Enhancing Security in Telemetry Post-Processing Environments with

Continuous Diagnostic and Mitigation (CDM)

Jeff Kaibjian

Hewlett Packard

ABSTRACT

While great strides have been made in recent years by government agencies in deploying proactive network security tools, the federal government as a whole desires to continue to press the state of the art in protecting its IT infrastructure. To this end, the US Department of Homeland Security (DHS) has created the Continuous Diagnostic and Mitigation (CDM) program [1] (also known as Continuous Monitoring, CM). It strives to establish a technology framework whereby agency federal government IT networks can be continuously monitored for threats and vulnerabilities, providing an analysis and correlation capability that will enable entities to better evaluate risk. It also defines a hierarchical dash-boarding capability that facilitates both aggregation and communication of each agency's network health status into abstracted levels of summary so the federal system as a whole can be better evaluate their IT security posture. Going forward, these technologies will dramatically impact all government agencies, the Department of Defense (DOD), and commercial entities.

KEYWORDS

Continuous Monitoring, Continuous Diagnostics and Mitigation

INTRODUCTION

The concept of continuous monitoring is not new [2]; however, its widespread actual use and deployment in the federal government in a closed loop fashion is. It is important to stress that it is one thing to identify potential threats in an IT environment and attempt to address them in an ad hoc, manual, fashion; and quite another to systematically and regularly weigh the severity of those threats, and methodically remediate them at regular intervals using a semi-automated or automated regimen----this is the essence of the CM challenge. The DHS sees their CM initiative as a three phase effort. The first phase emphasizes asset management including: Hardware Asset Management (HWAM), Software Asset Management (SWAM), Configuration Management (CM) and Vulnerability Management (VUL). The second phase highlights infrastructure integrity and user accounts and privilege involving network access controls, managing trust in users, managing security related behavior, managing credentials and authentication, and managing account access. The third and final phase relates to managing events such as preparing and responding to contingencies, policy, planning and quality and managing audit and operational security.

CM ARCHITECTURAL ELEMENTS

The goal of a CM system (Figure 1) it to enable an organization to make smart triaging decisions about addressing potential threats and vulnerabilities to their IT environment by evaluating risk at regular interval (i.e. closed loop). Identifying risk requires the deployment and use of security sensor applications whose data must flow into a monitor/dashboard application where it can be correlated and processed to quantify that risk. Security sensor applications of interest can involve end point or server protection applications that can assist organizations in identifying the following:

- Hardware that is not authorized or does not have active management.
- Software that is unmanaged or unauthorized running on servers (physical or virtual).
- Configuration settings of both hardware and software items that are inappropriate.
- Vulnerabilities (from the National Vulnerability Database ,NVD) that may exist on organization IT assets.

The security sensor information must be collected and forwarded to the monitor or dashboard application at regular intervals. This can be accomplished with a dedicated data transport tool. Data formats are also an issue and the hope is to leverage a unifying format like the Secure Content Automation Protocol, SCAP version 1.2 [2] to ease those challenges.

Once the sensor data is in the dashboard it can be processed and analyzed to quantify risk. Other information from the IT environment is also leveraged by the dashboard in this effort including the organization IT Configuration Database. The dashboard must then have an intuitive user interface to visualize the risk, so security personnel in the organization may evaluate and prioritize the vulnerabilities and threats which are to be remediated. Other information may be used by the dashboard to complement risk evaluation including input from other types of operational security tools (e.g. Security Information Event Management, SIEM, Intrusion Prevention, IP, Data Leak Protection, DLP, etc.). Anything that can augment or assist the dashboard in properly depicting the risk situation is of value.

An example using Data Leak Protection (DLP) will illustrate this point. Data Leak Protection tools seek not only to identify sensitive information which might be illicitly or accidently be removed from an organization, but simply identify where sensitive information may reside anywhere inside the corporate IT network. If a vulnerability is found on a server (which makes it more likely to be compromised) there is obviously a risk in not remediating that vulnerability.

However, if a DLP tool finds sensitive documents are residing on that server, then that should influence the calculated risk value for that server. The risk should be higher since if that server were compromised, sensitive documents would immediately be at risk.

