21st April 2014

The DML model

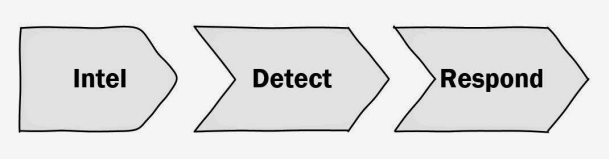
In a different blog post [http://ryanstillions.blogspot.com/2014/04/on-ttps.html] , I discussed TTP's and how they relate to Incident Detection and Response. This blog post will introduce the Detection Maturity Level (DML) model, which builds on the the concepts in that post.

Defined

The Detection Maturity Level (DML) model is a capability maturity model for referencing ones maturity in detecting cyber attacks. It's designed for organizations who perform intel-driven [http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf] detection and response and who put an emphasis on having a mature detection program. Two of the key principles driving the establishment of this model are:

1. The maturity of an organization is not measured by it's ability to merely *obtain* relevant intelligence, but rather it's capacity to *apply* that intelligence effectively to detection and response functions.
2. Without detection, one has no opportunity to respond.

While in practice this is not strictly linear, but you can conceptualize the relationships between your intelligence, detection, and response missions somewhat like the diagram below.



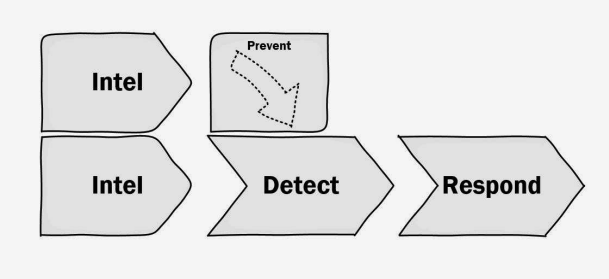
[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhVLQDqaYkKnYM7ohJ2yUbk8AAHm9ruhart2kPmXdqig2NOenodYBwq2me37K3rz-CBED8f4YsKSX5Yne08p9InUnBviwC1sn_W-t77U_UHC0QNWJibZa6A5_nuIBkK8wGA6Ma6EMIh9kEi/s1600/idr.JPG]

This suggests that maturation (or lack thereof) in any prior area will directly influence the ability of the latter to function optimally. In other words, I'm suggesting that one must have their stuff together from left-to-right, and not in the right-to-left reactive "organically grown" model that most IR organizations have been built from.

This diagram often raises the question about prevention and where prevention technology fits into that? Well, since we haven't gotten to the DML yet, now would be a great time to cover this. In short, prevention technology doesn't yield value until you reach a maturity level in which you can use it effectively. Prevention systems are not "set it and forget it" technologies, and deploying them assumes the organization intends to update them as their knowledge of the threat landscape changes. In cases where you know you can safely prevent something, you should. I firmly support Richard Bejtlich's observation that "prevention eventually fails [http://taosecurity.blogspot.com/2006/02/bears-teach-network-security.html] ". When this happens, we still need a mature detection and response function at the ready to detect and respond as quickly as possible.

Secondly, we must be able to independently detect when the prevention technology has succeeded or failed. Blindly ignoring successful preventions can lead to missing out on the intelligence gained from knowing those adversary attempts even existed in the first place. I know this may sound odd on the surface, but for some threat actors temporal analysis of reconnaissance and attack delivery attempts (even when unsuccessful) can be very important to timeline

and campaign analysis.



[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgVGY1h78MxnAZz9AaMKOO4hrfJo_nkynoqD0sq5QsXDk4gunzsXc4kna7-QFDWkAc9BYzsIgPb9fhO4DKYIxay7hYR98UYmGknJdtmJDCJ7dF4ITbp7X3UNic6_DUXD-tamwM6PBDb6eJN/s1600/ipdr.JPG]

This distinction between prevention and detection is important because a successful detection program is based on detecting all forms of adversary activity regardless of whether or not they were stopped, delayed, or aggravated by prevention technology. Detection is the critical junction point to all other functions because it provides the necessary visibility and context which enables us to observe, orient, decide and act [http://en.wikipedia.org/wiki/OODA_loop] . Because of this, the Detection Maturity Level (DML) model is aimed at measuring the efficacy of ones Detection capability.

