SOLARWINDS WHITEPAPER

Cybersecurity – A Practical Approach to Actionable Intelligence

Brad Hale

SOLARWINDS WHITEPAPER

Cybersecurity – A Practical Approach to Actionable Intelligence

cy•ber•se•cu•ri•ty
- noun
measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack[1]

Introduction

Cybersecurity is an enormously broad topic and covers a breadth of technologies and tools. The Cybersecurity Act of 2012 is a whopping 205 pages long and, interestingly enough, never actually defines what exactly Cybersecurity is. The variety of Federal Cybersecurity initiatives and broad 'comprehensive' approaches being discussed today can create gridlock and slow down the practical implementation of solutions that can help now.

From the first well-publicized international security incident on ARPANET in 1986, there has been a rapid evolution in the requirements of network security. Security threats have morphed from network level threats (intrusions and denial-of-service attacks) to much more sophisticated content based threats (viruses, worms, Trojans, spyware, etc…). As a result of this ever-increasing complexity, there is also a need for more sophisticated levels of intelligence to identify, analyze, and defend against cyber threats.

The White House's comprehensive national Cybersecurity initiative discusses implementation of tools, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS), but security is more than the implementation of point products. We define Cybersecurity in terms of our ability to collect and observe data to detect distributed attacks; to correlate and analyze that data into something that is actionable; to decide on the courses of action to take; and then to act on the decisions that have been made.

This paper will provide a practical approach to actionable intelligence. It is written under the assumption that network security policies are in place that are aligned with the Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) Special Publication 800-53 to some extent.

Network Security Challenges

Network complexity has evolved rapidly over the last 10 years. Today's networks consist of many different network devices (firewalls, routers, switches, etc…) from many different vendors, with many access mechanisms into the network (wireless, mobile devices, email, portals for partners and customers, FTP servers, and peer-to-peer applications and communications).

Workforce mobility has had the unintentional consequence of making internal threats as prevalent, if not more so, than external threats. When users take their laptops home at night or connect at the local Starbucks, they are at increased risk of infection. Once the user returns with the compromised device, the entire network is at risk.

As both commercial and internally developed applications increase in complexity, so does their vulnerability and so are the attacks targeted against them. **Intrusion Attacks** (Trojans, Worms, SQL injections, Exchange server attacks, Apache/IIS buffer overflow attacks) targeting the application and the application layer protocols as opposed to the physical network are designed specifically to bypass traditional security methods such as firewalls and anti-virus; **Viruses and Worms** have become sophisticated and complicated enough that they can no longer be detected by simple anti-virus techniques; and **Spyware** that has moved from the harmless but annoying variation to malicious information collecting that includes full keystroke logging now present some of the greatest security risks.

OODA Cybersecurity Framework

The OODA loop (for *observe, orient, decide, and act*), originally developed by military strategist and USAF Colonel John Boyd and applied to the combat operations process, can be a powerful concept in Cybersecurity. According to Boyd, decision-making occurs in a recurring cycle of observe-orient-

[1] http://www.merriam-webster.com/dictionary/Cybersecurity

decide-act. An entity (whether an individual or an organization) that can process this cycle quickly, observing and reacting to unfolding events more rapidly than an opponent, can thereby "get inside" the opponent's decision cycle and gain the advantage. In the case of Cybersecurity, the ability to observe and react to threats more rapidly than the attacker will significantly enhance your network security. Let's take a look at how this can be practically applied.

Observe – Collect data from everything in your environment (Network Devices, Servers, Storage, Applications, etc…)

