A Fresh Look At
SECURITY ANALYTICS

ThreatConnect's Drew Gidwani on the Promise of Orchestration

THREATCONNECT®

iSMG
INFORMATION SECURITY
MEDIA GROUP

Drew Gidwani

Gidwani is the director of analytics at ThreatConnect. He drives data modeling, collection and analytics both within the core ThreatConnect platform and in CAL™. Previously, he worked for the Department of Defense, where he leveraged his varied analysis experience to scale growing intelligence teams in the face of ever-changing threats.

Most enterprises are at least discussing security analytics. But how are they actually deploying these tools? And with what levels of automation and orchestration? Drew Gidwani of ThreatConnect shares insight on how to maximize analytics.

How are security analytics commonly deployed today?

"It really depends on the pattern you're looking for and what you're trying to predict," says Gidwani, director of analytics at ThreatConnect. "It's interesting to slice and dice it based on the size of the data you're looking at, or the computational nature of the problem at hand."

Gidwani looks at data in three categories: "regular" data, big data and "too-big-for-you" data.

In an interview with Tom Field, senior vice president of editorial at Information Security Media Group, Gidwani discusses:

- How security analytics is commonly used today;
- The potential of automation;
- How orchestration impacts efficiency and scale.

Defining Analytics

TOM FIELD: Drew, everybody is talking about analytics today, but what is analytics beyond just a popular buzzword?

DREW GIDWANI: It's really an investigative way to look for patterns in data, usually with the hope of predicting some kind of future outcome.

In security, we obviously have a very difficult job. We're trying to go up against human adversaries that can be well-funded and well-trained. And generally they only have to be right once to make our lives really difficult. Anything that helps us shift to proactive identification of that behavior is a must have.

Tightening timelines for incident responders and network defenders when those adversaries eventually do get through is pretty critical as well. So analytics helps us bridge that gap by identifying those patterns so that we can predict adversary behavior a bit better.

Deployment Trends

FIELD: Talk to me about our security industry today. How do you see analytics being deployed?

GIDWANI: It really depends on the pattern you're looking for and what you're trying to predict. I could sit here and talk for hours about the different kinds of analytics that we see out there. It's interesting to slice and dice it based on the size of the data you're looking at, or the computational nature of the problem at hand.

“Having orchestration means that your automation itself can be put to work in a way that’s actually a force multiplier.”

There are three kinds of categories that I like to put these things into. You’ll probably hear people talk about big data. You may hear people talk about data that’s just “too big for you.” And then there’s regular data, which isn’t as sexy so it doesn’t get talked about as much.

Starting from the bottom with regular analytics, any time you’re asking a question of your data to figure out a pattern, even if it’s a completely manual thing, you’re doing an analytic. If you’re asking whether this ASN is a bad neighborhood for an IP address to live in, that involves you looking for a pattern that would help you take proactive action against future IP addresses that you might see. You’re kind of convicting them by association, and that predictive behavior is really helpful.

That data can get too big for you pretty quickly. And I draw the line there based on things that are too big for an individual or a team just based on the resources that they have available. How do you actually say that that ASN is a bad neighborhood for an IP address to live in? Do you have enough information about all the constituent IP addresses that live there to make that determination? What’s you’re heuristic for doing that? And how timely is that information? And how confident are you in all of that? That quickly becomes a little intractable for a team or for an individual to do adjacent to their day job.

And then that “too big for you” data can truly become big data if you start to collect even more things around it. And when those things just become too computationally intensive to do without some really cool technology, you start to have to move into some specialized means and methods to get it done. That could be disparate data sources that need normalizing, or if you want to start doing time series analysis. If you wanted to profile every single IP address in that ASN and maybe every domain that resolves to every one of those IP addresses and then start looking for changes that might indicate malicious behavior, now you’ve got a really big information need, a really big computational need.