The DML Levels

The DML consists of nine maturity levels (0-8), with the lowest levels being most technically specific and the highest levels the most technically abstract. That is to say, this is a complete model that appreciates several levels by which present day detection methodologies operating at the host, network, or event log data domains cannot readily master, but human analysts can.

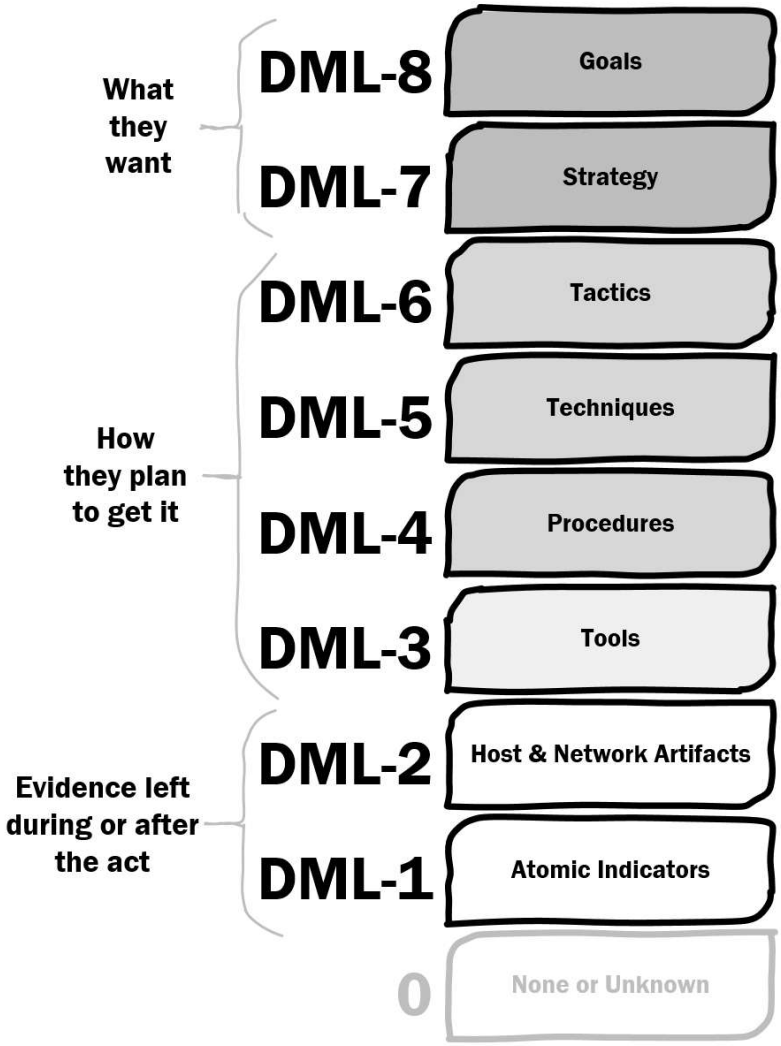
DML-8 Goals

If the actor is part of a larger organized operation they may be receiving their goals from a higher level source or handler. Depending on how organized and sophisticated the adversary's campaigns are, these goals may not even be shared with the operator(s) themselves. In cases of non-targeted threat actors, this may be much less organized or distributed.

Goals are nearly impossible to detect (directly) but they're almost always the toughest question C-level leaders ask about post-breach. "Who was it and why?" These kinds of questions can never truthfully be answered unless you're operating at Detection Maturity Level 8 against your adversary and can prove reliably that you know what their goals are. Short of that, it's guessing at what the adversary's true intentions were based on behavioral observations made at lower DMLs (e.g. data stolen, directories listed, employees or programs targeted, etc). I anticipate less than a handful of organizations truly operate at this level, consistently, against the threat actors they face because it's nearly impossible to detect based on goals alone.

