Part 2: Continuous Oversight

By Pamela Warren, Cybercrime Strategist and Director of Public Sector Initiatives

In the second of this multipart series for government cybersecurity planning, we take on the issue of awareness and oversight in the government agency’s cybersecurity program. The first editorial brief entitled “What’s the User Got to Do with It?” discusses the role of users in government cybersecurity and can be found at [www.mcafee.com/us/resources/solution-briefs/sb-whats-the-user-got-to-do-with-it.pdf](http://www.mcafee.com/us/resources/solution-briefs/sb-whats-the-user-got-to-do-with-it.pdf).

There are many incidents of global government or defense industrial base (DIB) targeting we can point to in the recent past. Whether it’s a disgruntled employee who has abused unfettered access, a social engineering attack against an unwitting government official, or an attack against the email system to steal much-valued intelligence about projects of interest to other nations or competitors, there is a need to be aware of every significant modification to the network, movement of sensitive data, new targeted malware tunneling deep into network, or something as simple as the use of an unapproved external peripheral.

**Times of Disconnect: The Need for Continuous Visibility**

One thing is certain: your network will continue to change. Regardless of where you are in the world, we know government IT decision makers are facing numerous pressures. Whether your particular pressure is to move part of your operations to a cloud-based model, approve the adoption of consumer mobile devices for the government work environment, or adopt social media use, the irony is that you are being pressured at a time of the greatest global attention in history to insidious cyberattacks. Our nations’ economies are at stake as our intellectual property is targeted. Our infrastructure and way of life is at stake. Our trusted government secrets are more aggressively targeted. To open our networks further at this critical time seems a complete disconnect.

A US government model for continuous awareness

The US government’s approach to having continuous visibility of threats and their “revision” of annual information security reporting is a “continuous monitoring” project, CyberScope (see OMB 10-15 and NIST Special Publication 800-137), which will be followed by a more encompassing architecture. CyberScope does not focus on all-encompassing visibility such as sensitive data movement or broader network changes, but rather focuses on three primary host data elements that should be reported:

- Asset inventory using SCAP common platform enumerations (CPE)
- Configuration data to report on SCAP common configuration enumerations (CCE)
- Common vulnerability enumerations (CVEs) and an aggregate value of systems affected by the specific CVE

CyberScope is a subset of a broader vision of what the US government has called “Continuous Asset Evaluation, Situational Awareness, and Risk Scoring,” or CAESARS.

CAESARS

The CAESARS architecture with framework extension provides the framework for “smarter” networks in which operations can have greater risk visibility and allow for large enterprise implementations that need a multitier architecture. This framework provides for “context” considering the existence of impacted vulnerable platforms in the first place, status of needed patches on those vulnerable systems, or compensating controls for the vulnerabilities. As the goal is to analyze data, perform scoring, enable user queries, and provide overall situational awareness, the risk scoring and
continuous monitoring provides information at the right level of detail. Managers and system administrators can then understand the state of the IT systems for which they’re responsible, the specific gaps between actual and desired states of security protections, and the numerical value of every remediation action that can be taken to close the gaps.

Frameworks should support a dynamic defense with “prescriptive flexibility”

Any good framework must allow enough leeway to allow for technological innovation by anticipating future solutions to complex problems. But it must still do so with just enough prescriptive measures to make framework adoption meaningful.

Working with governments around the world to build “dynamic defenses” that must stand the test of time, we know that such frameworks must anticipate evolving threats, new threat vectors, and the adoption of new platforms and applications on your network. Because the advisory moves fast, you’ve got to know your posture immediately. The security operations center (SOC) needs continuous visibility of status (the configuration, patch level, and so on), events (for incident response), and your risk—think of it as a continuous process of learning. Consequently, the framework must provide continuous visibility that considers what data or information you need to see, how often, and how deeply. For example, you don’t have true visibility until you know what your applications and your data are doing.

It’s been a bit of a shift in thinking, but we continuously remind our customers to expand their definition of “asset” to include their data and users as well as their traditional assets. And optimally, it should be based on standards, easing the burden on the government agency that must actually implement the given framework, leveraging numerous vendors and solutions. With a framework based on standards, the government can help promote rapid adoption of the new compliance structures—so we all win.

