us more than helping us prepare for current and future scenarios by obscuring a larger invisible threat.

An analogy helps to place the issue in context – “while an army has specific capabilities relating to its various weapon systems, training and logistics support elements; ultimately it is an intricate combination of all factors that eventually become synthesized into specific tactics and strategies.”

Incidents or exploits detected in network attacks are but individual elements within an arsenal of Cyber-weapons or capabilities and by themselves are not as meaningful as the manner in which they may be employed or orchestrated. Incidents are in fact part of larger “Event Patterns” which may in turn be part of Cyber tactics and strategies.

# The CCS Solution:

## Part 1 – Cyber Strategy

Security has always been driven by Strategy, Operations and Tactics – Cyber Security is no different. Cyber Security encompasses “Cyberspace” not only from a traditional security management approach, but includes the emerging role of Cyber operations as well. Given the evolving nature of Cyber Security, the ability to address Cyber Strategy is the most logical place to begin providing comprehensive solutions.

The CCS Practice Cyber Strategy solution consists of the following core capabilities:

- ❖ **Application of the CCS Methodology** – to any individual environment or across federated environments. The CCS methodology is designed to coordinate previously separate Cyber “Stovepipes.”
- ❖ **Enterprise Cyber Lifecycle Management** – The CCS Methodology includes the ability to deploy and manage complex Security Lifecycle coordination both within and across organizations.
- ❖ **Enterprise Cyber Governance** – The CCS Methodology also includes program and project governance as well as the ability to govern dynamic technical solutions once deployed.
- ❖ **Cyber Doctrine** – As the arsenal of Cyber capabilities continues to grow and the complexity of Cyber Security increases, many organizations will require guiding principles upon which all other capabilities or actions will be derived from. Doctrine differs from Strategy in that it is not dynamic in nature.
- ❖ **Cyber Operational Strategy** – The day to day management of Cyber infrastructures is becoming ever more dynamic. The ability to coordinate cross domain operations requires clear definition of operational strategies. Those strategies must also be dynamic and cannot be solely reactive in nature.
- ❖ **Cyber Operational Tactics** – The key to ensuring a unified Cyber Security management solution is the ability to define dynamic Strategy & Tactics in context with one another – the tactics are more specific and subordinate to strategies which in turn are derived from doctrine.
- ❖ **Predictive Strategy** - This represents the ability to model and counter threats *before* they’re experienced.

# The CCS Solution:

## Part 2 – Semantics & Analytics

Data without meaning has no value. Data that is interpreted too late to respond to a situation has only forensic value. For too many years, computer network security and information assurance practices have focused solely on forensic capabilities. Semantics is the science of applying meaning – to symbols, to language, to data and to events. If meaning can be mastered, it can then be portrayed effectively in analytical displays. The combination of Semantic definition of the Cyber landscape with innovative analytic engines provides us for the first time with the ability to link multiple communities together in a proactive unified Cyber response, in real-time.

The CCS Practice Cyber Semantics & Analytics solution consists of the following core capabilities:

- ❖ **(Attack) Pattern Definition** – The beginning of the Semantic foundation is the collection and / or predictive definition and provision (or definition) of attack patterns.
- ❖ **Dynamic Threat Correlation** – Attack elements are correlated against patterns in real-time to help determine both the threat level as well as potential actions. This becomes a pattern matching exercise; and more importantly, one that occurs across multiple partner organizations.
- ❖ **Dynamic Incident / Event Collection** – Provides the ability to collect and synthesize attack data as attacks are occurring (for use both in immediate remediation as well as later analysis and reconfiguration)
- ❖ **Cyber COP** – COP stands for ‘Common Operating Picture.’ The ability to build this atop a Semantic foundation allows for dynamic and community views as well as comprehensive activity aggregation.
- ❖ **Cyber Enterprise Architecture (EA)** – Enterprise Architecture is the blueprint for infrastructure environments as well as the software and analytics which are housed in those infrastructures. Our Cyber EA approach is built using the same focus on Semantics – allowing for coordination from the ground up.
- ❖ **Intelligent Reporting / Cyber Health Dashboards** – One thing that has become abundantly clear over the past decade is that Cyber Security is a time sensitive activity and that traditional security analytics are painfully slow. In order to get ahead of the curve – there must be automated alerts and warnings built into our Cyber oversight mechanisms. This Cyber Health Dashboard can exist within or separate from a Common Operating Picture. The Cyber Health Dashboard allows individual security managers to catch activity real-time and then coordinate within their larger communities through collaboration to reduce the impact of the attacks.

# The CCS Solution:

## Part 3 – Federation

Cyberspace is a continuum, not a single destination. Any Security solution that does not account for the nature of Cyberspace is doomed to failure before it even begins. Cyber attacks today can consist of hundreds or even thousands of coordinated actions against thousands of specific targets – yet be focused upon a single goal. To counter the potential scope of Cyber threats now facing us, we need solutions that can manage related environments in unison or coordination with one another – this is Cyber Security Federation.

