NETEVENTS

# EUROPEAN MEDIA SPOTLIGHT

# "INNOVATORS IN CLOUD, IOT, AI & SECURITY"

**DRAFT**

## *Track and Attack the Hackers: Don't Be Passive, Fight Back!*

Chair:

**Mike Spanbauer, P of Security, Test & Advisory, NSS Labs**

Panellists:

| | |
|---|---|
| Josh Applebaum | VP of Product Strategy, Ziften |
| Scott Register | VP, Product Management, Ixia |
| Paul Ferron | Director Solutions Sales, CA Technologies |
| Guy Franco | CTO & Co-Founder, Javelin Networks |
| Laurance Dine | Managing Principal for the Verizon Investigative Response Team |

**Manek Dubash**

So let's move onto our next session. I'd like to invite Mike Spanbauer to come down with his panel please, and let's talk about tracking and attacking the hackers. Don't be passive let's fight back.

**Mike Spanbauer**

Thank you, and welcome all. So our topic is a bit unique given that there's no one way, I think, to ultimately secure the enterprise, the world in which we live. But there's certainly some new approaches and considerations as we've grown more aware and progressed along these timelines.

So very quickly I want to introduce the panel today, certainly I'm very pleased to have such capable experts and veteran insights to share here with you. So I'd certainly encourage you guys to reach out after this session too since we are going to race through this in about 30 minutes, so I doubt very seriously we'll be able to get through all the questions that may come to mind as we walk through. Briefly if you guys want to just quickly take a second your name and company.

**Josh Appelbaum**

Josh Appelbaum, with Ziften. Vice President, Product Strategy.

**Scott Register**

I'm Scott Register, Vice President, of Security and Cloud Products Ixia.

**Paul Ferron**

Paul Ferron, with CA Technologies, the Director for Strategy on Digital Identity

**Guy Franco**

Guy Franco, CTO of Javelin Networks.

**Laurance Dine**

Good morning, I'm Laurance Dine from Verizon. I'm the Incident Response Manager for the EMEA region

**Mike Spanbauer**

Thank you, guys. And for others, who aren't familiar with myself or NSS Labs, we test products, but from that we glean insights and know what works, what does not work. I have the luxury of travelling around the world and talking with [Scissors], security teams, organisations, boards, et cetera, to find out what the next steps are. So, ultimately, if I secure then hopefully my kids will be in a better place, but it's going to be a long time, I think, before we get there as an industry.

Something that in fact the previous panel mentioned a few times, and it's, I think, where we've come from is this position of reactive security. Oftentimes you wait for something to happen and then process, interpret and determine what the right response or next steps are. It's easier. It is a simple approach. Oftentimes you can invest accordingly.

It's more cost effective in respect to up front investments, as well as it's easier to staff, because you just simply handle things as they come in. But at the root of this, does it work? Doesn't it work? No. It absolutely does not work. And in many cases, especially as the awareness has grown, is the cost of breach and what it takes to do incident response well.

Frankly, it's increasingly common to find folks now trying to break the paradigm and shift their organisations. It's easier for me to say this, though, than for organisations to achieve this. Moving from that position of comfort and history is not a simple one.

And just briefly, the concept of proactive security investments and handling these challenges, you can't protect everything. So one of the key things is to understand where those critical assets - or the purpose that you have as an organisation, regardless of whether your public sector, private sector, you need to know which assets you're going to invest in and protect, as well as where they are. So who are your users? Where are they located? When are they to access this material, these resources?

Processing through that, understanding how you need to, as an organisation, invest for that success. So, right intelligence is at a macro level, a context applied information construct. Meaning that it's not intelligence until you have context to apply that information to your organisation.

So I take a bit of an affront with the concept of TI. Because marketing has implied that it's more than it can be, but when applied well, it is truly a valuable resource and capability.

With that, I mean, we're going to talk about here, and I think get some insights on is how to evolve your posture and the topic specifically about tracking. Who, what the bad guys are doing, how they're both infecting your organisation, as well as what they're after. At the root of this is, I think, understanding their motives helps you to protect the organisation more effectively and really to change the paradigm from one of reaction to proactive investments.

It's the only way that we regain security sanity, and frankly, build more security - secure solutions from the beginning, right. Bolt on versus built in. Developers will code exactly what they're asked to. I don't think that there's a directive that says, you will incorporate vulnerabilities into your software, when you're writing this, right? And so the reality is that cost and time are the two priorities for most software organisations.