DML-7 Strategy

If the adversary's high level goal is to "replicate Acme Company's Super Awesome Product Foo in 2 years or less" their supporting strategies might include:

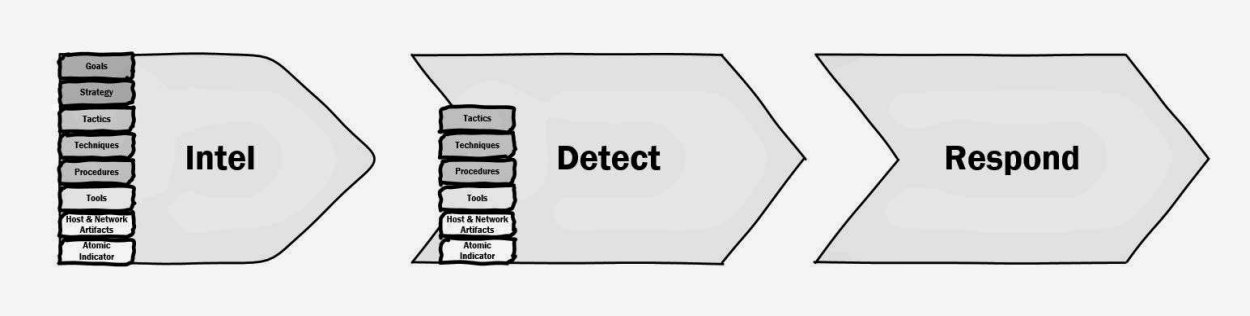


[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhig3sHjjUq3VF8w-_qIFq7Oa0aHGsARZtIwdmIOpIDHhBRaqC5ksG4BC9kcpH12NmhDEbieWtll_W4diPervJaPBztCS_j4IUZP5PXNJcIY0N9G1bGYVFqVMR46sQRXoV7S9VSu4eFumzR/s1600/DMLlevels.png]

1. Implant physical persons into the companies that produce this technology, in positions with physical access to the information necessary to fulfill this goal.
2. Compromise these organizations via cyber attack, and exfiltrate data from the systems containing the information necessary to fulfill this goal.

For less targeted attacks, the strategy may be completely different, with shorter durations or different objectives.

The important distinguishing factor about Goals (DML-8) and Strategy (DML-7) is that they are largely subjective in nature. They are very non-technical, and are often reflective of the adversary's (or their handler's) true intentions (and strategies for fulfilling those intentions). They represent what the adversary wants. For these reasons, they are not easily detectable via conventional cyber means for most private organizations. It's very common for DML-8 or DML-7 to not even be on the day-to-day radar of most Detection or Response specialists, and if they are it's typically in the context of having received a strategic intelligence report from an intelligence source about the adversary.



[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjSogICUFPRxH8z8qSvBVZ3rnl5-QDxBuAFKauqqvxYzAKegwJ1BsXdU8yXKcgNyoNG4jgSND0u8ApETxcaRKJlf_fvpqEVKRkskesJsfFh1FT10kW7F8uaEeu85CHvfm86jmvj2CdSS8WD/s1600/idr2.JPG]

This is an important distinction regarding downstream consumption of disseminated threat intelligence, as it relates to our detection and response missions. Assuming you even have access to a mature intelligence resource capable of disseminating a complete DML-1 through DML-8 profile of an adversary (most organizations don't, which is a topic for another day), the top two levels (Goals and Strategy) can't even be consumed by most detection technologies. Their technical contribution to the detection & response mission becomes largely supplementary, but they do lend situational context to the responders which could be of great value. A common assumption of junior intelligence analysts is that downstream consumers only care about atomic indicators that can get automated into detection technologies, and this couldn't be further from the truth. In fact, the more mature the detection and response functions become, the higher in the DML they expect to consume threat intel. Hence, a higher Detection Maturity Level.

The next three levels of Tactics, Techniques, and Procedures are distinguished in my other post here [http://ryanstillions.blogspot.com/2014/04/on-ttps.html] , but in regards to their application of the DML, they are as follows:

DML-6 Tactics

To successfully operate at DML-6, one must be able to reliably detect a tactic being employed regardless of the Technique or Procedure used by the adversary, the Tools they chose to use, or the Artifacts and Atomic Indicators left behind as a result of employing the tactic. While this may sound impossible on the surface, it absolutely is possible. In nearly all cases, tactics are not detected directly by a single indicator or artifact serving as the smoking gun, or a single detection signature or analytic technique. Tactics become known only after observation of multiple activities in aggregate, with respect to time and circumstance. As a result, detection of tactics are usually done by skilled analysts, rather than technical correlation or analytics systems.

