Leveraging the OODA Loop for Better Endpoint Security

January 14, 2015 / Ryan Nolette / Advanced Threat Protection, Community Perspectives, Detection and Response, Endpoint and Server Security

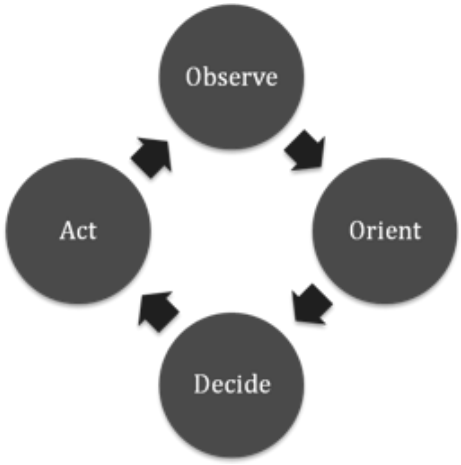
Are you leveraging the OODA (Observe, Orient, Decide, Act) loop or are you just running in circles?

In December 2014, I gave a presentation at ISC‘s Secure Dallas and introduced the OODA loop to a number

of people. After the presentation, we discussed current industry strategies and techniques to better leverage a company's current assets for security. The hottest topic in those conversations was the OODA loop.

In this blog post, I'll discuss how Bit9 + Carbon Black effectively executes the OODA loop and how you can leverage it.

What is an OODA loop?



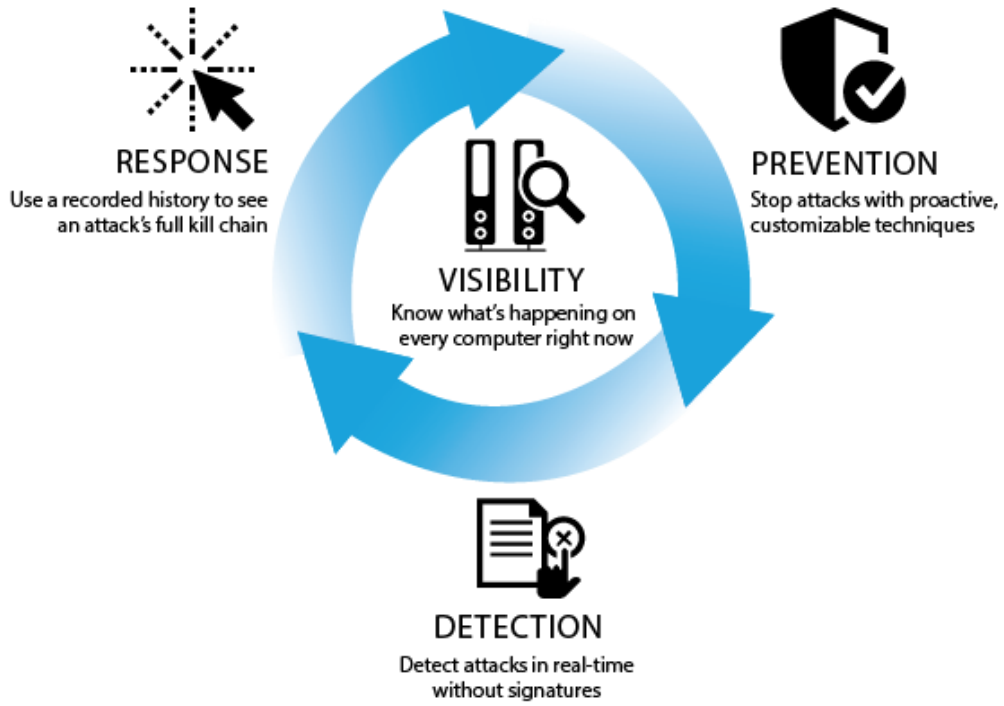
The OODA loop was developed by United States Air Force Colonel John Boyd and is a military decision-making methodology that is shockingly relevant in cyber security. It is a repeating cycle aimed at continuous improvement, with the end goal of achieving the fastest, most effective action. To do this, one must take into account all active components, conceivable situations, and consequences of each action. This is done by prioritizing and excluding the individual acts according to the decision.

The OODA loop consists of four parts:

- **Observe** – Decisions are grounded on observations of an evolving circumstance. These observations are the raw data for assessments and actions.
- **Orient** – Orientation shapes the way we observe, decide and act. Orientation here could be referred to as "tuning." Filtering and analyzing all the raw data according to rules assists in making decisions and taking action.
- **Decide** – From the data observed and filtered, the decision-maker has to select the best possible action.
- **Act** – based on your decision, execute your plan.

This theory matches up very well with the Bit9 + Carbon Black approach to the security lifecycle.

How does Bit9 + Carbon Black help you complete the OODA loop faster than your advisory?