Orient – Correlate and analyze the data into something that is actionable

Decide – What is the next step

Act – Respond to the decision

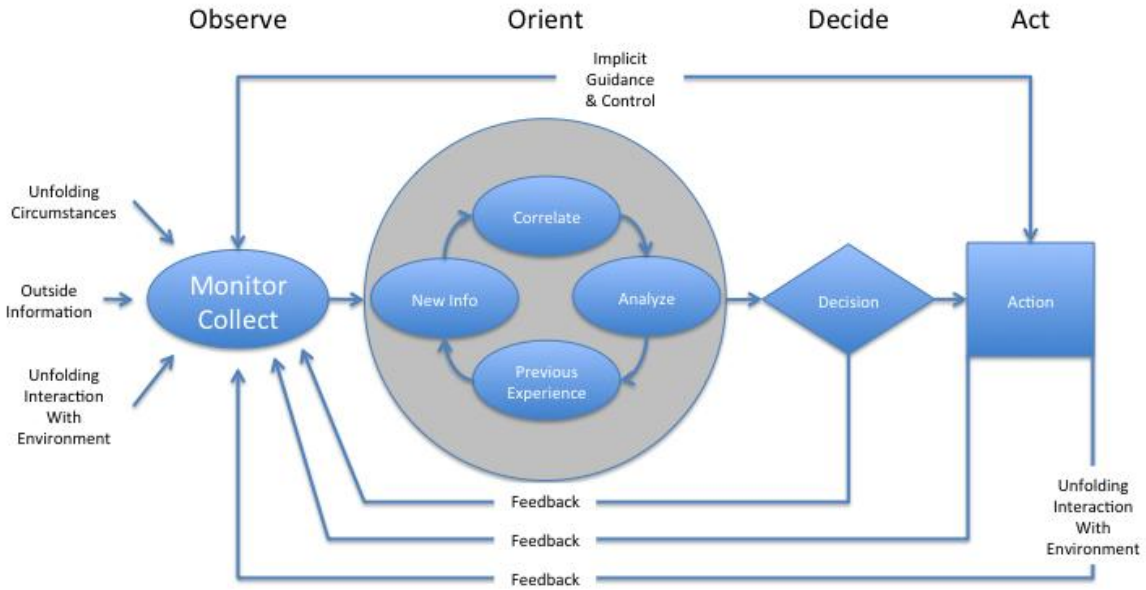

Figure 1 OODA Loop Modified for Cybersecurity

Taking the OODA loop one step further and overlaying the NIST SP 800-53 based security controls an effective Cybersecurity plan can be created.[2]

OODA Loop	NIST SP800-53 Security Control	Example Practices
OBSERVE	CA-7 Continuous Monitoring	Continuous monitoring program that includes: Configuration management process; Determination of security impact of changes; On-going security control assessments; Reporting security state to appropriate officials
	SI-3 Malicious Code Protection	Employ, update, and configure malicious code protection
	SI-4 Information System Monitoring	Deploy monitoring devices to monitor events, detect attacks, identify unauthorized use
	SI-7 Software and Information Integrity	Detect unauthorized changes to software and information

[2] The FISMA Implementation Project was established in January 2003 to produce several key security standards and guidelines required by Congressional legislation including NIST Special Publications 800-53. The objective of NIST Special Publication 800-53 is to provide a set of security controls that can satisfy the breadth and depth of security requirements levied on organizations, mission/business processes, and information systems and that is consistent with and complementary to other established information security standards. The catalog of security controls in Special Publication 800-53 can be effectively used to protect information and information systems from traditional and advanced persistent threats in varied operational, environmental, and technical scenarios.

OODA Loop	NIST SP800-53 Security Control	Example Practices
	AU-6 Audit Review, Analysis, and Reporting	Review and analyze audit records for indication of inappropriate or unusual activity
Orient	IR-4 (CE-4) Incident Handling	Correlation incidents with responses
	RA-5 Vulnerability Scanning	Scan for vulnerability in system and applications
DECIDE	RA-3 Risk Assessment	Assess risk, document and review results, update as changes occur
	CM-4 Security Impact Analysis	What are the impacts of changes to the system
ACT	IR-4 (CE-2) Incident Handling	Dynamically reconfigure the system as a result of incidents.
	IR-4 (CE-3) Incident Handling	Identify classes of incidents and take appropriate actions as a result of incident class
	SI-4 (CE-3) Information System Monitoring	Employ automated tools to integrate Intrusion Detection tools into access control and flow control for rapid response
	SI-2 Flaw Remediation	Identify, report, and correct system flaws

Observe

As the OODA loop implies, observation is one of the foundational elements of Cybersecurity. It can be best described as the monitoring and collection of data within the network. In every network today, we have the ability to capture detailed performance and event log data on just about every network device, system, or application that, in turn, provides us vital information about what is happening on our network. One might also refer to observation as detection, specifically the discovery of malicious activity through internal monitoring tools or external services that publish information about detected incidents. Proactive observation differs from reactive in that the IT organization is the first to know of an incident or performance issue as opposed to the end-user first reporting an incident thus resulting in a reactive observation.

Observation is achieved through the use of all or a combination of internal monitoring tools that can include:

- Network Management Systems – monitors the health and performance of devices on the network
- Server & Application Management Systems – monitors the health and performance of servers and applications that run on the network
- Storage Management Systems – monitors the health and performance of storage environment
- IP Infrastructure Management Systems – monitors the health and performance of the IP infrastructure including IP address management, DHCP management, and DNS management
- Device Tracking and Switch Port Monitoring Systems – monitors the connected location of devices on the network
- Intrusion Detection Systems (IDS) – monitors network and system activity for malicious activities or policy violations and reports back to management system
- Firewalls – controls the incoming and outgoing network traffic through data packet inspection based on a predetermined rule set

One of the many challenges that IT pro will face is the vast amount of data gathered by the various monitoring tools. It is easy to see how issues can simply slip through undetected and therefore not acted on. This leads us to Orientation.

Orient

Orientation shapes the way the network, systems, and applications are observed, the way we decide, and ultimately on the way we act. This is where the filtering or the intelligence is applied based on new or existing information, correlation, analysis, and past experience. Cybersecurity examples of orientation would be the real-time collection and correlation of performance information, log and event data, and traffic analysis just to name a few. To get even more specific, one can correlate network traffic with device and application log data to identify the sources, destinations and generators of intrusions.