In addition to applying the right framework, your solutions must also always provide you with context, not just information for the sake of information. In our existing cyber environment, this is ever more critical, or you will be back to the same game of information overload—frequently the attack was right there in the logs, but nobody saw it. Context provides a personalized view of the threat or vulnerability information: “Here is the threat, but given our existing countermeasures, we are protected.”

Many governments will monitor what the US government is doing and determine whether it is right for their own environment. Regardless of whether your own government adopts the CAESARS model, the ability to have a comprehensive framework for its dynamic defense—one providing ongoing visibility—is an urgent need all governments have with the changing environments we face.

McAfee Support for Continuous Monitoring

Regardless of which framework your government follows, the good news is that McAfee provides the foundational components today to begin that transition to an effective continuous monitoring environment. Between the open architecture of the McAfee® ePolicy Orchestrator® (McAfee ePO™) management platform to the US Department of Defense-driven technology partnering program we call McAfee Security Innovation Alliance, we can provide even greater awareness network-wide. This means we can help governments reduce time to problem resolution, lower operational costs, and increase efficiencies while enhancing their security posture. McAfee not only continuously adheres to industry standards, but also takes pride in its active membership in the development of industry standards and the adoption of standards and protocols like SCAP, among others. McAfee is proud to be actively participating in the CAESARS standards development. We feel our active participation in CAESARS development pays off for our customers—we can accelerate interoperability and integration of third-party solutions within complex customer environments and reduce time to problem resolution, among numerous other benefits.

Ask our team about how McAfee Policy Auditor and McAfee Vulnerability Manager are helping realize CyberScope goals today. You might also be interested in learning how Insightix, our McAfee Security Innovation Alliance partner, continuously monitors the network for newly attached devices and, through our integration work, can trigger McAfee Vulnerability Manager to scan the new devices, update the McAfee ePO asset database,
and provide the government with a complete, up-to-date inventory and security status of their devices. Add to that the fact that McAfee Risk Advisor can get updated threat information, tie it to the insights of your countermeasures, and give any government that contextual perspective on their risk posture—what my teammates call “total risk intelligence.” It’s also a great way to determine the ROI of the investments you’ve already made. I believe all of it together provides a pretty impressive support to this latest iteration of major government initiatives in which we can all benefit when our governments can validate that they’re more secure.

Summary
To create a truly dynamic defense with the focus on all threat vectors, all data movement, all network anomalies, and finally, the context for your unique environment, you need continuous visibility. Regardless of which model your own government adopts, we recommend a framework that gives you that visibility without wasting precious resources and time to chase a contextually irrelevant threat. An automated process is meant to save you time and resources, provide you enough granularity of your issues to resolve them expeditiously, and overall guard your most sensitive data and protect your network—regardless of what technology shifts your organization takes and the growth in targeted threats directed against you.

McAfee Public Sector
McAfee serves the world’s governments, meeting the most stringent military and civilian government requirements and providing swift deployments across the largest, most complex government networks. With access to the most comprehensive threat intelligence, our well-experienced Public Sector Professional Services team tests against real, up-to-the-minute threat scenarios and uses processes and methodologies from some of the most complex and secure government deployments.

Resources
For additional resources on government situational awareness, visit http://www.mcafee.com/us/industry/public-sector/index.aspx where you will find “Part I: What’s the User Got to Do with It?”

Pamela Warren is the Director of Public Sector and Critical Infrastructure Protection initiatives at McAfee. She has spent her entire career in the security industry, serving both the US intelligence community and the private sector. During her tenure in private industry, she has worked on US Homeland Security initiatives, solutions to the global data loss problem, and has worked closely with global governments on key initiatives. Ms. Warren has testified for the Senate Select Committee on Intelligence, served on the DSL Forum security working group, the X9 standards group for financial security standards, and the cybersecurity working group of the US National Security Telecom Advisory Council on critical infrastructure. She also speaks at numerous industry events. She holds a master’s degree in telecommunications from George Washington University and is a Certified Information Systems Security Professional (CISSP) and Certified Information Privacy Professional (CIPP).

---