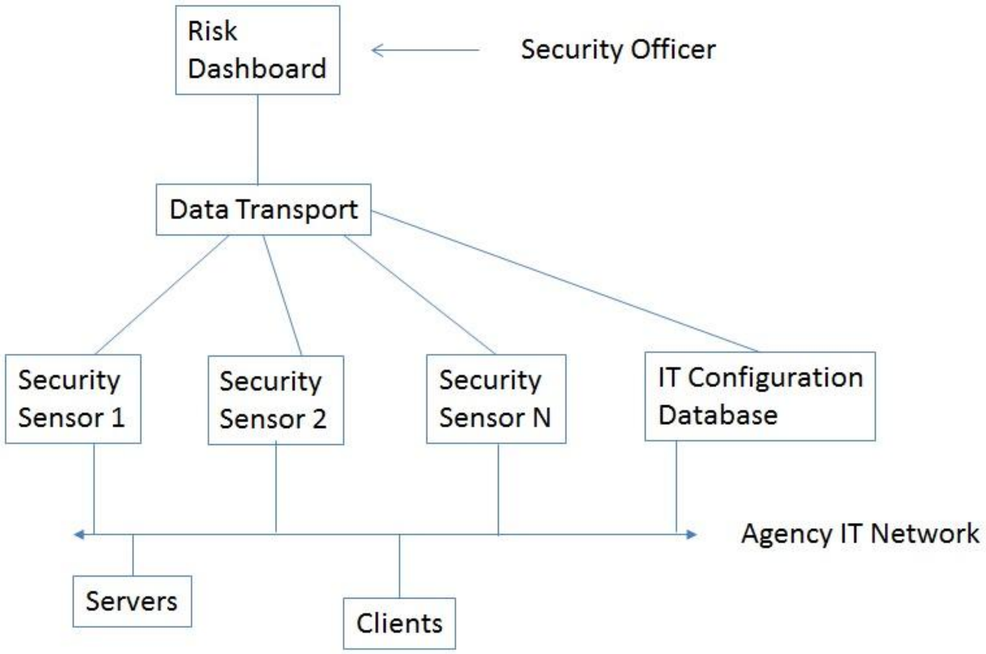

Figure 1. A basic CDM Phase 1 framework.

DASHBOARD ROLL-UP

The government CM vision also includes rolling-up individual agency IT security status/risk to higher level dashboards which could give the government a macro view of overall federal agency IT risk. The challenge with this mandate involves seamless communication of information in a blinded fashion to prevent any sensitive information from individual agencies from being compromised. This concept is illustrated in Figure 2.

THE OTHER CM PHASES

The other two phases of CM help to augment and enhance the risk evaluation. Identity, privilege and access control applications (in Phase 2) will help better quantify and manage user risk.

Information such as what the user has access to, what computer security training the user has had, and what the user actual behavior has been, can significantly impact risk in an IT environment. Thus, while Phase 1 deals with the hardware/software or machine risk; Phase 2 involves accounting for the human element in the IT environment. Phase 3 relates to utilizing operational security (e.g. Database Activity Monitoring, DAM, Intrusion Prevention, IP, etc.) and audit tools (Security Information Event Management, SIEM) to help better integrate the risk story.

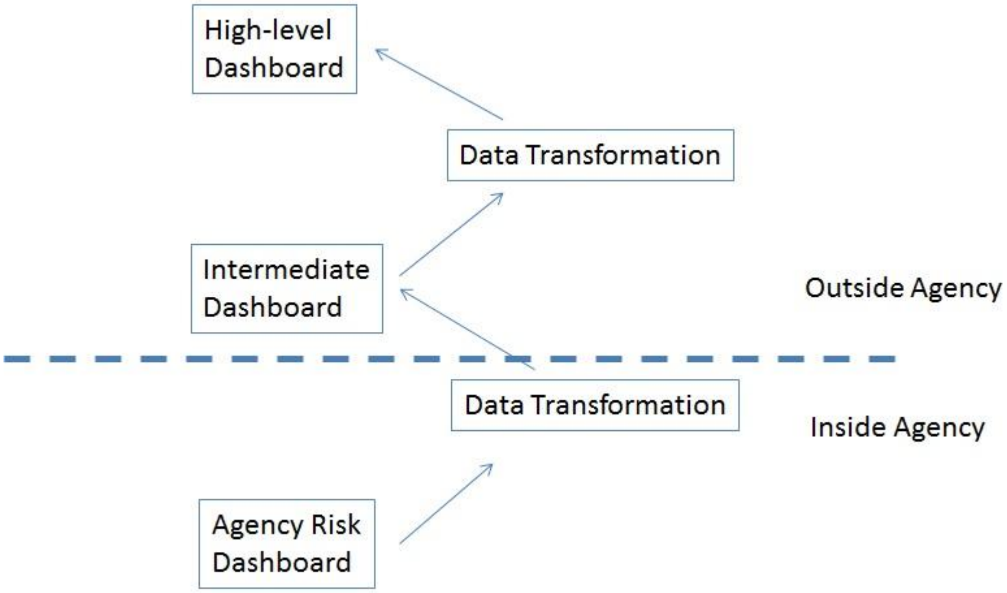

Figure 2. The CM Dashboard roll-up concept.

IMPLICATIONS FOR TELEMETRY POST-PROCESSING ENVIRONMENTS

There are a number of important takeaways with respect to the DHS CDM initiative. First, the technology is going to be required to be deployed in all federal agency environments. However, not all at once; and thus, some agencies will have longer to think about deployment strategies than others. However, it should be clear: this is an initiative that is not going to go away. So the best approach at dealing with it, is to accept the challenge and start planning how each organization can get the maximum value out of it! Commercial vendors should also take notice. Although the DHS mandate does not effect them, it is not outside the realm of possibility that the government will be so enamored with the success CM that they could mandate their commercial contractors to utilize it!