The CCS Practice Cyber Federation solution consists of the following core capabilities:

- ❖ **Development of Communities of Concern / Interest** – The COI construct has been in use now for nearly a decade – it provides a viable building block for more complex and active community structures. These structures are vital for developing federated response capabilities.
- ❖ **Dynamic Collaboration** – Today's information security often consists of one way and asynchronous communication; often times top-down directives or bottom-up incident reports. In order to mitigate attacks there must be a real-time collaboration infrastructure and conceptual framework. Dynamic collaboration is the heart of Federated Cyber Security Management. The goal is not to merely survive with a handful of disconnected networks, but rather to prevent, mitigate and repel attacks using a Federated shield.
- ❖ **Collaborative Incident / Event Collection** – There is great value in being able to collect information as it is occurring from an array of locations / networks rather than just one at a time. Only the full context of the attack potential will reveal the true nature of the threat.
- ❖ **Cyber COP Collaboration** – A Common Operation Picture is not merely an analytic platform – when done properly it is also a framework for both collaboration and lifecycle management.
- ❖ **Federated Configuration Management** – If some parts of a security Federation protect themselves and others don't then the weakest links provide entry points to enable larger Cyber disruptions. Configuration Management of NETOPS environments has always been challenging but now will become unmanageable without more sophisticated capabilities. Configuration Management needs to be both dynamic and coordinated across diverse sets of organizations / partners.
- ❖ **Collaborative Semantics** – As with COIs, the real power of our solution comes with the ability to harness the expertise of the community. This begins through community wide definitions of threats and attack patterns.
- ❖ **Response Orchestration** – Informing partners what's happening is but one step in a larger process. Response within a federation must be coordinated to thwart attacks and mitigate potential damage.

# The CCS Solution:

## Part 4 – Cyber Operations

Nearly every major IT enterprise already has an IT security infrastructure. The current security infrastructures for Network Operations (NETOPS) include the deployment of hardware and software as well as oversight by a variety of security personnel (such as network administrators and communications experts). This legacy capability is vital to any future solution – it should not be viewed as something which has to be replaced in order to achieve evolving objectives for improved security, but rather needs to be viewed as a resource to be harnessed by those new solutions.

Our solution recognizes the need to maintain and integrate these capabilities into the emerging proactive Cyber solutions of the future and to support Cyber operations.

The CCS Practice Cyber NETOPS solution consists of the following core capabilities:

- ❖ **Network Architecture & Design** – The practice of network design will undergo a radical change near-term as it is understood that every network, no matter its size, will need to take the larger community into consideration in both its structure and daily operations.
- ❖ **Network Deployment** – The ability to deploy new data centers or reconfigure existing ones.
- ❖ **Network Consolidation** – This represents one of the most pressing challenges facing large organizations today. We specialize in developing Area Processing Center (APC) and Network Service Center (NSC) consolidation constructs.
- ❖ **Network Management** – Existing networks require constant care and oversight. Even without design changes to those networks or data centers, the management processes must be modified to achieve more proactive capabilities.
- ❖ **Frequency Management** – IP networks are only one part of the much larger Cyber spectrum. Phone, mobile, broadcast and satellite infrastructures are all now very much part of Cyberspace.
- ❖ **Communications Management / IA** – The medium and the message are often thought of as different things; however in Cyberspace we must manage both. This involves the ability to manage content from a security perspective and also to ensure communications-related processes are operational within service level parameters.
- ❖ **DIB Management** – The Defense Industrial Base (DIB) is the commercial counterpart to government and military networks. Solutions that ignore impact to one sector or the other leave both vulnerable. This capability offers security coordination between connected government and commercial networks.

# The CCS Value Proposition

Cyber Security represents new challenges and new opportunities and for those reasons it requires new solution approaches . We have built our Comprehensive Cyber Security practice from the ground up in recognition of those impacts. The CCS Practice advantages include:

- ❖ **The Ability to break through Security Stovepipes** – Most providers are not used to developing federated security solutions – their vision and solutions are limited by the stovepipes they are used to managing. We've built our solution to accommodate federated environments whether they are specified in requirements or not.
- ❖ **A Proactive Security Stance** – All of our capabilities are designed to provide ever-higher levels of real time data and decision making capabilities to our clients. These capabilities are radically different from existing infrastructures and must be designed from the ground up.
- ❖ **The Ability to Leverage Legacy Capabilities within a new Solution Approach** – Our solution practice takes into account the precise steps necessary to accommodate existing infrastructure within new solution paradigms. The integration impact is understood up front – we never view new capability introduction as an afterthought.
- ❖ **A Practice Built atop Innovation** – We understand this simple truth, Cyber Security cannot become institutionalized; it must become and remain dynamic to counter evolving threats. This requires an entirely new methodology, like the one we've developed and one that will need to evolve along with Cyberspace.
- ❖ **Incorporation of Tomorrow's Technology rather than Yesterday's** – One reason that no one ever has been able to successfully anticipate or counter a new cyber threat is because traditional technologies we're not up to the task. New Semantic technology and web collaboration capabilities have opened an entirely new avenue for solution development.
- ❖ **Agility** – Being small has its advantages. Speed is one of them – not just speed in solution delivery, but agility in the nature of the solutions themselves.

For more information – contact:

Staff Ouderkirk  
The Teksouth Corporation  
1-800-842-1470  
<http://www.teksouth.com>

Joe Alt  
Sumaria Systems Inc.  
(703) 465-9193  
<http://www.sumariasystems.com>