Again, given the vast amount of data that is being observed, it is nearly impossible to manually sift through the data in a reasonable amount of time thus driving the need for automated, real-time tools such as:

- Intrusion Detection and Prevention systems (IDPS) – identifies possible incidents, logs information, reports to management system and attempts to prevent

- Security Information Event Management (SIEM) systems – provides real-time analysis of security alerts through the analysis of network hardware and application logs
- Network Traffic Analyzers – provide real-time analysis of network traffic including source IP, destination IP, protocols, and more

Decide

Following the observation and orientation phases, one can formulate a hypothesis and decide on the correct course of action to pursue based on the overall risk management profile of the organization. The process of risk management is an ongoing iterative process that must be repeated indefinitely. The environment is constantly changing and new threats and vulnerability emerge every day. The choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Decision outcomes will typically fall into one of four categories:

- Risk assumption – accept risk, continue operating
- Risk avoidance – avoid the risk by eliminating the risk cause and/or consequence
- Risk limitation – limit the risk by assigning controls that minimize the impact
- Risk transference - transfer the risk by using other options to compensate for the loss

Automated tools, while not designed to make the decision, aid in the situational and vulnerability assessment as well as speed the decision making cycle.

- Security Information Event Management (SIEM) – synthesize and correlate multiple events to provide better situational analysis and aid in the decision cycle
- Patch Management – assess software vulnerability

Act

If we were able to actually follow the OODA loop in a truly linear fashion, then we would now be entering the Act phase. The more we can automate the Act process, or train our system, the more we can speed the process, reduce the chance for introduced error, and move closer to risk avoidance. Also, action is far from the end of the process, it is simply the step before we feedback into the observation, orientation or decision phases. Automation, again, aids in the process of action by offering speed, repeatability, and documentation.

- Security Information Event Management – take automated actions to respond to security and operational issues
- Configuration Management Systems – dynamically configure network as a result of incidents
- Patch Management Systems – ensure the latest software updates and patches are implemented
- Device Tracking and Switch Port Monitoring Systems – track and isolate users and devices at the port location

Best Practices

Based on NIST FISMA guidance and our OODA Loop modified for Cybersecurity we have developed a list of recommended best practices.

1. Inventory your hardware and software assets – know what's on your network
2. Benchmark first – you can't improve what you don't measure
3. Secure your configurations – network configuration errors are the single greatest cause of network downtime
4. Keep your systems updated - with regular application updates and patches
5. Defend your boundary – they can't hurt you if they can't get in
6. Look at your logs – over 80% of all network intrusions can be detected through proactive log analysis
7. Limit access – to those with a need to know
8. Test, test, and test again – before and after changes
9. Defend against data loss – internal threats are just as great as external threats
10. Audit, Audit, Audit – see Test, test, and test again

Practical Solutions From SolarWinds

SolarWinds portfolio of IT products covers a wide spectrum of practical and actionable solutions for Cybersecurity that align directly with the OODA loop for Cybersecurity. SolarWinds solutions for Cybersecurity deliver scalable, cost-effective, enterprise-class products and have received certifications and approvals from ARMY CoN, AIR FORCE APL, NAVY DADMS, FDCC/USGCB. In addition, a number of SolarWinds products are FIPS compatible, meet DISA STIG requirements, and are in process for Common Criteria EAL2 certification.

Observe	Orient	Decide	Act
SolarWinds Network Performance Monitor **makes it easy to detect, diagnose, and resolve network performance issues and delivers real-time views and dashboards that allow you to track network performance at a glance.**	SolarWinds Log & Event Manager delivers powerful Security Information and Event Management (SIEM) capabilities in a highly affordable, easy-to-deploy virtual appliance. It collects log and event data from thousands of network devices, systems and applications, performs real-time log analysis, and event correlation to deliver visibility, security, and control over your IT infrastructure.		
SolarWinds Server & Application Monitor **delivers performance and availability monitoring, alerting, and reporting for applications and servers.**	SolarWinds NetFlow Traffic Analyzer collects and analyzes Cisco® NetFlow, Juniper J-Flow, IPFIX, sFlow, and Huawei Netstream™ data to deliver a complete picture of network traffic.	SolarWinds Patch Manager is an affordable and easy-to-use solution you can use to manage software patches for Microsoft Windows workstation, servers, and 3rd party applications.	
SolarWinds Storage Manager, Powered by Profiler **provides end-to-end control over your shared storage environment with storage management for virtualized environments.** SolarWinds IP Address Manager **is an easy-to-use, centralized IP infrastructure monitoring and management solution that includes comprehensive IP Address Management, DHCP Management, and DNS Monitoring.**			SolarWinds Network Configuration Manager simplifies managing network configuration files in multi-vendor network environments by continuously monitoring device configurations and providing immediate notification of config changes. It also provides config backup, detects policy violations, speeds troubleshooting, and generates network device inventory reports. SolarWinds User Device Tracker allows you to track and locate users and devices on your network and retrieve user name, switch name, port, port description, VLAN, and more.

Summary

SolarWinds® IT management software solutions deliver actionable intelligence for monitoring, analysis, and prevention of Cyber-attacks. By applying the OODA loop for Cybersecurity and using practical solutions from SolarWinds, one can create a robust and effective Cybersecurity plan that can be implemented easily and cost effective. Learn more about SolarWinds Cybersecurity initiatives.