And if security and super code is on the list, it's third or fourth, and when you get crunch time, when you get to the point of getting that code over to QA and getting it out the door to hit your tape schedule, I'm sorry, but security often falls off the list. So it's not that they're wilfully writing malicious code or vulnerable code. It's simply that we have, and as a society, held them accountable and priced accordingly. So we haven’t stopped buying products because it's insecure. We continue to pursue it. So just a bit of a perspective.

So, what I want I think, first pose to the panel, is the question of, with this change, the shift in industry from reaction to this proactive stance, what are the benefits that you've seen and/or believe are immediately there? Because this is how we get ROI. This is how we justify investments in the process chain, and so forth. So let's just start there and being able to be aware of what's going on by the bad guys in the environment. Where do we go from here, from a benefits perspective first? So what are the possibilities?

**Josh Appelbaum**

We see that a lot folks are really keeping their operations teams, their securities teams separate and security teams are looking for these exposures, these vulnerabilities and are looking at the operations teams to address these, but unfortunately, they're usually very separate organisations, and are using separate products.

So we believe that taking these two organisations and bringing them closer together so that they can work over a single platform, take what the security team might find to be the exposures within the organisation and very quickly be able to address them is extremely important.

**Scott Register**

One of the things that came out several times in the previous discussion was the idea of ROI. That you have a certain amount of resources that you can spend and you want to figure out how to invest those the best, and if you look at escalating levels of active defence, or whatever, you can think of it as annoyance, attribution and attack. I don't think any of us are talking about attack. I mean, that's a very state level thing.

But you get the most ROI out of just the annoyance piece. Slow people down. You don't want to be the low-hanging fruit. You want to - you don't want to be the one that's easy to compromise. And the previous speaker had it right - the basic security hygiene, you get a lot of ROI after that.

And then there are some additional levels of things, like tar pits and things that will slow people down, make them think they've found something, and they realise later they've wasted six months and they haven't gotten anything out of your network. Things like that are really good ROI as well.

**Paul Ferron**

Yes, I think the best we can do is to look at what we're doing from a security perspective slightly differently, if we look at the user journey and what the user is trying to accomplish, and start to evaluate how that works and how these systems need to operate together, we can build in security much more easily.

And it goes a little bit towards what you were saying around the cost and time. Those are the crunch number for development, right. We need to be more agile, we need to deliver more apps to the market space. And cost and time are the two factors they're looking at.

So actually, if you look at - if you do your defaults better, you free up resources. You free up time for your developers to actually start thinking about security and doing things differently.

So those are the things that we need to look at. It's a holistic problem and you need to approach it holistically.

**Guy Franco**

I think we should all change the mind-set which we're currently thinking of. We should change the mind-set of how to prevent a breach to the mind-set that, okay, I'm already breached. I'm already breached,

And he should also embrace the way attackers thinks. Basically, they should look for a common ground on all attacks or [APT] that happens in their industry, and look how attackers operated and see if they can actually find indicators that attackers have done already stuff like that in other places, are doing it in their places. What we call now in the industry, purple team.

Purple team is basically a personnel that also know very good offensive techniques and also defensive technique. If you combine those two together, I think you get the perfect person to do this kind of operation that basically search for the attackers inside the network.

**Laurance Dine**

I'm just going to follow up on exactly on the same kind of line as what Guy's going on. And if you take the thought process that you

If you imagine how stressful the situation is, if you just identified that you've been breached - having something written down, with step-by-step guides on what you're going to do when that happens, and actually practising that and doing it regularly, so that everybody who's going to be involved in a breach response knows what their jobs are, then that is the best thing that you can do.

**Mike Spanbauer**

Yes, and I think, regarding those, the low bar right, oftentimes in orgs the quick hits around doing some of the, quote, unquote, best practices more effectively, right, so work isolation, password hygiene, simple rules - how often does the system require you to change that password? Oftentimes 365 is a little too long, right. A password in place for a year - I'm sorry, but compromised credentials are almost a certainty.

**Paul Ferron**

Yes, but password is a good example, right? We're still using passwords and we all know they're ineffective.

**Mike Spanbauer**

Indeed.

**Paul Ferron**

They have a role to play, but they need to be combined with other measures as well. We need to get to a more granular state of how we approach these things.

