

Cybersecurity Quarterly

Fall 2022

A Publication from  CIS Center for Internet Security®

**How Our
Members Help
Guide Us Forward
in Our Mission**

**A New
Collaboratively
Developed Guide
to Defend Against
Ransomware**

**Expert Tips and
Recommendations
to Harden
Windows Servers**

**Best Practices to
Help Stop Exploits
of PowerShell**

An Action Plan for Cyber Defense

Examining some of the most common attack patterns, issues, and challenges facing the industry, as well as concrete approaches, recommendations, and tools that can help your organization effectively solve them





Stop cyber attacks in their tracks

with **CIS Endpoint Security Services**

[Learn more](#)



Contents	Featured Articles	Members Lead the Way in the MS-ISAC	8
		How recent feedback and guidance from our members is driving future services	
		Unlocking the Windows Server Benchmark Puzzle	12
		Expert recommendations and tips for the baseline hardening of Windows Servers using the CIS Benchmarks	
		A Blueprint for Ransomware Defense Using the CIS Controls	16
		A new action plan for small and medium enterprises to defend against ransomware	
		Living Off the Land: The Power Behind PowerShell	18
		Best practices to help prevent the exploit of a common network administration tool	
		CIS Controls Enterprise Asset Management Policy Template	20
		Our new guidance to help implement an effective asset management policy	
Quarterly Regulars	Introducing the CIS Controls OSCAL Repository	22	
	Making our security best practices more machine-friendly with NIST's framework		
	Quarterly Update with John Gilligan	4	
	News Bits & Bytes	6	
	Cyberside Chat	24	
	ISAC Update	25	
	Event Calendar	26	



Fall 2022
Volume 6 Issue 3
Founded MMXVII
 Editor-in-Chief
Michael Mineconzo
 Supervising Editor
Laura MacGregor
 Copy Editors
Jay Billington
Autum Pylant

Staff Contributors
Ginger Anderson
Sean Atkinson
Paul Hoffman
Carlos Kizzee
Rylee Mowen
Robin Regnier
Valecia Stocchetti

Cybersecurity Quarterly is published and distributed in March, June, September, and December.

Published by
Center for Internet Security
 31 Tech Valley Drive
 East Greenbush, New York 12061

For questions or information concerning this publication, contact CIS at info@cisecurity.org or call 518.266.3460

Copyright © 2022 Center for Internet Security. All rights reserved.

Quarterly Update

with John Gilligan



"It is clear that many organizations are still lacking in adequate cyber defenses, leaving them open to costly attacks."

Welcome to the fall issue of *Cybersecurity Quarterly*. As we move into fall, my thoughts turn to a couple of questions: will Russia actually launch a cyber offensive against the West; what can we expect from nation states as we gear up for the mid-term elections in November; and what can we do to turn the corner against the increasing number of cyber attacks? While we have not had any broad cyber attacks like Log4j, SolarWinds, or Kaseya in the recent past, many organizations continue to be the target of ransomware and other damaging cyber threats. It is clear that many organizations are still lacking in adequate cyber defenses, leaving them open to costly attacks. Moreover, our ability to effectively counter sophisticated attacks sponsored by nation states remains uncertain at best.

The theme of this issue of *Cybersecurity Quarterly* is appropriate — Cyber Defense Strategies and Actions. In this issue, we examine the most common attack patterns, as well as approaches and tools that are effective in preventing or reducing the impact of these cyber attacks. The articles provide concrete, actionable recommendations.

Two articles in this issue discuss how to address two of the most common cyber attack patterns: ransomware and "living off the land" attacks. Valecia Stocchetti has provided an article describing a blueprint for defending against ransomware—a must read for everyone. In addition, Valecia and Ginger Anderson have provided an article that describes the new 'Living off the Land: PowerShell' guide. As the article indicates, while PowerShell is a powerful and valuable tool for task automation and configuration management, it is also difficult to secure. The recently published guide provides advice on securing PowerShell.

Ginger Anderson has also provided a piece that describes the CIS Controls Open Security Controls

Assessment Language (OSCAL) Repository. This OSCAL repository provides a more machine-friendly version of CIS Controls v8 for those who want to leverage tools to assist in implementation and assessment of Controls. The team from the CIS Security Best Practices (SBP) organization has also authored an article in this issue that outlines our Controls Enterprise Asset Management Policy Template.

The MS-ISAC and the EI-ISAC recently hosted their annual conference. After a break due to COVID, the annual conference resumed this year in Baltimore, Maryland with a very strong attendance of over 600 members, as well as a number of staff, vendors, and industry partners. Carlos Kizzee's article in this issue summarizes the feedback from state, local, tribal, and territorial attendees of the conference, highlighting the expressed cybersecurity needs and issues. Not surprisingly, a focus on the challenges and needs of smaller government organizations is a consistent recurring theme. Also in this issue, CalCom, a CIS SecureSuite Product Vendor, describes the challenges and practical strategies for hardening Windows Servers using the CIS Benchmarks.

Finally, our CISO, Sean Atkinson has provided his regular column. This quarter, he focuses on developing and implementing an effective cyber defense strategy.

I hope that you enjoy this quarter's issue, and I hope you have a great fall!

Best Regards,

John M. Gilligan
President & Chief Executive Officer
Center for Internet Security



GET UP TO 20% OFF
new Memberships
through October 2022

Save now! Use code **CYBER2022** at
<https://enroll.cisecurity.org/memberships/>

Scale your cybersecurity program with ease.

Get tools to help your program grow
as your business grows.



CIS SecureSuite[®]
Membership



CIS


News Bits & Bytes

October is Cybersecurity Awareness Month.

Now in its 19th year, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) lead the collaborative effort and dedicate every October to creating resources for organizations to talk to their employees and customers about staying safe online. This year's theme is "See Yourself in Cyber," and will focus on the "people" part of cybersecurity. CISA and NCA will be providing information and resources to help educate the public and ensure all individuals and organizations make smart decisions whether on the job, at home, or at school – now and in the future. Check out ways you can participate and support Cybersecurity Awareness Month on [CISA](#) and [NCA's](#) websites.



The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) has published the *Essential Guide to Election Security*, just in time

 **for the 2022 midterm elections.** Over 25 organizations volunteered to help provide input on the *Essential Guide*, which includes actionable guidance that supports election offices and their resources. Not all election offices have the same resources or capabilities, which is why the *Essential Guide* includes three different maturity levels, allowing everyone from beginners to experts to find guidance that fits their jurisdictions to protect against real-world attacks. The *Essential Guide* can be accessed on [GitHub](#).