That’s really just one example. There’s analytics for discovery reputation, classification, prioritization. I could go on forever and name other things that end in “ion.” The key, though, is that there are a lot of different types of information needs, and each of those information needs could be tackled at different scales. And even if you are taking a bite out of that, it can be really tough to gauge how well an analytic is performing when you’re doing your day job fighting fires in the SOC or as an incident responder.

Collective Analytics Layer

FIELD: So Drew, it’s easy to see that people could be at risk of information overload, maybe even paralysis. What can be done to make sure that these analytics are actually helping the people as they’re intended to?

GIDWANI: As I mentioned before, if an analytic is meant to be predictive, then we can be helpful by making sure that those predictive insights are being delivered in an actionable way. And in order to do that, you really need to tailor the insights and analytics, and how they’re being delivered based on the consumer and information need that you’re answering.

So, for example, CAL™, our Collective Analytics Layer, provides a lot of human readable context for an analyst. One simple example is that CAL can tell you if a particular IP address is owned by Amazon, it’s used for their AWS infrastructure, etc. So an analyst who’s in the middle of an investigation and encounters that knows how to handle that appropriately.

ThreatConnect’s CAL™ also provides classifiers so that all of the machines that are reading information about that IP address can categorically take actions – like block or white listings based on that information. And there are other types of analytic outputs like indicator reputation, which can be a simple score. We use a 0 to 1,000 scale. That allows both types of consumers to make use of that information. And so, in general, if those insights are tailored appropriately for that information need and for the actions that the consumers themselves need to take, then you’re going to be less of a risk than increasing the overload.

Orchestration

FIELD: Drew, you talked about machines as consumers. Can you explain how people can start to automate analytics in their security operations?

GIDWANI: There are a lot of problems with information overload, like you mentioned. I like to look at it both within a team and across teams; you've got different sets of problems. Within a team, you largely have to worry about scale and the "too big for you" kind of problem. Even if you've got great analytics people, they just get fatigued when they're presented with too much information, no matter how valid it is.

A good analytic will probably bubble things up at the top. If you can prioritize things appropriately, save people time on actions, all that stuff can be pretty critical when it's automated. We've had this in the industry for a while; now you can click a button to perform an enrichment or a look up. Analysts used to have to do all that stuff manually and copy and paste into spreadsheets and emails and all that sort of stuff. And it's good that that's no longer the norm.

But, a good analytic will tell somebody that they need to push that button a thousand times, and here are the 50 really critical ones that you need to start with.

When you start working across teams, things get a little stickier. You've got disparate processes; you've got people with different access levels; you've got people who have different information needs. So the ability to orchestrate these processes in a repeatable fashion is the Holy Grail. And we're starting to move in that direction as an industry.

Having orchestration means that your automation itself can be put to work in a way that's actually a force multiplier. Those enrichments that you got by pushing that button can now drive SOC or incident response processes way faster. And as they finish their investigations, the artifacts that come out of that can juice any further intel-driven investigations and that cycle can continue to feed itself.

"It can be really tough to gauge how well an analytic is performing when you're doing your day job fighting fires in the SOC or as an incident responder."

The Risks

FIELD: Given the emphasis on efficiency and on scale, what are the risks for an organization that fails to adopt orchestration as you described?

GIDWANI: Well, I think you're going to have one of two issues. Either you're going to have to stop growing or way more likely you're going to outgrow your defense capabilities as an organization. We can discount the first one. It's not realistic for SOC or IT managers to tell their leadership: "Sorry boss; we're not going to deploy 1,000 new laptops to that new work site. I don't think Drew over there has the bandwidth to track them." Those laptops are going to get ordered, and that new work site is getting its new network. And if you're an IT or a security professional, you basically just inherited that juicy new surface area as far as an attacker is concerned. At some point we hit this asymptote when it comes to manpower. You can't just say that for every X laptops we're going to hire Y more security people. There's not an infinite pool of security people out there; that doesn't really scale well. Those security people are very expensive.

And the funny thing is that with the investments that you've already made, you should, in theory, be getting more information as you deploy more assets. It's a network effect; it's the opposite of the diminishing return. The beast that hungers for information can be better fed assuming that you can digest it.