DML-5 Techniques

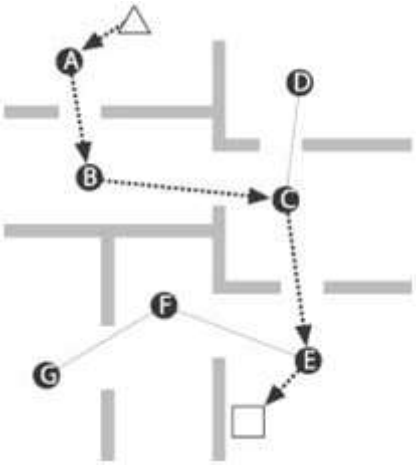
From a maturity perspective, being able to detect an adversary's techniques is superior to being able to detect their procedures. The primary difference being techniques are specific to an individual. So when respecting this distinction, the ability to detect a specific actor operating within your environment by technique exclusively is an advantage. The best analogy to this is a rifled barrel, which leaves uniquely identifiable characteristics in the side of a bullet. Because of this, ballistics specialists can forensically match a spent round to the exact weapon from which it was fired with a high degree of certainty. Not just any weapon by calibur or model, but the exact weapon used to fire that specific round. Human beings are creatures of habit, and most adversaries aren't aware of the fact that every time they attack they're leaving evidence of their personal techniques behind for us to find. The same applies for the tool builders writing the tools these adversaries use. It's our obligation to find these distinctions and ensure we're looking for them. It's

[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhfys3Up574a_twF6d6zzDOKU-lHk_fm6QWCNf3oz-V5O8eBNQDMd_O-Xv73iT9KVL4nAPcoPa1AiKXHjqtxuSgdu7t4Yys7jXb3AMFspMOPA1gy_DxbNdbJQ8VdMP_80C8gkuHKddIuq8w/s1600/220px-Zuege.jpg]

personal behavior and habits that are the hardest for humans to change, so put the hurt on your adversaries by finding creative ways to detect their behaviors and habits in your environment.

> **"*Do not repeat the tactics which have gained you one victory, but let your methods be regulated by the infinite variety of circumstances.*" - Sun Tzu**

DML-4 Procedures



[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiFuRV1ep2cRwkHLIq6cjAORTKfAMm2IcKRQwZEPMys_HVb49jUa_5Ii1nD3h0wwh7fPQCARAWFUjSudP0QVsohzau8guIETowYIxCGusiJhrZU3b1mIE2AiZ9NJE0IQBUEedcl-eKxI8cK/s1600/Waypoints.png]

Given today's detection technology, and readily available correlation and analytics techniques, it's amazing that more organizations haven't reached Detection Maturity Level 4 for most of their adversaries. Procedures are one of the most effective ways of detecting adversary activity and can really inflict the most pain [http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html] against lesser experienced "B-teams". In it's most simple form, detecting a procedure is as simple as detecting a sequence of two or more of the individual steps employed by the actor. The goal here is to isolate activities that the adversary appears to perform methodically, two or more times during an incident.

A great example of this is pre-exfiltration reconnaissance that often occurs during the Act on Objectives phase of the Kill Chain, when most predictably, the adversary systemically connects to victim systems one by one performing directory listings, and dumping those results to a file that is later extracted and exfiltrated. From here, you might as well start the countdown timer because it's only a matter of time before they come back to swiftly collect specific data for exfiltration. I've always viewed this directory listing procedure as one of the very last events before "things heat up" for a victim organization. One would have reason to believe that this textbook example of a procedure being performed over and over would be a priority for most detection programs, yet to this day many organizations fail to detect this activity on their endpoints.

Incidents are chalk full of procedures. Anyone having performed significant timeline analysis of decoded C2 commands knows what I'm referring to. It doesn't take long after reconstructing a sequence of events temporally for you to start picking out patterns of repeat behavior. Those patterns are indicative of procedures and become detection opportunities unto themselves. It's important to not only pay attention to the steps, and the repetition of those steps, but also the dwell time in-between each step of the observed procedure. Are they fast? Does it appear scripted or manually run? If manually run, do they ever make a typo somewhere along the way? If so, how did they react? I recall once watching an actor try feverishly to get pwdump to run, passing all sorts of syntactically incorrect command line arguments to it, before ultimately giving up and moving onto another box. This not only confirmed manual interaction, but also gave us a sense of the actor's skill level. Some actors get through their procedures faster than others. When comparing multiple hosts involved in a compromise, observations as subtle as the dwell time between commands across hosts can indicate if there are multiple operators in the environment working together as a team, or just one. These are all very important factors to record. This same information can also be used to train your detection methods for efficacy and false positive reduction.