CIS and Aqua Security together have released the first formal guidelines for software supply chain security.

The *Software Supply Chain Security Guide* provides more than 100 foundational recommendations. Along with the guide, Aqua has released a new open-source tool called [Chain-Bench](#) for auditing the software supply chain to comply with these new guidelines. The guide establishes general best practices that



support key emerging standards while adding foundational recommendations for setting and auditing configurations on CIS Benchmark-supported platforms. CIS and Aqua hope to build a community interested in furthering the development of platform-specific benchmark guidance. The *Guide* is available for download on [CIS WorkBench](#). If you'd like to contribute to this or other CIS Benchmarks projects, please contact the [CIS Benchmarks Development Team](#).

Does your organization have "non-domain-joined," "stand-alone," or "workgroup" systems? If so, you aren't easily able to apply our current Windows

 **CIS Benchmarks™** 10 Benchmark, which is made for domain-joined

systems. **We've answered your requests and produced a stand-alone CIS Microsoft Windows 10 Benchmark that applies to all build versions of the Windows 10 OS**, including older versions. We made several changes in this new Benchmark that differentiates its content from our existing Windows 10 coverage, and provided detailed guidance on how to apply the CIS Build Kit utilizing Microsoft's Local Group Policy Object (LGPO) tool, which is made specifically for non-domain-joined systems. Download the new Benchmark [here](#).

The government of Puerto Rico has partnered with the Multi-State Information Sharing and Analysis Center (MS-ISAC) on a new \$7.6 million initiative aimed at strengthening cybersecurity measures in government agencies across the island.



The program includes building out a security operations center at the Puerto Rico Innovation and Technology Service (PRITS) and implementing protective services provided by the MS-ISAC. The new plan centralizes the entire island's cybersecurity with PRITS and serves as a model for what other U.S. states and territories can do to secure government systems and information through "whole-of-state" policies. Read more about the initiative on [StateScoop](#).

A Partnership for State, Provincial, Local, Tribal, and Territorial Government

The SANS Institute and Center for Internet Security Partnership Program

Improving Your Security Posture

Cyberthreats appear as fast as a mouse click in today's environment. Your best defense is an educated workforce. Eligible organizations use this Partnership Program to allocate technical cybersecurity and security awareness training to their employees, taking advantage of highly discounted rates on superior training to protect national security.

Special Offer:

For a limited time, save more than 50% when you purchase SANS technical and security awareness training through our partnership purchase windows. Special discounts are available:

Winter Program:
December 1 – January 31

Summer Program:
June 1 – July 31

Make a positive impact on your cybersecurity protection. Get the training you need at an affordable cost.

SANS SECURITY AWARENESS

Technical training is a critical component for adoption of core security awareness concepts. Compliance and behavior change becomes difficult for non-technical individuals without the proper content. SANS Security Awareness offers a comprehensive solution for end users and individuals of all levels with expert-authored content. Created by a trusted global network of cybersecurity professionals, this Partnership Program includes several key Security Awareness products:

- **End User** - Comprehensive security awareness training for all computer users based on the Critical Security Controls
- **Healthcare** - Computer-based security awareness training tailored to healthcare organizations
- **Developer** - Train your developers in secure coding techniques and how to recognize current threat vectors in web applications
- **ICS Engineer** - Rigorous computer-based training for those interacting or operating with Industrial Control Systems
- **Phishing** - Test your employees through phishing simulations consistent with real-world attacks
- **CIP** - Relevant training addresses NERC CIP reliability standards for the utility industry

A Smart Approach to Security Awareness and Training
www.sans.org/partnerships/cis

Members Lead the Way in the MS-ISAC



How do the MS- and EI-ISACs decide on what services, educational efforts, and other opportunities to offer next? It all comes back to the members they serve.

By Carlos Kizzee

The MS-ISAC and EI-ISAC held our 15th Annual ISAC Meeting this year, bringing over 600 attendees from our member state, local, tribal, and territorial (SLTT) government entities, along with numerous partners in the industry, together to experience 20 hours of instruction and best practices, as well as countless hours of valuable networking. This year's ISAC Annual Meeting was the first gathering since the two-year hiatus due to COVID-19 and provided over 50 high-quality sessions covering high-interest, contemporary cybersecurity topics developed based on input from those attending. Preparations for the Annual Meeting included communication with our membership to identify and prioritize areas of

The feedback and guidance that we have received from our members is exceptionally valuable to us and will help guide our upcoming ISAC Monthly Meetings, future webinar sessions and series, and our 2023 Annual Meeting... Stay tuned to see your feedback in action in our continuing security best practices and whole-of-state governance webinar series.



member interest, which helped drive agenda development. We heard our members, and we are still listening!

During our Annual Meeting, we solicited feedback on the event and the quality of the session content. Following the ISAC Annual Meeting, we also surveyed all of our attendees. The feedback and guidance that we have received from our members is exceptionally valuable to us and will help guide our upcoming ISAC Monthly Meetings, future webinar sessions and series, and our 2023 Annual Meeting, scheduled for August 6 – 9 in Salt Lake

City. Stay tuned to see your feedback in action in our continuing security best practices and whole-of-state governance webinar series.

What are some things we're hearing that might be of interest to you as well? I'm glad you asked!

Members seem to be collectively resonating with our efforts to inform and collaborate around the State and Local Cybersecurity Grant Program, so you can expect to see more opportunities to learn and share around that topic. Since the law was signed authorizing that grant program, the MS-ISAC has been holding monthly sessions on how states are preparing for that grant program, including specific best practices from various states that others can emulate. The MS-ISAC has also initiated bi-weekly grant focus groups with state CISOs/SAs to assist with the sharing of best practices, has developed a foundational assessment for ease of determining capabilities in this first year of the grant, and is developing a matrix aligning CIS/MS-ISAC service offerings to the required elements in the grant.

