A network diagram with orange lines connecting various nodes. Several nodes are represented by a cloud icon inside a circle. The background is a light blue gradient with a faint, larger-scale version of the network diagram.

The State of Cloud (In)Security

FireEye's EVP & CTO Grady Summers on
What's Needed to Bolster Cloud Security Strategies





Grady Summers

As executive vice president and chief technology officer at FireEye, Summers oversees the global CTO team that supports R&D and product engineering. He joined FireEye through its acquisition of Mandiant in 2014. At Mandiant, he led the company's strategic consulting and customer success divisions. Previously, he was a partner at Ernst & Young, responsible for the firm's information security program management practice, and CISO at General Electric, overseeing a large global information security organization.

FireEye is in a unique position to see global cybersecurity threats, threat actors and their impact on breached organizations. Grady Summers, FireEye's CTO, discusses how organizations can use staff and intelligence to bolster their cloud security defenses in 2019.

"It almost feels cliché, because every year we say 'the threat landscape continues to evolve' ... but this really was a unique year in terms of the types of actors we saw and threat vectors they're going after," Summers says. "We're starting to see more and more attacks against cloud infrastructure."

In an interview with Tom Field, senior vice president of editorial at Information Security Media Group, Summers talks about:

- The evolutions of threat actors and vectors;
- Where enterprises are most vulnerable;
- Key challenges to overcome in strengthening cloud defenses.

Evolving Threat Landscape

FIELD: How have you seen the threat landscape evolve this year in terms of both the attackers and their attack vectors?


SUMMERS: It almost feels cliché because I feel like every year we say, "Oh, the threat landscape continues to evolve." This really was a unique year, though, in terms of the types of actors we saw and the threat vectors that they're going after. At FireEye, we do a lot of research into the threats, and this year, if I look back, we talked about emerging threat actors out of North Korea with APT 37 and APT 38, both of whom we wrote reports about this year.

We exposed a big Iranian influence operation that impacted Facebook in a pretty large way and had a lot of media attention around that. We saw APT 10, an actor we've tracked for a while, targeting Japanese companies in a new way. We talked about Triton malware that attacked ICS environments. We saw Fin7 in the news. You go on and on.

China seems to be back after a few years of laying low. We saw them using groups like TEM Periscope targeting Cambodia in front of their elections and targeting engineering and maritime companies. You could go on and on down the list, right? ... It's old threat actors coming back and targeting new industries.

And then in the vectors, we've started to see more and more attacks against cloud infrastructure. Because more and more of our clients are moving to the cloud, it would make sense that the threat actors follow there. But that's something new as we do more and more investigations that start to touch on public cloud properties – assets that are workloads running in AWS or Azure.

So it's certainly been a continued evolution and continued targeting of organizations in different ways and new vectors.



“In so many ways, we see security being better in the cloud.”

Security in the Cloud

FIELD: So Grady, to follow up on that, where do you see organizations the most vulnerable to attack, particularly when it comes to cloud defenses?

SUMMERS: Well, I don't know that organizations are really more vulnerable to attacks when they're targeting the cloud. In fact, in so many ways, we see security being better in the cloud. It seems kind of counterintuitive, because for years organizations have been a little bit reluctant to move to the cloud feeling that “Well, I can't have my hands on it, it's not in my data center, maybe I'm lacking visibility.” We find that if instrumented right, though, ... public cloud environments at least tend to have better visibility. It's just a matter of making sure that organizations are harnessing some of the built-in telemetry that you get from those Azure tenant logs or the AWS cloud trail logs.

We find visibility can often be better, but organizations have to grab that, have to know what to look for and have to make sure they've got that on hand in case they need to do threat detection or incident response. So it's partly making sure you've got that visibility, and then a big part is making sure you have the expertise to analyze a different sort of telemetry than what you might be used to when you have the servers in your own data center.

Playing Catch-Up

FIELD: For organizations that lack the visibility, lack the expertise, how do you see their enterprises being impacted?

SUMMERS: Well, it often means that organizations are caught a little bit flat-footed. So sometimes we'll get a call from an organization that needs help doing incident response because they think they've been breached. Some organizations have done pretty well to start to get the right data up front that they need for detection and response in the traditional IT infrastructure. Some ... organizations that have started to put workload in the cloud without thinking these processes through in advance are kind of scrambling.

So you say, “OK, have we been capturing those cloud trail logs? Can we go back and get them? Do we have VPC flow logs available to us?” I think it impacts those organizations because they often haven't thought about it upfront and we see maybe a little more scrambling. Everybody understands how to send proxy logs into their SIEM or to be capturing DNS lookups in a traditional IT environment. It's just a little bit different in the cloud, so it's just that process of learning – but unfortunately, sometimes learning in the midst of a breach.

Key Challenges

FIELD: You're seeing a range of cloud maturity in the organizations you see. If you were to summarize, what would you say are the key challenges for these organizations as they shape their cloud security strategies for the new year?

SUMMERS: Workloads are moving to the cloud, but the fundamental challenges are the same that they've been for the last several years. ... We see a lack of talent resources in information security in general. Organizations are struggling to have the right folks in the SOC and to have people who then do instant response and forensics. And that doesn't change whether we're talking about traditional IT or the cloud – it's not having that expertise when you need it.

So lack of talent is a constant. Another constant is a lack of actionable intelligence and knowing how to apply it. More and more organizations are starting to pull in threat feeds from different sources – a commercial intel provider or maybe collecting open source intel or they are part of an ISAC that's providing threat intelligence.