Observe: Bit9 + Carbon Black gives you the visibility to observe what's happening on every computer—right now.

– You have immediate real-time visibility—without sweeps, scans or polls—into the files, executions, network connections, and critical system resources on every machine, and the relationships between them. You'll know how every file got there, what created it, when it arrived, what it did, if it made a network connection, if it deleted itself, if a registry setting was modified, and much more.

Orient: Bit9 + Carbon Black helps you orient yourself with detection. You are able to see and record everything and detect attacks in real time without signatures.

– Bit9's threat research team analyzes threat techniques and creates Advanced Threat Indicators (ATIs) to alert you to the presence of an attack. These ATIs look for the indications of a threat and are not based on signatures. Now, you can detect advanced threats, zero-day attacks and other malware that evades signature-based detection tools—in real time. No waiting for signature file updates. No testing and updating .dat files. No sweeps, scans or polls. You get immediate, proactive, signature-less detection.

– Using watchlists and custom rules, you can customize alerts based on your environment.

Decide: Use a recorded history to see an attack's full "kill chain" and contain and stop attacks.

– When you need to respond to an alert or threat, you'll instantly have the information you need to analyze,

scope, contain and remediate the problem. With the recorded details about every machine, you can "go back in time" to see what happened on any of your machines to understand the full "kill chain" of an attack. You'll also have a copy of every binary that ever executed so you can analyze it yourself, submit it to a third party, etc. You also can contain and stop attacks by globally blocking the execution of any file automatically or with a single click.

Act: Stop attacks with proactive, signature-less prevention techniques.

– With Bit9, you can choose from different forms of advanced endpoint protection. Bit9's proactive "Default-Deny" ensures that only software you trust can run on your machines. Bit9's "Detect-and-Deny" uses ATIs to detect malware and stop its execution, and Bit9's unique "Detonate-and-Deny" automatically sends every new file that appears on network security tools for detonation. If these tools find malicious files, Bit9 will automatically stop them from running on all of your machines—instantly.

So how does this actually work in a real world? Take the below scenario:

Background: *Somewhere out in the cold dark darkness of dark, there is a system administrator deploying Bit9 + Carbon Black in their enterprise. This hero is about to learn just how well that continuous monitoring works…*

9:30 a.m. – An email comes in from "FedEx" about a package apparently ordered that was accidently sent to Florida instead of Boston. Attached to the email is the corrected itinerary in PDF form.

10:00 a.m. – A user clicks on this email that miraculously got through all the spam filters. So it must be legitimate, right?

10:01 a.m. – The user downloads the PDF and then opens it.

10:01 a.m. – Bit9 detects a new file on the network named "Fedex_Invoice.pdf.exe" executing and generates a detection alert. Bit9 then emails the admin staff letting them know what just happened.

10:02 a.m. – An admin opens the email alert from Bit9 and sees what happened. They immediately go to their Bit9 console and check the full extent of the damage. Bit9 shows that the file Fedex_Invoice.pdf.exe executed and is the parent of multiple file artifacts in <AppData>\aefv12m*.

Cut to flashing red lights and alarm sounds in the background. Admins are running everywhere. This is not a drill!!!!

10:03 a.m. – The admin can see the binary that executed. The admin selects the binary and all of its children and selects the option to ban it. Crisis averted. The admin also searches for this binary across all other hosts to see if anyone else has downloaded or opened the malicious PDF, and remediates as necessary.

10:04 a.m. – The admin moves user@clicksoneverything.com to high enforcement so this will not happen again in the future. Future crisis averted.

10:05 a.m. – Admin coffee break. This hero can rest his cape for a while.

Now let's break it down into the OODA Loop that just occurred.

1. **Observe –** The admin leveraged Bit9 here to watch and collect all executions on the host in question. This gave him a huge advantage when the alert came in and made it very quick to read the information about the event.
2. **Orient –**Bit9 also enabled him to quickly filter out all the recorded events to just those from this host during this time period. This greatly reduces the scope of the incident and allows for faster action. Also, Bit9 used detection to send the initial alert that started off the OODA loop to begin with.
3. **Decide –** Now that the admin has limited the scope of the incident, he can quickly find the file in question and all of the child files that the malware has created. He can decide to ban the file, not ban it, create a rule around it, etc.
4. **Act –** The admin drops the ban hammer. Not only does the admin ban the malicious files in question (reactive) but also moves the user to high enforcement (proactive) so this will not happen again. This action greatly increases the efficiency and speed of the OODA loop for the future.

Rinse and repeat.

This same process can be used for Carbon Black.

Until next time, remember my motto: "Flag it, Tag it and Bag it."

Tags: Air Force | bit9 | Carbon Black | endpoint security | Headlines | incident response | OODA Loop