As an update on that grant program, the [Notice of Funding Opportunity \(NOFO\)](#) for the first year of the multi-year State and Local Cybersecurity Grant Program was released September 16, 2022. Funds are awarded based on a formula of baseline



Our involvement and assistance to our members in this first-of-its-kind federal grant program for state cybersecurity interests is a direct outcome of member input, enabling us to focus as an ISAC on what matters most to the membership.

minimums and population, with allocations for each state or territory outlined in the NOFO. The 56 states and territories have until November 15, 2022, at 5 p.m. to apply for their funding. While local governments are not eligible to apply to the federal government for the funds, the program stipulates that 80% of the federal funding must be passed through to the locals, including at least 25% to rural areas. This pass through may be in the form of items, services, capabilities, or activities that have a broader statewide impact and may more effectively reduce cybersecurity risk when managed at the statewide level. States are required to form a Cybersecurity Planning Committee that must include local government representatives. This Committee will be charged with developing and refining the statewide Cybersecurity Plan and making decisions regarding funding. Awards are anticipated to be made no later than December 31, 2022. It is anticipated that much of the first-year funding will go toward development of cybersecurity plans and capability assessments across the state. Additional guidance on how to apply as a sub-recipient of the grant should be forthcoming from your [State Administrative Agency](#). Our involvement and assistance to our members in this first-of-its-kind federal grant program for state cybersecurity interests is a direct outcome of member input, enabling us to focus as an ISAC on what matters most to the membership.

Beyond member interest in that grant program, we have noticed increasing interest among our membership in getting exposure to peer use cases and solutions. How are other peer SLTT entities leveraging MS-ISAC, CIS, or CISA services and capabilities? How are they managing the vetting and selection of vendors and evaluating their

performance and value? What novel content are they placing in the policy and governance documentation that they are developing? What are emerging best practices that they have identified and applied that they can share so others can learn and avoid common mistakes? We have witnessed the most demand for this information in areas like cloud adoption, controls implementation, and security awareness.

We also heard from our members that a prime value of the ISAC Annual Meeting and our other webinars and collaborative activities is the opportunity to come together in key segments (like K-12 entities, or CISOs connecting with one another) or around key topics of interest (like ransomware or Zero Trust). We noticed continued interest in increased opportunities for peer-to-peer engagement and best practice sessions with peer or topical segmentation and are looking to continue our development for sessions and events like these, including regional workshop events to help reduce travel cost and time.

One final element of feedback that we heard from our members is the value of the ISAC Annual Meeting as an opportunity to actively network and participate with peer organizations. Of everyone surveyed, 99% noted that they would recommend attending the ISAC Annual Meeting. This included many who also indicated that if there were other conflicting meetings, or when budget limitations limit their attendance at conferences and events, the ISAC Annual Meeting is at the top of the stack in their budget and travel planning.

We couldn't be more proud of our vibrant MS- and EI-ISAC community and are excited to continue to develop it to meet members' cybersecurity needs and interests.

We couldn't be more proud of our vibrant MS- and EI-ISAC community and are excited to continue to develop it to meet members' cybersecurity needs and interests. We pledge to maintain our habit of actively gathering member feedback and using that input to focus on and deliver what matters most to our ISAC community.

Carlos P. Kizzee is the CIS Senior Vice President for Stakeholder Engagement Operations. In that position, Kizzee is accountable for the engagement, account management, and training and education activities associated with MS-ISAC membership as well as key programs assessing and enhancing the security maturity of state, local, tribal, and territorial government agencies and activities. Previously, Kizzee served with the Retail & Hospitality Information Sharing and Analysis Center (RH-ISAC) as Vice President of Intelligence, building and supporting retail and hospitality industry security collaboration; and with Defense Security Information Exchange as Executive Director, promoting threat intelligence sharing and collaboration within the defense industrial base and actively supporting the development and establishment of the National Defense ISAC.





Advanced Threats. Maximum Protection.

Ensure users and devices can safely connect from
anywhere, with industry-leading protection.

Proactively identify, block, and mitigate targeted threats,
including zero-day attacks, malware, and phishing.

[See Why >](#)

carahsoft The Trusted Government
IT Solutions Provider

Unlocking the Windows Server Benchmark Puzzle



As organizations look to improve their cybersecurity, those leading security awareness efforts must adapt to ensure staff has the knowledge to avoid potential attacks

By Dvir Goren

Organizations have a set of configuration standards and industry best practices to harden their digital configurations in the CIS Benchmarks. These configuration guidelines are set and developed by the Center for Internet Security (CIS) with their global community of IT security experts, and can be used to measure the effectiveness and efficiency of organizational cybersecurity policies and practices. With IT infrastructure being so complex, multiple dependencies need to be configured with these best practices in mind. The technical task of hardening an organization's servers to comply with comprehensive security policies is an involved process that is very time-consuming.

The gap between Security and IT/DevOps teams is a significant pain point for many organizations. IT

With IT infrastructure being so complex, multiple dependencies need to be configured with these best practices in mind. The technical task of hardening an organization's servers to comply with comprehensive security policies is an involved process that is very time-consuming.

and Security teams have a fundamental conflict of interest that stems from differing objectives and KPIs. The Security team must protect and monitor every asset, server, desktop, and device using best practices and strict standards, and devise the policy and strategy for securing and hardening the organization's assets. Server hardening includes a set of security configurations that need to be changed to create a robust security baseline, and it is the IT team's responsibility to actually perform the work. Therefore, collaboration between the teams is crucial for the organization's success.

A survey conducted by CalCom Software asking IT teams from over 100 enterprise organizations to offer their top three reasons for inadequate baseline hardening said:

Testing: Implementing a server security policy requires changing server configuration settings to meet policy requirements. Applying the policy directly to production systems can often damage or break server operations and applications. In order to generate an impact analysis report detailing how the policy will affect production, a test environment will need to be built. Setting up a test environment to perfectly simulate each policy on a server that is running different operating systems versions, roles, and applications, all at the same time, is near impossible.

Configuration Drift: A drift from the baseline that goes unnoticed can expose the organization to configuration vulnerabilities, and failure to identify and correct the cause means lost productivity and downtime.

Policy Monitoring and Reporting: Ongoing monitoring of the baseline is required to keep a record of the multiple environments, their compliance scores, and audit results. With the production environment constantly changing, new vulnerabilities are often found. Logging information about what changes were made, where, and when is crucial and often not done.