So that's gotten a lot better in the last few years. But they don't always know how to apply that efficiently to the data they're getting. We always say that threat data is not the same as threat intelligence. How do you take those data feeds from a provider or from open source and actually turn that into actionable intelligence that you can use in your organization, rather than just having inboxes filling up with lots of threat feeds?

Bolstering Defenses

FIELD: So Grady, if you look at these two areas you talked about, talent and intelligence, what does FireEye bring to the table to help these organizations to bolster their defenses?

SUMMERS: Well, you know, FireEye and our Mandiant division is certainly known for the expertise we have. We're very well known for incident response, and more and more clients are using us for preparedness as well. Proactive organizations are saying: "We're flat-footed and we're behind the ball. And frankly, it's more expensive if we're just calling Mandiant when we get breached. How can we use Mandiant to help develop our defenses upfront?"

So we help fill that talent gap through our Mandiant division. But we also know that when you have an industry like ours with so many open positions and such a shortage of talent, you can't always just throw more resources at it. We have to be smart with technology that enables services. So we're pretty proud of how we try to build what we've learned from consulting into our products.

We talk a lot at FireEye about the innovation cycle, and at first glance it might just look like a marketing thing – have a little cycle that talks about that flow from services and incident response into

“Lack of talent is a constant. Another constant is a lack of actionable intelligence and knowing how to apply it.”

our products. But this is something that's very real to us, and it's something that our CEO Kevin Mandia has pushed from his first day leading the company: What separates FireEye is that we can build on what we learn in the field – on the cloud specifically. About 15 percent of the breaches we've worked over the last year have had a cloud element.

So how can we take what we're learning and put that into our products? We can help customers with services, but we also want to help with technology-enabled services and products that reflect what we're learning. One way we've been doing that, and the big focus of the company, has been FireEye Helix.

Helix is where we can bring together not only data from FireEye products, but third-party data from across the enterprise, from any vendor, and pull that into one place, make it quickly accessible for incident response, make it easy to pivot and stack and analyze that data for threat hunting. But then we apply the industry's best threat intelligence to that data as well.

I talked earlier about organizations that are challenged to make intel actionable. Well, we want to do that out of the box. We don't think organizations should have to spend a lot of resources and time and money to make that intel actionable.

With FireEye Helix, organizations get eyesight threat intelligence, the entire corpus of that FireEye intel, applied to their data as it comes in. Sometimes that's through atomic indicators where we'll match on a domain or an IP address. But more and more frequently now, that's through analytics and through the machine learning modules that we've baked into Helix. Again, born in the field, born in the trenches, the stuff that we see on an engagement, and we can turn that into an analytics module or heuristic module in Helix.

Data is coming in, and we're applying everything we know, the TTPs and our knowledge of how an attacker works. We make it quickly accessible. And then, perhaps most importantly is driving orchestration off of that.

Helix embeds our FireEye security orchestrator, a product based on technology we acquired about three years ago and we've continued to develop. It's really a full-featured, mature suite to

“There’s one thing that FireEye does uniquely well compared to everybody else in the space. And that is, we’re the ones that are responding to those breaches that matter.”

enable orchestration. We support about 160 third-party products. We can manipulate those according to a predetermined playbook that an organization has. We run it all for a company, and that managed infrastructure has been a big boon for organizations that are short on talent.

I was just meeting with some financial institutions this week who are struggling with the fact that they have ... a team of 15 people who were responsible for just maintaining a SIEM infrastructure for writing playbooks. We want to take that burden off of a company. So if I string all that stuff together, you have a place now you can bring any kind of intelligence, make it easily accessible, make it available for response, for hunting. We’re applying everything we know to that data, and that really helps organizations understand “Where do I need to focus? What’s the most important? I might have gotten 40,000 ADS alerts in the last several weeks. I’m overwhelmed.”

We can apply that FireEye intelligence and tell you, “Look, out of those 40,000 alerts, here are the 10 that are state-sponsored actors that you need to start with.” And then like I said, most importantly is using orchestration so you can drive down your costs; you can improve your cycle time; and you can do it with fewer resources.

We’re putting a lot of effort into making sure we can deliver on that promise of that operating system for the security operations center.

breaches that matter. We’re fortunate that when a customer is in a tough spot, we can help them out. We can help them out more quickly because we understand the attacker. We take what we learn and we put that in our products.

So we’re proud of the fact that we can say our FireEye suite of products and services is probably the best-informed, and the most knowledgeable in the industry. We focus on making that real in our products.

When a customer buys FireEye Helix or another one of our FireEye products and services across endpoints or networks or email or a managed defense offering, they’re getting threat-informed, actionable information so they can prioritize better and solve incidents quicker.

What’s different? It’s what we know. It’s expressed through orchestration, our rules and our intelligence. ...

This offering wouldn’t be complete if we couldn’t natively integrate with the sources of cloud telemetry that I was talking about. Our customers can know out of the box, when they get FireEye Helix, they can integrate with those, whether it’s Google’s platform or Azure or AWS. Within minutes, they can point those sources into Helix and be getting those actionable alerts that they can then use to drive orchestration or response. ■

Standing Out in Crowded Market

FIELD: Grady, we started this conversation talking about the crowded threat landscape. The marketplace is just as crowded. How does FireEye differentiate itself from others in this marketplace?

SUMMERS: I’m glad you asked, because that’s probably the first question a prospective customer asks. They say: “OK, that’s great, Grady. But everybody seems to have an intel feed now. We hear a lot about orchestration. It’s easy to get lost in the sea of buzzwords.”

But I always bring it back to one thing: There’s one thing that FireEye does uniquely well compared to everybody else in the space. And that is, we’re the ones that are responding to those

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