Orchestration is the only way to make sure that those insights can still be gleaned at scale across all those different teams and across those geo boundaries. How do you get the telemetry from those 1,000 laptops and the new network infrastructure at that work site? How do you swirl that in to all the other telemetry that you've already got and the thread intel that you're pulling in? Even if you find something suspicious, what do you do? How do you reach out to that new work site? Orchestration is the only way that you can implement those processes without saying: "Well, we'll just hire five new security people."

Some places do hire five new security people and then they end up having a lot of budget issues down the line because they can't keep up with the new information needs.

"Being really aware and honest about those gaps should help you identify the best opportunities where you can fill them with analytics and orchestration"

Help With Orchestration

FIELD: So talk to me about what you're doing at ThreatConnect. How are you helping organizations succeed in orchestration?

GIDWANI: We're trying to focus on getting that network effect fully operationalized in people's IT and security programs. Generally getting all of that stuff into one place is a solvable problem that isn't entirely solved in the industry. Similarly, normalizing that information is solvable, but not entirely solved in the industry. Adding analytics and orchestration on top of that is another tier of issues that we're tackling pretty aggressively. We want to make sure that those human and those machine consumers that we talked about, regardless of what team they're on or what function they have, can work together at the scale they need to. That means a lot of automation, a lot of orchestration, a lot of processes being captured. And, more importantly, those processes also need to be measured. ... Beyond the core platform where we do all that, we use CAL, which I mentioned earlier, and that adds our own expertise and trade craft on top of your data set.

CAL can answer questions on millions of artifacts, or tell you about something before you even know to ask about it, which makes all the problems that we talked about so far way more trackable.

Advice

FIELD: Drew, a final question for you. If you were to boil it down to a single piece of advice for someone who's looking to start implementing some analytics or orchestration in their security program, what would that advice be?

GIDWANI: Orchestration does what it says on the tin. It takes a disparate set of pieces and it makes them work together. For that to work, each of those pieces has to understand their role and be able to execute it well.

A good coach knows when to put which players into which situation in the game, which plays to call and so on. But there's also an onus on the players to practice and know the playbook and all that. If you're looking to dip your toe into orchestration and analytics, I'd recommend ensuring that you have a very firm grasp on what processes you're doing manually and where you're running into trouble. Where are they working? Where are they not working? The last thing that you want to do is add automation to the wrong thing and then end up scaling up a mistake into a really big mess.

I mean, none of us has all the pieces that we feel we want in our job. None of us can say that all those pieces are firing at 100 percent. But being really aware and honest about those gaps should help you identify the best opportunities where you can fill them with analytics and orchestration. ■

Listen to the full interview at https://www.bankinfosecurity.com/interviews/fresh-look-at-security-analytics-i-4098

About ISMG

Information Security Media Group (ISMG) is the world’s largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

About ThreatConnect

In 2011, ThreatConnect’s founders decided to disrupt the cybersecurity market with a unique way forward for measuring, minimizing, and mitigating threats. Their belief? That organizations require security operations as scalable as attackers ’- to close the gap between compromise and detection for immediate response or even better, to get ahead of their attacks. Their goal? To shift the paradigm and address cybersecurity’s lack of automation, analytical tools, and actionable insights. But timing is everything, right?Some thought they were too early to the marketplace. But unconcerned with how to fit in with the industry status quo, the founders risked charting a non-traditional approach to security models, knowing that when their product was ready, the market would be too – and they were right.ThreatConnect was born from this vision. And our core concepts were pioneered around threat intelligence. Today, ThreatConnect offers the industry’s only extensible, intelligence-driven security platform.

Contact

(800) 965-2708 • threatconnect.com

BANKINFO SECURITY® CUINFO SECURITY® Just for Credit Unions GOVINFO SECURITY® HEALTHCAREINFO SECURITY®

infoRisk® TODAY CAREERSINFO SECURITY® Data ~~Breach~~. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io