Process of Implementing Windows Benchmarks

While Windows Server is the backbone of many IT infrastructures, it is the Windows System administrator's responsibility to deploy technology, maintain services, and ensure computing uptime for the organization quickly and flexibly. Manually implementing CIS Benchmarks for Windows Servers to meet the best practice standards is resource-intensive and time-consuming. Benchmarks vary according to different Windows versions, and also differences between member servers and domain controllers and other Windows roles and applications servers. A Benchmark can include 1,000+ pages with hundreds of objects to address. To better understand the implementation, let's review the process:



Production Environment When Implementing a Windows Server Benchmark

The only way to avoid outages once the Windows Server Benchmark is implemented is to thoroughly research the potential impact of the configuration setting change on server operations. This impact analysis typically requires testing in a lab environment that has been set up to replicate the production environment.

Deployment Location of the Benchmark

Once the Windows Server Benchmark has been tested, it will then need to be managed. In an optimal situation, the Benchmark would be managed in a centralized location, making it easier to properly configure and manage updates. Because there is no "one" Windows baseline, but multiple ones that are differentiated by the Windows Server version and role, GPOs can't enforce granular policies for every server and intensive work needs to be performed.

Monitoring the Benchmark

When a Benchmark is added and there is a modification to the server's applications, there are also infrastructure changes. Constant monitoring of the Benchmark once implemented requires a lot of time and effort to prevent configuration drifts and vulnerabilities.

System Administrator Challenges When Implementing Benchmarks

System Administrators have the very laborious job of continually implementing Windows Server Benchmarks according to the given recommendations. For a single Benchmark implementation, dozens of pages must be read and a vast amount of research must be done before applying it to production. If done manually, aligning the existing assets to relevant Benchmarks while making sure that they remain compliant with the recommended Benchmark standard can take years.

As of today, the CIS Benchmarks introduce about 474 security settings recommended to include

as a baseline for Windows Servers. Imagine having to manually configure 100 servers or more with the Windows operating system in an organizational environment. Managing all of them means configuring and performing checks on almost 50,000 configurations, and those are only the configurations of the operating system. Other system configurations such as IIS and SQL also need to be managed, and this adds up to thousands of actions and decisions which makes it incredibly demanding and time-consuming.

How to Become Audit Ready

Windows is a complex operating system with many subsystems and features. This complexity makes it difficult to identify which metrics and workloads are most important to measure. Also, the Windows codebase is constantly changing, which can invalidate existing implemented Benchmarks and requires considerable effort to keep them up-to-date. IT leaders recognize the advantages of automation and look to solution providers such as CalCom Software to automate the impact analysis process, reduce the occurrence of change-related outages, and provide a framework for maintaining an effective security posture after implementation.

Our advice to anyone beginning a hardening project is to carefully review the hardening management platform. Be sure that it's capable of providing a drill down to a single server so that the security policy can cascade to all servers based on role and applications installed. Avoid wasting time and choose a solution that eliminates the cost of creating

As of today, the CIS Benchmarks introduce about 474 security settings recommended to include as a baseline for Windows Servers. Imagine having to manually configure 100 servers or more with the Windows operating system in an organizational environment.

lab environments for simulating the impact of security policies on servers. Save your department's resources by using a solution that analyzes the direct impact of your policy on the production environment and gives you real-time data.

Dvir Goren is the Chief Technology Officer at CalCom and is a veteran of the IT industry with over 25 years of experience in system, security, and Microsoft infrastructures. Goren has been managing complex hardening projects for over 15 years and is considered a thought leader in his field. Goren also leads CalCom's product team, including developing the product strategy and road map.





BASELINE HARDENING AUTOMATION MADE SIMPLE

Configuration changes to reduce
The attack surface while keeping
Your operations intact

GET STARTED >

www.calcomsoftware.com

A Blueprint for Ransomware Defense Using the CIS Controls



CIS and other like-minded industry stakeholders have collaborated to create a definitive action plan for small and medium enterprises to defend against ransomware

By Valecia Stocchetti

If the past few years are any indication, ransomware attacks aren't going away anytime soon. In a 2022 report, [SonicWall](#) revealed that it had detected more than 623 million ransomware attacks over the course of 2021 – an increase of 105% over the previous year. By comparison, it observed just 188 million ransomware attacks back in 2019. This means that ransomware detections more than tripled in the span of three years.

These findings don't bode well for disaster recovery and business continuity, as many enterprises are already struggling in the wake of a ransomware

In a 2022 report, SonicWall revealed that it had detected more than 623 million ransomware attacks over the course of 2021 – an increase of 105% over the previous year. By comparison, it observed just 188 million ransomware attacks back in 2019. This means that ransomware detections more than tripled in the span of three years.

infection. Such challenges extend beyond the reputational and economic costs that take shape in an attack's immediate aftermath. There's also what the [Cybersecurity & Infrastructure Security Agency](#) (CISA) calls the "extended recovery" challenge. Here, enterprises might prioritize backing up their data without doing the same for their software, components, and dependencies, noted [CSO](#). This can further amplify disruption resulting from a ransomware attack.

A Shift in Approach

Whether your enterprise is big or small, you can't afford to take a passive approach to ransomware. The ensuing recovery process might entail additional financial and operational damages. To overcome this obstacle, you need to shift to active ransomware defense using a comprehensive framework.

That's the logic behind a recent initiative from the Ransomware Task Force (RTF), which consists of more than 60 members spanning across several sectors including government, law enforcement, nonprofits, and other institutions. Over the last year, members of the initial RTF partnered with CIS, among other industry organizations, to form the Blueprint for Ransomware Defense Working Group. The purpose of the Working Group is to "develop a clear, actionable, framework for ransomware

mitigation, response, and recovery” as part of Action 3.1.1 from the [Ransomware Task Force Report](#).

We are pleased to announce the Working Group’s release of the *Blueprint for Ransomware Defense*. It is comprised of a subset of [Implementation Group 1 \(IG1\) Safeguards](#) from the [CIS Critical Security Controls \(CIS Controls\) v8](#).

Ransomware Defense for Most U.S. Businesses

Our audience for the *Blueprint* focuses on one group in particular – small- to medium-sized enterprises (SMEs). According to the [U.S. Small Business Administration’s Office of Advocacy](#), there are over 32.5 million small businesses in the United States, a number which makes up 99.9% of all U.S. businesses. These enterprises face unique challenges when it comes to establishing cybersecurity best practices, as they are often overwhelmed and understaffed. For many, it is difficult to know where to start.

The *Blueprint* provides a set of 40 Foundational and Actionable Safeguards from IG1 that will assist with ransomware defense while considering those SMEs that have limited cybersecurity expertise. As many IG1 Safeguards are foundational and process-oriented, they are often required to successfully implement additional actionable (e.g., technical) Safeguards.