How many detection signatures or correlation rules do you have that are strictly based on detecting these kinds of procedural events? If the answer is "not many" you are probably not inflicting much pain [http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html] on your adversary yet.

DML-3 Tools

Being able to detect at DML-3 means you can reliably detect the adversary's tools, regardless of minor functionality changes to the tool, or the Artifacts or Atomic Indicators it may leave behind. Detecting tools falls into two main areas. The first is detecting the ***transfer and presence*** of the tool. This includes being able to observe the tool being transferred over the network, being able to locate it sitting at rest on a file system, or being able to identify it loaded in memory.
The second, and more important area of tool detection, is detecting the tool reliably by ***functionality***. For example, let's take a given webshell that has 25 functions. If we want to claim DML-3 level detection for this webshell we have to exercise each of those 25 functions and understand what each of them do. What do they look like at the host, network, and event log level when they are exercised? We then aim to build detections for as many of those 25 functions across those data domains as we possibly can, reliably, balancing false positives and other constraints. The reason behind this is simple, we want to be able to detect this version of the tool and as many future variants of the tool as we can by function that it performs. If the adversary decides to change up 5 of the 25 functions for which we have detections, we're still detecting the entire tool. In order for the adversary to use this tool completely undetected in our environment, they'll be forced to change every one of those functions; or at least the ones that we were able to reliably build detections against.

Realistically, DML-3 is an area that a lot of technology vendors are trying hard to operate at today. The problem is that they're not doing it very effectively. Take a look at commodity virus detection software. Because of the sheer increased volume of malware samples, they've automated away the detection creation. This reduces the efficacy of the detection technology because they're often only detecting just one or a few of the functions of the malware. Obviously, there has

[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj2ldlej9fWkmmFgEXwvvIrvo4Usc3ojx_5N0TP5qiqCnnZssv4DqTDHQ96h60X17IvIuy-FYQoINH86tKsmL3PBI_0ZM9GQWuCi9Z8rb4ZTD0Dmb3Yp5E_gIC0aHLrAGBi4aRgYEY2P4y2/s1600/Glazier_tools.JPG]

to be a balance. We can't reverse engineer every binary, and write holistic detection for every function it performs across all data domains, but in cases where you absolutely HAVE to bring the hurt to your adversary, this is the level of detail one must go to in order to operate at Detection Maturity Level 3. Find their tools, and deny them the use of those tools in your environment by building detection for a majority of it's functions, then monitor with each new incident how the adversary changes their toolset over time and update accordingly.

How many detection signatures or correlation rules do you have that are based on detecting adversary tools in this fashion? If the answer is "not many" you're definitely not inflicting much pain [http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html] on your adversary.

DML-2 Host & Network Artifacts

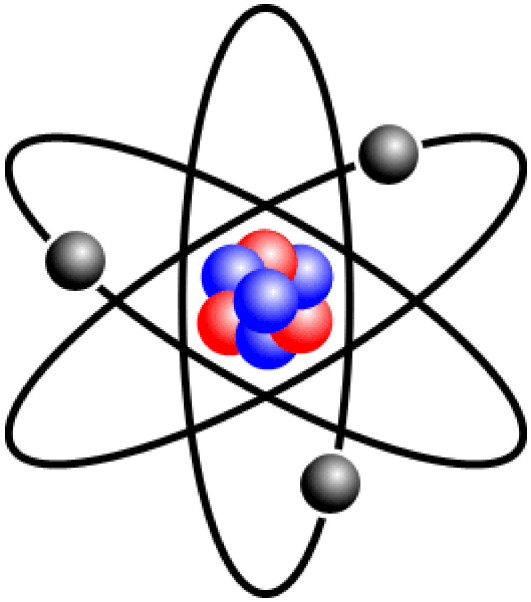
[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEizxw_fzKqC8VEIqa3mLxW4LGwCaqCzUXxioQaFqzyYqX99mQc9SgE41UvFgG2QO_1YsOBs8pCRKm5b5ntEMc3wxeri1mMXk-6pH0IZFLJJYTWDM7XFcEI0QVOi5t_0hLQmFJRQpdVcz2yY/s1600/1024px-F-22_Raptor_vapor_trails.jpg]