**Mike Spanbauer**

Actually, that's an excellent segue. The question is, so where to start? What are some of the simple opportunities to both, (a) validate that you're doing a best practice well? I mean, there's simple scanning and so forth, but to that point, there are some innovations and advances that I think help us - perhaps not even deal with the password issues, but rather just change the paradigm and the approach to potentially look at it differently. So anything else we can…

**Paul Ferron**

No, I agree. I think that that is one of the areas that there's still a lot of ground that can be gained. I mean, if we look at the capabilities we have. We all have the phones. We all have these things. They are integrally linked to my identity. So having the fact that I have my phone is an additional step in my authentication process.

So I'm not saying we should do away with passwords, because that's just not reality. But today it's either a password or it is a very complex token based thing that makes my life horrible. So I think there's a middle ground there, where we can get to. The technologies are there. We're just not leveraging it.

**Mike Spanbauer**

Okay. Josh, anything to add?

**Josh Appelbaum**

Yes. I think one of the things that really needs to be addressed is the critical assets in the organisation and making sure that those assets are really being protected and are being monitored in a different way than the average asset in the organisation.

And another level on top of that is knowing what is out there and knowing what your assets even are. A lot of organisations don't have a full inventory of what's out there and a lot of times you'll find old systems. They may have been virtual systems that were spun up by an IT administrator, that are out there and are not being patched or not vulnerable because they're not being managed.

So you really have to have visibility into everything out there, so that you can make sure that the basic level of security, patching, is really being taken care of. And then when you do know what those critical assets are, that you're really focusing on those and protecting those in a slightly different way than you would with other assets, the average asset in the organisation.

**Scott Register**

Right, yes. I was just going to add that's - that idea of tagging your important assets is obviously a good one. You think about your hotel room, right. You've got a lock on the

door but the important stuff you put in the safe. There's an elevated level of security where you keep your passport or whatever it is you keep there.

But one of the challenges, and I don't think anyone really has an answer to this yet, although a lot of people are working on it, is when that asset is on the inside of your network, and maybe it's an old server, whatever, yet that requires maintenance, it requires - but we know how to do that.

The - one of the big challenges that I think no one has really solved yet, although there's a lot of work, is when that moves out of your control and it moves to the cloud, which we haven't really talked about, that's a whole new ballgame. Because you - all of those things - securing the infrastructure and access controls and - that goes away, right, and that's an area where we'll have to evolve very rapidly, is applying the same level of security and hygiene and everything else, to cloud-deployed assets, because the techniques and approaches will be very, very different.

**Josh Appelbaum**

Going along those same lines, I think IOT is another interesting aspect, where it's an asset that you're not going to be managing. It's an asset that you're going to have your connected TVs and so forth, but these are things that are still vulnerable, that can still be attacked and if an attacker gets in there and accesses that, can spread laterally.

So it's the next frontier beyond cloud that we'll be talking about in a few years probably.

**Scott Register**

Yes, when the CEO of Samsung tells you not to have sensitive conversations near your television, that's not really comforting.

**Guy Franco**

I mean, it's already public that you can get the CIA tools so out there.

**Scott Register**

Right.

**Mike Spanbauer**

Indeed. So it's challenging, but orgs are, I think, finding themselves oftentimes plagued by resource constraints, chasing fires and so forth. How do you move to this position? As well as how do you capitalise on the potential wealth of vertical information, industry content, knowing what's occurring within your sector, for a targeted, potentially, attack, or frankly, just more broadly, as we saw with some of the ones recently, that for Internet-facing systems, and again, best practices.

I know that these reports that are supposed to be disabled, however, oftentimes we find systems that are just sitting to there. Moving organisations to wards that, I mean, relative to the wealth of threat intelligence or information, what advice might you offer

to enterprises to be able to capitalise and to recognise what the motives and the direction for these folks are?

I mean, Guy, I think you've quite a bit of experience in this. If you want to kick us off, and then head on round?

**Guy Franco**

Yes, sure. I would recommend every company basically look for the common ground for every attack. You can start from there. Basically you can see the most attackers, most CPTs, most campaigns are going, either after your credentials or your active directory. So looking for this kind of stuff is extremely important.

So any sort of persistency created either in the active directory, usually this stuff are pretty easy to find out. Monitoring specific security groups, like the groups of the admins, to see if another user was added. Those are basic stuff that everyone can do. Auditing and it can - I can stop by using these methodologies, at least 70%, 80% of the attack methodologies inside the network.

**Laurance Dine**

I could talk on this subject for the rest of the day, probably, but I can give you a couple quick hits. So, for actionable, real intelligence, the only way to have that is for people to share information between them. And one of the things that we encourage our clients to do is to - if you're in the same industry, speak to your - speak to the CSOs of the other organisations. Have that real stuff. I mean, there's so many different threat intel lists out there. If you tried to review them all, you'd never be able to do it.