The Working Group prioritized these Safeguards based on their value in combatting ransomware using analysis from the [CIS Community Defense Model](#). The *Blueprint for Ransomware Defense* also aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), focusing on the framework’s five Security Functions – Identify, Protect, Detect, Respond, and Recover – to help enterprises prioritize their efforts to determine a starting point in developing ransomware defenses.

Strategic Ransomware Protection

SMEs who implement the *Blueprint* will be well-positioned to defend against ransomware, enforcing the value of a relatively small number of well-chosen defensive steps. As a result, SMEs should start with CIS Safeguards from IG1 in



the *Blueprint* to obtain the highest value and work up to the other IGs, as appropriate.

The *Blueprint for Ransomware Defense* is available for download from the [Institute for Security and Technology](#), the organization that created the Ransomware Task Force, at <https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf>.

Valecia Stocchetti is a Senior Cybersecurity Engineer for the Center for Internet Security (CIS). Stocchetti came to CIS from the eCommerce field, where she worked complex financial fraud cases. She is a graduate of the University of Albany with a degree in Digital Forensics. Prior to joining the CIS Controls team, Stocchetti worked in the MS- and EI-ISAC Computer Emergency Response Team (CERT), where she managed CERT and spearheaded multiple forensic investigations and incident response engagements. In her current role, she works with various attack models and data, including the MITRE Enterprise ATT&CK framework, to help validate and prioritize the CIS Controls. Stocchetti holds many certifications, including GIAC Certified Forensic Examiner (GCFE), GIAC Certified Forensic Analyst (GCFA), and GIAC Security Essentials Certification (GSEC).

Living Off the Land: The Power Behind PowerShell



Our new guide to help mitigate and defend against the exploitation of a commonly used network administration tool for nefarious purposes

By Ginger Anderson and Valecia Stocchetti

PowerShell is a powerful tool used for task automation and configuration management that is built on the .NET framework. This robust tool helps IT professionals automate a range of tedious and time-consuming administrative tasks, as well as find, filter, and export information about a system on a network through combining commands, called cmdlets, and creating scripts. It is also a utility that is often abused by cyber threat actors (CTAs) using [Living off the Land](#) (LotL) techniques. As far back as 2016, for instance, at least 38% of observed incidents by [Carbon Black](#) and partners included PowerShell as part of the attack. The majority (approximately 87%) of those attacks used PowerShell in commodity malware such as click fraud, fake anti-virus, and opportunistic malware. Fast forward to more recent times, and we find that approximately 49% of threats analyzed in 2021 used PowerShell in the attack chain, according to [Red Canary](#).

Ultimately, CTAs can use PowerShell in several ways to achieve a variety of objectives. For example, as PowerShell is a native Windows tool and functional on other operating systems, CTAs are able to use it without raising red flags and thus evade traditional network defenses. Additionally, CTAs can use post-exploitation frameworks that leverage PowerShell components to compromise a network and steal credentials. PowerShell also allows CTAs to automate activities, escalate privileges, and move

As far back as 2016, for instance, at least 38% of observed incidents by Carbon Black and partners included PowerShell as part of the attack... Fast forward to more recent times, and we find that approximately 49% of threats analyzed in 2021 used PowerShell in the attack chain, according to Red Canary.

laterally throughout a network – all increasing the attack surface and wreaking havoc on the enterprise.

Defending Against PowerShell Attacks

Unfortunately, simply blocking the PowerShell executable is not a viable solution, nor is it effective. PowerShell can be invoked in a number of ways without using the actual executable – and it is often used this way. Additionally, a number of legitimate applications use PowerShell to perform everyday business functions. A more strategic and multi-faceted approach is therefore necessary to secure against an attack using PowerShell.

Fortunately, the Center for Internet Security (CIS) is already in the process of publishing guides that address common LotL attack vectors. Our guides provide prioritized best practice guidance to address some of the most commonly used vectors and exploited protocols to conduct attacks. Some of our most recent guides focus on [Remote Desktop Protocol](#) (RDP), [Server Message Block](#) (SMB), and [Windows Management Instrumentation](#) (WMI), for example.

Our newest guide, *Living off the Land: PowerShell*, is next in the series of LotL guides. It covers the use of this legitimate network administration tool in cyber attacks and provides guidance to defenders on how they can protect against a PowerShell-based attack. Toward that end, it introduces related CIS Critical Security Controls (CIS Controls), CIS Benchmarks, and MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) (Sub-)Techniques.

A Stronger Cybersecurity Posture

Ultimately, it is important to implement defensive processes and measures such as understanding and managing your PowerShell environment, securely configuring PowerShell, malware defenses, logging, continuous vulnerability management, email and browser protections, and security and awareness training. By implementing the recommendations introduced in *Living off the Land: PowerShell*, enterprises can confidently strengthen their cybersecurity posture while protecting their assets.

Living off the Land: PowerShell is available for download from the CIS website at <https://www.cisecurity.org/insights/white-papers/living-off-the-land-powershell>.



By implementing the recommendations introduced in *Living off the Land: PowerShell*, enterprises can confidently strengthen their cybersecurity posture while protecting their assets.

Ginger Anderson is a Senior Cybersecurity Engineer for the Center for Internet Security (CIS). In her current role, she is project owner on the Security Best Practices team, leading the following initiatives: Information Modeling, Controls Assessment Specification, OSCAL Repository, and editor of Living Off the Land guides. She previously led the Cyber Threat Intelligence team as well as the Federal Liaison Program for the MS- and EI-ISAC. Anderson started her career as an enlisted intelligence analyst with the U.S. Army and later as a commissioned intelligence officer. She has additionally supported the FBI and U.S. Department of Homeland Security in the cyber space. She holds B.S. in Systems Engineering from the United States Military Academy, a M.S. in Geospatial Analysis from Pennsylvania State University, and is working towards a Ph.D. in Data Science through the University of Maryland.

Valecia Stocchetti is a Senior Cybersecurity Engineer for the Center for Internet Security (CIS). Stocchetti came to CIS from the eCommerce field, where she worked complex financial fraud cases. She is a graduate of the University of Albany with a degree in Digital Forensics. Prior to joining the CIS Controls team, Stocchetti worked in the MS- and EI-ISAC Computer Emergency Response Team (CERT), where she managed CERT and spearheaded multiple forensic investigations and incident response engagements. In her current role, she works with various attack models and data, including the MITRE Enterprise ATT&CK framework, to help validate and prioritize the CIS Controls. Stocchetti holds many certifications, including GIAC Certified Forensic Examiner (GCFE), GIAC Certified Forensic Analyst (GCFA), and GIAC Security Essentials Certification (GSEC).