DML-2 is where most organizations spend too much of their resources; attempting to collect what they call "threat

intelligence" in the form of Host & Network Artifacts. The reality is, these are merely just indicators that are observed either during or after the attack. They're like symptoms of the flu but not the flu itself. I often use the analogy "chasing the vapor trail" when I think of DML-2 because chasing after Host & Network Artifacts is much like chasing the vapor trail behind an aircraft. We know the enemy aircraft is up there in front of us somewhere, if we just keep chasing this vapor trial we'll eventually catch up to the aircraft and find our enemy right? Wrong. Having a mature detection and response program means your operating above DML-2 and you're actually locked onto the aircraft itself. You know how it operates, you know what it's capabilities are, you know the Tactics, Techniques, and Procedures of it's pilot and you can almost predict what it's next moves might be. This is precisely why good Cyber Intelligence Analysts will almost never attribute activity to a specific threat actor, group, or country based on just Host & Network Artifacts alone; they understand this DML concept and realize when they're likely just staring at the vapor trail. They understand that in reality the vapor trail (indicators) could be from any number of aircraft (tools), with any number of pilots (actors) behind the stick.

Host & Network Artifacts are vitally important. I don't mean to de-emphasise their contribution to detection and response, but they should be thought of as the individual building blocks that support our work at the higher levels. They should not be the premise for putting alerts in front of analysts, and they definitely should not be what wakes us up at 3AM when the pager goes off. If this sounds like your organization, stop chasing the vapor trail and start thinking about how you can drive your detection program up the DML to a higher maturity level.

DML-1 Atomic IOCs



[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiWDNwQssDYYsBICq1szQrKIJSroKhG496Pc6OX7SFwer8DWkBUZM9KZe4OhKj0ZewLaa2qNw4n7g6ARqVHzqmoOJMUns8y_Bo9Ir3YFgS2ZCci9hFCYJyAuUoCGpeMp2xfOo4rQbz17chm/s1600/Stylised_Lithium_Atom.png]

These are the atomic particles that make up Host & Network artifacts. If you're detecting at Detection Maturity Level 1, it means you are probably taking "feeds of intel" from various sharing organizations and vendors in the form of lists, like domains and IP addresses, and feeding them into your detection technologies. Let me be clear on my position here. There are a few, and I mean a very precious few, circumstances where this makes sense and can be done reliably. These are edge cases where specific atomic indicators have a high enough "shelf life" where it makes sense to go ahead and create detection capabilities from them. Examples of this include unique strings found inside a binary, or perhaps an adversary is foolish enough to sit on the same recon, delivery, C2, or exfiltration infrastructure allowing you to detect reliably on their domain names or IP addresses. These might be viable cases where detecting on atomic indicator alone makes sense. Unfortunately, for the remaining 99% of the time, attempting to detect on this kind of

data is suboptimal, for a number of reasons.

1. The rate of change on the data is extremely high. If you don't believe me, just count the number of new atomic indicators you collect each year vs. the number of tools or TTPs you collect. There's a cost associated with collecting, analyzing, and managing this data. Does it make sense to do this for data that has a high rate of change, but yields a low alert-to-true positive detection ratio?
2. It usually doesn't inflict much pain [http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html] on the adversary.
3. It usually inflicts a lot of pain on your detection technology. Believe it or not, every technology has a glass performance ceiling under which it can operate. Do you know how many atomic indicators you can shove into your detection technologies, SIEMs, and the like before they start dropping packets, missing events, or malfunctioning in unexpected ways? Is it five thousand? Ten thousand? If one doesn't know the answers to these questions they are most likely missing things (to include true positive compromises) and not even knowing it. The most tragic of circumstances is when a high value detection capability (DML-3 or higher) fails to alert because the hardware or software is struggling to keep up processing all the DML-1 and 2 based detections. This kind of self-inflicted Denial of Service attack on your own detection infrastructure, is a real problem for many organizations and many of them aren't even aware of the fact that they're doing it to themselves. I once dashboarded out the interface packet loss of a global NSM sensor deployment using a simple Splunk dashboard, just to quantify the impact of this problem. Needless to say it went over with varying levels of popularity, but it proved my point nonetheless. Operating at lower levels of the DML have a real measurable impact on technology.
4. It usually inflicts the most pain on your staff. This is by far the worst side effect of operating at DML-1. A company cares enough about addressing the threat head on that they make investments in all the right places. They start by hiring sharp, talented professionals, augmented with professional services from leading vendors. They buy themselves some prevention and detection technology. Then the organization makes the fatal mistake of shoveling atomic indicators into those systems by the truckload, expecting their responders to sift through the mountains of noise. Do your team a favor, and turn off all alerts unless they are Detection Maturity Level 3 (Tools) or higher, OR, they're proven to be so high-fidelity they're absolutely worth keeping on. Operating at lower levels of the DML has the most impact on your analysts, which can be difficult to measure until after they've long left the organization.