With respect to telemetry post processing environments, one of the key benefits is the protection of the post-processed telemetry data product. That is, a deployed CDM framework inside a telemetry post-processing environment will ensure that clients and servers in that computing environment where sensitive telemetry data may be stored, will be less vulnerable to compromise. Further, if an operational security application like DLP is also utilized in the CM framework, then anytime vulnerabilities are discovered, the dashboard can cross-reference where the most sensitive telemetry data in the organization resides; to make sure that if the sensitive telemetry data is residing on one of the servers that has a newly identified vulnerability; that its risk weighting will be substantially increased to account for the increased risk of sensitive data compromise. This concept is illustrated in Figure 3.

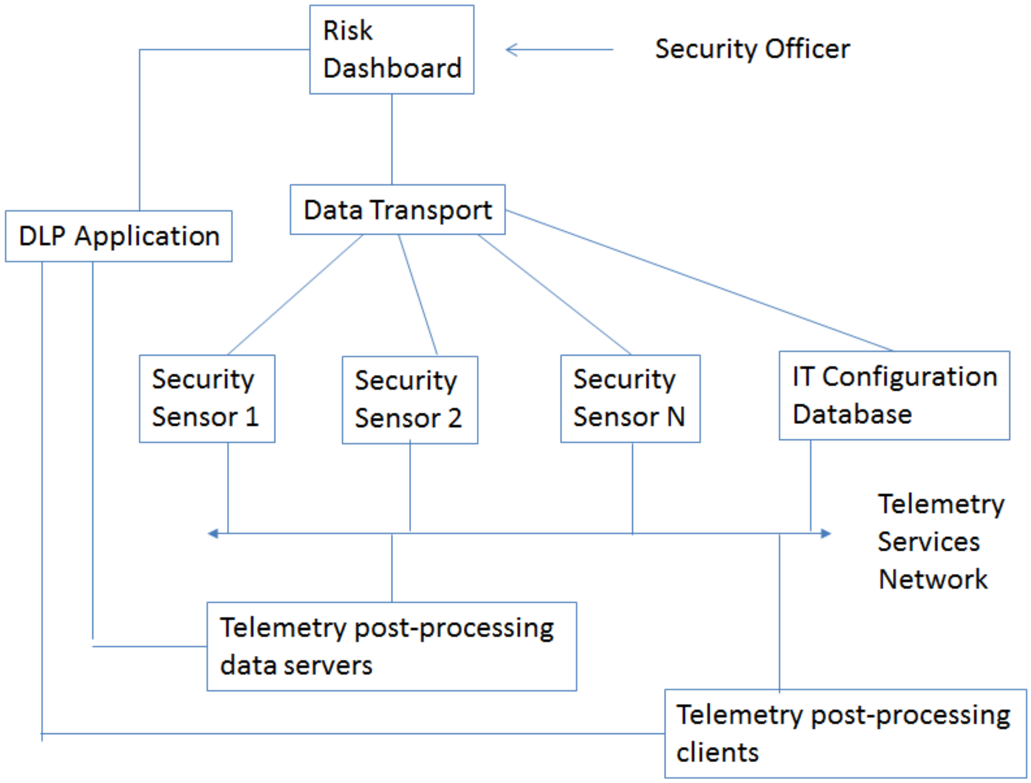
Risk Dashboard
Security Officer
DLP Application
Data Transport
Security Sensor 1
Security Sensor 2
Security Sensor N
IT Configuration Database
Telemetry Services Network
Telemetry post-processing data servers
Telemetry post-processing clients

Figure 3. Exmple CM use in telemetry post processing environments.

CONCLUSION

CM technologies involve aggregating and analyzing security sensor data and IT configuration database information in a dashboard/monitor application to gain better insight into IT risk giving organizations better insight on how to get from their actual (potentially insecure) state to a desired (more secure) state. Operational security applications can better augment risk calculations by giving the dashboard application better insight into specific client/server organization characteristics (e.g. Server A maintains sensitive telemetry data, Server B maintains personnel data, etc.) The federal government is committed to deploying Continuous Monitoring technology in federal agencies to better protect government IT environments. The implications of this commitment will span the federal realm; but most immediately will help to insure government IT environments will be better protected. Finally, CM technologies can offer telemetry post processing environments more robust protections by regularly checking to make sure production and test client and server machines are free of vulnerabilities that could potentially endanger valuable telemetry post processing data residing on those machines, leaving them vulnerable to compromise.

REFERENCES

[1] US Department of Homeland Security**, CDM Home Page, http://www.dhs.gov/cdm.**

[2] National Institute of Standards and Technology**, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, SP 800-137;** US Government Printing Office, September 2011.

[3] National Institute of Standards and Technology**, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2,** US Government Printing Office, September 2011.