CIS Controls Enterprise Asset Management Policy Template



Our new resource to help enterprises implement an effective and comprehensive asset management policy based on our security best practices

By Robin Regnier

When implementing a security framework, many security controls often start with creating a policy. This allows an enterprise to have a document to work off of, have a reference to look back on, and create an avenue to enforce the policy. After all, it is difficult to enforce a policy that is not written down.

In this way, information security policies are the cornerstone of a cybersecurity program. But they are rarely one large document that covers multiple topics. Instead, they oftentimes represent a large collection of individual documents. Additionally, many security frameworks recommend or require different types of policies to be created, implemented, and enforced within an enterprise.



In this way, information security policies are the cornerstone of a cybersecurity program. But they are rarely one large document that covers multiple topics. Instead, they oftentimes represent a large collection of individual documents.

Enterprise Asset Management as a Starting Place

The CIS Critical Security Controls (CIS Controls) recommend several policies that an enterprise should have in place. The first of many policies we are working on, *Enterprise Asset Management Policy*, is meant as a “jumping off point” for enterprises that need help drafting their own enterprise asset management policy.

Enterprise asset management is the process of procuring, identifying, tracking, maintaining, and disposing of an asset owned by an enterprise. These assets can consist of end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers that exist in virtual, cloud-based, or physical environments, including those

that can be connected to remotely. Enterprise asset management is a difficult problem for an enterprise of any size, as managing all these assets can often be a struggle. New assets are constantly acquired, others are retired, and many others are simply lost. With work from home becoming more prominent, enterprise assets may also disappear from the main enterprise network, only to reappear months later or never again. Additionally, there are multiple types of enterprise assets that often need to be managed differently. Such dynamism highlights the need for a formalized way of managing enterprise assets.

How To Use the Policy

To implement an effective enterprise asset management process, enterprises should build a solid foundation which starts with a good, working policy. They can choose to create their policy on their own. Alternatively, they can use a policy template to streamline the process.

Our policy template, *Enterprise Asset Management Policy*, is meant to supplement the CIS Controls v8. The policy statements included within this document can be used by all CIS Implementation Groups (IGs), but they are specifically geared towards Safeguards in IG1. IG1, commonly referred to as [essential cyber hygiene](#), represents a minimum standard of information security for all enterprises. It is a recommended starting point for creating an asset management policy for an enterprise of any

To implement an effective enterprise asset management process, enterprises should build a solid foundation which starts with a good, working policy.

size. In particular, it uses Safeguards 1.1 and 1.2 of CIS Control 1: Inventory and Control of Enterprise Assets to create an enterprise asset management policy template. IT and security professionals can use this resource to visualize and streamline the enterprise asset lifecycle in their workplace.

Future versions of this template will expand the scope to both IG2 and IG3 Safeguards.

Looking to get a head start on creating policy templates for your enterprise? Download the *Enterprise Asset Management Policy* today by visiting <https://www.cisecurity.org/insights/white-papers/enterprise-asset-management-policy-template>.

Robin Regnier serves as the Controls Coordinator on the Security Best Practices team for the Center for Internet Security (CIS). In this role, she serves as project coordinator for the team dedicated to the development of the CIS Critical Security Controls (CIS Controls), promotes and furthers the adoption of the CIS Controls, and actively outreaches to CIS's global community of volunteers and adopters to facilitate the continuous development and updating of CIS's security guidance.



Introducing the CIS Controls OSCAL Repository



To help organizations using our best practices automate their security processes, CIS has released a machine-readable version of the CIS Controls

By Ginger Anderson

You have asked, and we have answered! We have created a more machine-friendly version of the CIS Controls v8 document by using the Open Security Controls Assessment Language (OSCAL) Framework, and we have posted it in our new GitHub repository: [the Center for Internet Security \(CIS\) Critical Security Controls \(CIS Controls\) OSCAL Repository](#). The repository contains OSCAL serializations of the CIS Controls; it will include a variety of OSCAL Catalogs for the main CIS Controls v8 document, CIS Controls Assessment Specification, and mapping documents.

A Shift in Approach

OSCAL was developed by [NIST](#), in collaboration with others in the industry, as a standardized, data-centric framework that can be applied to an information system for documenting and assessing its security controls. OSCAL aims to address a number of complicating factors faced by information system security professionals today.

Today, security controls and control baselines are represented in proprietary formats, requiring data conversion and manual effort to describe their implementation. Rarely does an enterprise only need to comply with a single security framework. They often need to comply with multiple regulatory standards and frameworks, which constantly change over time, can overlap in scope,

OSCAL was developed by NIST, in collaboration with others in the industry, as a standardized, data-centric framework that can be applied to an information system for documenting and assessing its security controls. OSCAL aims to address a number of complicating factors faced by information system security professionals today.

and often conflict or can be difficult to manage together. Additionally, enterprises often must apply and assess these control implementations across information systems that only continue to increase in size and complexity, especially as more enterprises move toward the cloud.

In order to properly assess and address information security and privacy risks, the implementation of selected controls on an enterprise's systems needs to be verified and shown to be effective. To assure a system's security and privacy posture, its control implementation must be both correctly described, assessed, and authorized. These tasks are resource-

intensive, and, given their complexity, are often challenging to perform within budget constraints.

An important goal of OSCAL is to move the security controls and control baselines from a text-based and manual approach (using word processors or spreadsheets) to a set of standardized and machine-readable formats such as XML, JSON, and YAML. With systems security information such as control catalogs, control baselines, system security plans, and assessment plans and results represented in OSCAL, security professionals can begin moving toward potential automation of their security assessment, auditing, and continuous monitoring processes.

The standardized formats provided by the OSCAL project help to streamline and standardize the processes of documenting, implementing, and assessing security controls, such as those contained in the CIS Controls. The automation enabled by these formats reduces complexity, decreases implementation costs, and enables the simultaneous, continuous assessment of a system's security against multiple sets of requirements.