DML-0 None or Unknown

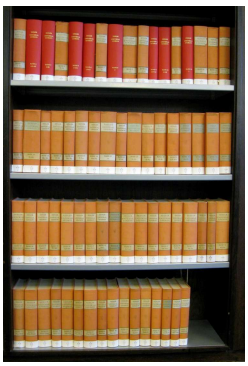
For organizations who either don't operate at DML-1 or higher, or they don't even know where they operate on this scale, we have Detection Maturity Level - 0. Instead of pointing out all the negative things associated with this level, I'll take the high road and lend a bit of positive encouragement. Congratulations, you are at ground zero. It can only get better from here.

Four use cases for leveraging the DML today

1. Providing a lexicon for easier communication

In this field of detection and response, we often talk past each other. While one person communicates their thoughts about detecting a lateral movement technique, the first person receiving that message might be thinking about the low level atomic indicators, while the second recipient of that same message may be thinking of the tools they use to accomplish it.

I once spent an entire week locked in IR strategy discussions with a large group of coworkers, many of whom I respect



[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjasn2qi8kzmSrUtDR8HzqiExeN1zmW_fCZep7I0ABp7PeeivAeuUxt3CnQFbhXS4oU_8IW6oZJfHrBfXKZYjauJXAGDnTkAG0qH7fJVq_b9d1yYTCY4njkefnkgCuE9JHmTh9aGY1eczML/s1600/UBN_Zedler_Universal-Lexicon.JPG]

as some of the most talented IR folks in the industry, and for several days we all talked past each other. We all meant the same thing, but had significant differences in how we shaped it in our minds and communicated our thoughts. Sometimes having something as simple and easy to understand as a lexicon can help put us all on the same page.

2. Assessing Your own Detection Maturity

One initial step organizations can take immediately is to stack this DML model up against all of the known & unknown threat actors that you track. Is your current Detection Maturity Level sufficient for this threat actor? If not, what additional information do you need to get to the next level?

Detection Maturity Level	Threat Actor Alpha	Threat Actor Bravo	Threat Actor Charlie	Threat Actor Delta	Threat Actor Echo	Threat Actor Unknown1	Threat Actor Unknown2	Threat Actor Unknown3	Threat Actor Unknown4
DML-8 Goals									
DML-7 Strategy									
DML-6 Tactics									
DML-5 Techniques									
DML-4 Procedures									
DML-3 Tools									
DML-2 Host & Network Artifacts									
DML-1 Atomic Indicators									
DML-0 None or Unkown									

[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgb96pIl2v1LDkhGYYGX5V438faNgeGuws5vC1ezc_awZH1B_2T5EAiwCvU7X7fovLGIhYtRZ_qRo5S2MQpgbTX4tNhmmtrL0v427gj4sO-8PDRww9N5_Xk8RJXtieDoQTDVFop_58f73Bz/s1600/DMLsByActor.png]

3. Assessing the maturity of a security product or service provider

Take this DML model and use it to evaluate the quality of a vendor or service providers' detection capability. It's easy for a vendor to claim they can protect you against "today's threats" but stack them up against the DML and start asking them tough questions like how they intend to prove they can prevent or detect at each of the DML levels. If you peel the layers of the onion back far enough, many technologies are only operating at DML-1 or DML-2 under the hood, and have marginal effectiveness at the higher levels.

Detection Maturity Level	Network IDS Vendor Alpha	Network IDS Vendor Bravo	Threat Intel Provider Alpha	Threat Intel Provider Bravo	SIEM Factory Correlation Alerts	SIEM Custom Correlation Alerts	Host Detection & LR Tool	Host Detection & LR Tool
DML-8 Goals								
DML-7 Strategy								
DML-6 Tactics								
DML-5 Techniques								
DML-4 Procedures								
DML-3 Tools								
DML-2 Host & Network Artifacts								
DML-1 Atomic Indicators								
DML-0 None or Unkown								

[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiSoJvl-YORRdBu-NSCjkZuqGfZ4uUgRKReYv7zjZFz9kVdAE63ZE-7r3K0Ywew6fDZheeFMWZ5VP3oLbz3v4eTZ3h3hoQ2DQqqV_JDwOsK-SS2sGV6D9W2XLjlESpGYmx4ms0DOSWjPhpV/s1600/DMLbyVendor.png]

Intelligence Management systems are a relatively new space. While I won't go deep into this topic at the moment, ask yourself if your intelligence management platform helps you perform this kind of analysis. If your upstream sources are providing you with some form of consumable "intelligence product" or "intel feed" (and I use those terms loosely) stand them up against this model and ask yourself if they're providing information in each of the Detection Maturity Levels. Most organizations are good at providing feeds of DML-1 / DML-2 type data, with written reports that describe DML-6 (Tactics) in more of a paragraph descriptive form. Do they include Techniques, and Procedures? Do their DML-3 (Tools) level reports explain the full functionality of the tool and how to detect it across host, network, and event based data, or does it merely report the Host & Network Artifacts left behind as a result of running the tool? Worse yet, does it just give you the Atomic Indicators like the callback C2 information?

Most importantly, does the product or service provider furnish this information in a format that allows you to navigate up or down through the relationships that exists between these levels. Given any Atomic Indicator like a User Agent string, can you navigate up the relationship tree to all the related Network Artifacts, which are related up to the Tools exhibiting those Artifacts, which are related up to the Techniques and/or Procedures associated with the use of those Tools, and so on. This is threat intelligence in context; being able to give your analysts the ability to rapidly navigate threat intelligence that ties it all together, empowering them to decide if the activity they're investigating matches what the intelligence says they should be looking for, and allowing them to act accordingly. I'm only half joking when I say "If you can't OODA [http://en.wikipedia.org/wiki/OODA_loop] through your intel quickly, you probably have crappy intel."

Also be sure to ask about machine readability at each level. Great work has been done in the area of sharing threat intelligence at the DML-1 / DML-2 levels because those are the levels at which our machines can more easily consume this data. Unfortunately, we all too often shoot ourselves in the foot by losing the context and not retaining the relationships that exist at the higher levels of the DML. Very few product and service providers can provide DML-3 and above data in machine readable formats.

4. Provide more context to your analysts

Starting immediately, you can annotate the Detection Maturity Levels right inside your detection rules themselves. You can bake it into your Snort signatures by using the *classification* rule option with custom classification.config statements. You can include the DML levels in your Yara rules. Think about adding this to your SIEM correlation rules so only the highest of DML rules are generating alerts. There are tons of technologies out there that would allow you to start referencing your existing detection capabilities by what level they operate at within the DML model. Consider

[https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiTeixYdcTR8NRQe4PIpSrO6KPdncDE3P6kU_dikDLuyJntPRbkmWOOLkz-NjnAg2yado3bB5K90a5dtP8sUyhfEzdtvn1bh-nkx-zJtbsPsmWII74jM6ROuQaZIvDOtu6ERIgZ0uP03U_r/s1600/Koebel.jpg]
adding this context to your detection signatures, correlations, and alerts so analysts can begin using them to prioritize response activities. If they understand even the basic premise of the DML this is a great way to give them added context and it also helps jumpstart junior analysts' understanding of the differences between Tactics, Techniques, Procedures, Tools, Artifacts, and Atomic IOCs.

Future use cases?

There are bound to be tons of additional use cases we've not discussed here, and I plan to post a few follow up blog posts relating to different applied DML use cases in the future. As always, I would love to hear your feedback and if you thought this post was useful. I'm especially interested in hearing how others have applied the DML in their organizations.

Ryan

email: ryanstillions@gmail.com [mailto:ryanstillions@gmail.com]
twitter: @ryanstillions [https://twitter.com/ryanstillions]

Posted 21st April 2014 by Ryan Stillions

Load more