A Work in Progress

Much of the CIS Controls resources are developed with the help of our global volunteer army of information security experts. As such, CIS invites you to please join and help us to continue to develop our OSCAL effort. We value your input on this important work in progress.



Much of the CIS Controls resources are developed with the help of our global volunteer army of information security experts. As such, CIS invites you to please join and help us to continue to develop our OSCAL effort. We value your input on this important work in progress.

You can view the repository by visiting <https://github.com/CISSecurity/CISControls> OSCAL. If you have any questions or concerns, please open an issue on GitHub by clicking the "Issues" tab, clicking the "New Issue" button, and completing the necessary sections with a full description of your question or idea.

To download the machine-friendly versions of the CIS Controls created through this project, you can access them via CIS WorkBench at <https://workbench.cisecurity.org/community/132/files>.

Ginger Anderson is a Senior Cybersecurity Engineer for the Center for Internet Security (CIS). In her current role, she is project owner on the Security Best Practices team, leading the following initiatives: Information Modeling, Controls Assessment Specification, OSCAL Repository, and editor of Living Off the Land guides. She previously led the Cyber Threat Intelligence team as well as the Federal Liaison Program for the MS- and EI-ISAC. Anderson started her career as an enlisted intelligence analyst with the U.S. Army and later as a commissioned intelligence officer. She has additionally supported the FBI and U.S. Department of Homeland Security in the cyber space. She holds B.S. in Systems Engineering from the United States Military Academy, a M.S. in Geospatial Analysis from Pennsylvania State University, and is working towards a Ph.D. in Data Science through the University of Maryland.

Cyberside Chat

This Quarter's Topic: Cyber Defense Strategies

By Sean Atkinson, *Chief Information Security Officer, CIS*

No business should be forced into the tradeoff of reducing business value in order to build a strong defensive posture. Well architected and efficient systems of control should be at its very essence, building on the requirements of business and practicality to ensure governance and control of risk.

Any plans put in place by an organization require point-in-time assessments with a growth reassessment requirement. As business processes adapt, change, or reengineer, the reevaluation for specific needs relating to the cybersecurity posture should occur. Change adaptation requires consideration of integrations that enable a defensive posture. With the new alignment, the organization should realign the risk posture to address the initial control, which has fundamentally changed.

An organization needs to consider not only the internal environment, but the external environment and associated impacts. Thinking about this from the adversary and regulatory perspective, business processes need to adapt to privacy and industry-specific security compliance and governance requirements. Secondly, without utilizing a threat informed approach, an organization is unable to adapt defensive strategies based on the opponent, but based on best practices and/or ignoring that an adversary is adapting to best practices in order to circumvent controls. Cyber defense becomes a change agent and requires evaluation from multiple internal and external factors.

Using the analogy of a football playbook, if you're not taking notes on your opponent's strengths, you will miss the opportunity to build defensive capability in order to mitigate that offensive ability. The plan would be to adapt the defensive posture based on understanding capability, likelihood of action, specific target of opportunity, and past

tactics used. Informing a defensive posture with this information provides a greater likelihood of thwarting the opponent's actions when a specific play is made against your defense. (I do say when here given the old adage of "it's not a matter of if, it's *when*" for being a target of a cyber attack.)

Chapters for a cyber-defensive playbook:

Schedule – updates, audits, control assessment

Players – inventory of systems, condition of those systems

Procedures – roles and responsibilities, how to treat and manage incidents

Plays – incident response scenarios, coverage of controls

Opponent strategy and threat informed plays – adversary assessment, TTP's and countermeasures; do we have the coverage?

If the defensive approach is thought of in this manner, the ability to address cyber defense will be well informed, enabling adaption to external stimulus, and be repeatable. Taking it one step further, a defensive posture is to be an offensive thought exercise. Red teaming in this space can strengthen the defensive posture as a condition of assessing both current defensive effectiveness with new offensive plays.

ISAC Update

By Paul Hoffman, *Director of Stakeholder Engagement, MS-ISAC*

It was a distinct honor and privilege to host the ISAC Annual Meeting in August after a two-year hiatus. We continually get feedback that the Annual Meeting is the in-person highlight of the year of the people who attend, and we feel the same way. There is nothing like the opportunity to meet face-to-face to discuss common challenges, share new ideas, and envision ways to improve our cross-organizational collaboration. We are better together, and the 2022 ISAC Annual Meeting was a wonderful reminder of that fact. Mark your calendars now for our 2023 ISAC Annual Meeting, taking place in Salt Lake City, Utah on August 6 – 9, 2023.

By the time you read this, the MS-ISAC will have reached a tremendous milestone – the 14,000 member mark. I could mark this occasion by reminding you why bigger is better, why more members means a more robust threat intelligence picture and enriched collaboration. Instead, I'd like to paint a picture of what 14,000 members looks like in the MS-ISAC. As a 14,000-member-strong community, this is who we are and how we support SLTTs:

More than 3,700 K-12 and more than 800 higher education member organizations

Nearly 3,500 EI-ISAC member organizations

Nearly 1600 cities and more than 1400 counties

All 50 states, all six territories and 112 tribes represented among membership

620 members participating in our various working groups

450 members participating as mentors/mentees in our Leadership Mentoring Program

486 members attended the ISAC Annual Meeting, complete with 52 sessions, 20 hours of member instruction, and 69 vendor representatives

Sent 278 cybersecurity alerts to members

Hosted 20 best practices webinars and 3 SNAP calls, totaling more than 18,000 attendees in 2022

Resolved 8200+ member requests year to date, with an average time to resolution of 1.2 hours

Serving more than 30% of our members with no-cost web security in our Malicious Domain Blocking and Reporting (MDBR) service

With less than two months until midterms, the EI-ISAC continues the important work of supporting elections through the [Cyber STRONG](#) campaign, the [Essential Guide to Election Security](#), and other initiatives. They will be convening a virtual "situation room" starting weeks before the election to help election offices report cyber threats and misinformation and share information. Connect with your EI-ISAC account management specialist or contact elections@cisecurity.org to learn more about any of these activities.

The future has never been brighter for the MS-ISAC, with exciting webinar series to help you learn about and implement security best practices, active working groups to guide our current and future community efforts, and a new funding stream available to SLTTs through the State and Local Cybersecurity Grant Program (SLCGP).

As members of our vibrant community, you are the most qualified ambassadors we have to share with your colleagues and peers the benefits of MS-ISAC membership. Thank you for the vital part you play in making the MS-ISAC the special community it is. At the MS-ISAC, we're here for you. More importantly, your efforts prove every day that MS-ISAC members are there for one another.

Upcoming Events

October

October 14

Cyber Security Summit: Scottsdale will take place at the Hilton Scottsdale Resort and Villas, bringing together business leaders and cybersecurity professionals to learn about the latest cyber threats. CIS CTO Kathleen Moriarty will lead a panel discussion on securing remote and hybrid workforces. SLTT entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/scottsdale22/>.

October 19 – 21

The North Carolina Local Government Information Systems Association (NCLGISA) will host its **2022 NCLGISA Fall Symposium** at the Renaissance Asheville Downtown in Asheville, North Carolina. Local government IT leaders and professionals from across the state will gather to hear from industry experts on the latest developments and difficulties facing local governments. EI-ISAC Senior Director Marci Andino will lead a session at the event on cybersecurity resources and best practices for election offices. Learn more at https://www.nclgisa.org/page/2022fall_symposium.

October 26

CompTIA will host its **Public Sector Cyber Leader Summit** at the National Association of Counties (NACo) and National League of Cities (NLC) City/County Conference Center in Washington, D.C. Local government IT leaders and professionals from across the country will come together to share the pressing issues and trends impacting public sector cyber resiliency, real-life examples and case studies, and a national view of local and federal cybersecurity issues with both national cybersecurity experts and their peers. MS-ISAC Senior Regional Engagement Manager Kyle Bryans and CIS Services Account Executive Jamie Ward will co-lead a session on cybersecurity resources for local governments. Learn more at <https://connect.comptia.org/events/view/comptia-pti-local-government-cyber-leader-summit>.

October 27

Cyber Security Summit: Los Angeles will take place at the Loews Santa Monica Beach Hotel, bringing together business leaders and cybersecurity professionals to learn about the latest cyber threats. CIS CISO Sean Atkinson will lead a panel discussion on ransomware and Zero Trust. Through our partnership, SLTT entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/losangeles22/>.

November

November 4

Cyber Security Summit: Columbus will take place at the Renaissance Columbus Downtown Hotel, bringing together business leaders and cybersecurity professionals to learn about the latest cyber threats. Through our partnership, SLTT entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/columbus22/>.

November 9 – 11

The Hoosier Educational Computer Coordinators (HECC) will host its **HECC Fall 2022 Conference** at the Crowne Plaza Hotel in Indianapolis, Indiana. K-12 technology leaders and professionals from across the state will come together at the event to network and collaborate with peers as well as explore opportunities, resources, and best practices for successfully integrating technology into their schools. MS-ISAC Regional Engagement Manager Elijah Cedeno will lead a breakout session at the event on no-cost cybersecurity resources for public K-12 schools. Learn more at https://s4.goeshow.com/hecc/annual/2022/hecc_home.cfm.

November 10

Cyber Security Summit: Boston will take place at the Westin Copley Place, bringing together business leaders and cybersecurity professionals to

learn about the latest cyber threats. CIS CISO Sean Atkinson will lead a panel discussion on ransomware and Zero Trust. Through our partnership, SLTT entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/boston22/>.

November 15 – 17

The Association of Oregon Counties (AOC) will host the **AOC Annual Conference** at the Graduate Eugene in Eugene, Oregon. The event will bring together local government and elections leaders and professionals from around the state for three days of education and networking aimed to help improve residents' lives and the efficiency of county government. The CIS Services team will be at the event, sharing our cybersecurity resources for local governments. Learn more at <https://oregoncounties.org/2022-annual-conference/>.

November 18

Cyber Security Summit: New York will take place at the Sheraton New York Times Square Hotel, bringing together business leaders and cybersecurity professionals to learn about the latest cyber threats. CIS CTO Kathleen Moriarty will lead a panel discussion on cloud security. Through our partnership, SLTT entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/newyork22/>.

November 28 – December 2

AWS re:Invent will take place in Las Vegas, Nevada. Spread across six dedicated venues along the Las Vegas Strip, AWS re:Invent will offer attendees a unique opportunity to immerse themselves in AWS learning. Cloud leaders and practitioners from around the globe will come together to connect and collaborate with the AWS user community, learn from AWS experts, boost their proficiency in core AWS services, learn best practices at over 1,500 breakout sessions, and gain valuable hands-on experience in bootcamps, labs, hackathons, and workshops. The CIS team will be on the show floor at Booth 127 sharing our cloud security resources with attendees. Learn more at <https://reinvent.awsevents.com/>.

November 29 – December 2

California IT in Education (CITE) will host its **62nd Annual CITE Conference** at the Long Beach Convention Center in Long Beach, California. K-12 technology leaders and professionals from across the state will come together at the event to network and collaborate with peers as well as explore opportunities, resources, and best practices for successfully integrating technology into their schools. MS-ISAC Senior Regional Engagement Manager Brendan Montagne and Cyber Threat Intelligence Manager TJ Sayers will co-lead a breakout session at the event on the ransomware landscape for K-12 schools, and Montagne will co-lead another session with CIS Program Manager Kelly Morris on no-cost cybersecurity resources for public K-12 schools. Learn more at <https://www.cite.org/2022conference>.

December

December 6 – 10

The Council of State Governments (CSG) will host the **2022 CSG National Conference** at the Hilton Hawaiian Village Waikiki Beach Resort in Honolulu, Hawaii. Each year, CSG brings together hundreds of state leaders from all three branches of government and who hail from across the United States, the U.S. territories, and Canada at its national conference. This year-end convening spotlights emerging public policy issues and challenges facing the states. The CIS Services team will be at the event, sharing our cybersecurity resources for state governments. Learn more at <https://www.csg.org/csg-events/csg-national-conference/>.

December 8

Cyber Security Summit: Houston will take place at the Westin Houston Memorial City, bringing together business leaders and cybersecurity professionals to learn about the latest cyber threats. CIS CTO Kathleen Moriarty will lead a panel discussion on securing remote and hybrid workforces. Through our partnership, SLTT entities can receive free admission. Contact the CIS CyberMarket team for more details. Learn more at <https://cybersecuritysummit.com/summit/houston22/>.

Creating Confidence in the Connected World.™



Copyright © 2022 Center for Internet Security, Inc., All rights reserved.



Interested in being a contributor?

Please contact us:

cybermarket@cisecurity.org

www.cisecurity.org

518.266.3460