The other thing that I would do, would say on this subject, is you have to have your own internal information tracked. So the things that are going on within your environment, you have to have that available so that you can see what the difference is from Monday to Tuesday and try to identify very, very small instances where something's slightly different. And then you have to track that down.

And if you don't have that information, from six months ago, there's no way for you to look. And that's how these guys that are in the state-sponsored - these really top level cyber guys that attack organisations for long periods of time, that's what they do. They don't go in on a Monday and they're taking your stuff on a Wednesday. They go in on a Monday and they're taking it six months later. They're very low, they're very slow, and you have to have all that tracked, actionable information to go back to.

**Mike Spanbauer**

No, that's a very good point.

**Josh Appelbaum**

Yes, I think a lot of security organisations really need to focus on knowing what their organisation should and shouldn't be doing, what's normal and what's not. But when it comes to response, I think there's only a certain level that the organisation - depending on what that organisation is.

Obviously certain organisations are going to have more critical assets or are going to have intellectual property that needs to be protected and needs to be done in house. But for a lot of organisations, when it comes to response, I do believe that it needs to be outsourced to the experts, like Verizon, over here, who really need to take the scalability that they have, as well as the information that they've gained, from working with many customers and many different industries, to do the right form of response.

Because we can only do so much internally, in our own organisations and be experts at what we know about our organisation. Share that with our outsourced response teams, to make sure that we're doing proper response and protecting our critical assets.

**Laurance Dine**

I was just going to add, it's very easy, sometimes, to see some headline or read, oh. there's Ransomware, Wannacry, whatever, there's some headline, and there's this urge sometimes, as the security guy, to chase that. Oh, I want to stop that. I want to make sure I'm safe from the latest, greatest attack. And your CSO or whatever may ask you about that.

It may not really be relevant to your organisation. So rather than having that threat-based model, it really makes more sense to identify your assets - like what are the things that I have? Make sure that your security investment profile fits that - that you're investing to protect the important things.

So you're not - it's not threat-based. It's more asset-based. And that's where you invest. And absolutely this - the decision of, what am I going to do internally and what am I going to do externally? That's an important one to make early on. Because for most people, you're not going to invest in a heavy-duty security response team. It's just cheaper to outsource, absolutely.

**Paul Ferron**

Yes, no, I agree, and I think it's also a two-way street. It's a shared responsibility. On the one hand, the vendors have a responsibility. For example, you may not know that CA Technologies protects a lot of the card now present in credit card fraud. Those systems are in place with banks. We manage that for banks. We track the fraud. We look at the fraud.

But strangely enough, until very recently, we didn't share the information from one bank to another bank. Which is weird. Because if one attacker is attacking one bank, he's probably also attacking cards from another bank. So that kind of stuff is where vendors need to take the responsibility, and we're doing

But it's also the other way around. The enterprises also need to come back to the vendors and tell them what they're trying to accomplish. Tell them what their goals are and how to build security. There's a tremendous amount of knowledge there.

But today we still see a lot of RFBs, which are very specific to - we want to buy this microphone, and it needs to be this one. That just doesn't give us room to think with you on what could be a better approach to dealing with the issue.

**Mike Spanbauer**

Right. I think one thing I want to add and that was hinted at already in the firmer panel, this reluctance to share materials. I mean, with government, but frankly, even within industry. I know oftentimes I'd wager that the banks contracts were those that dictated the inability to share, not CA owning that portion. So I'm certain it was from the client side that mandated it.

But relative to what the actors have done these days, they have built robust databases and assembled this personal information that has been acquired from dozens of breaches over the last six to eight years. They have better profiles than most of your governments do on how to answer your secret questions and how to solve for your password.

So back to single-factor, and password concepts. It's merely a piece of mind that you think it's secure, because I'm sorry that in cases where folks are still using secret answer responses, which is largely a lot of industry, it's not.

Especially if you've had any social influence or posted anything to - oh yes, that blue site that has quite a bit of material as well, linked and that bridge. They have an immense amount of information. Kids' graduation years, classes, where you lived as a kid, zip codes. And they don't let the data just expire. They've built this and have an incredibly robust history. So the reality is the criminals are tracking us incredibly well.

**Scott Register**

And there's things that go round on Facebook, whatever, which Beatle are you? Which whatever - don't answer those. Let's just please don't. I mean, that has…

**Mike Spanbauer**

That's good advice.

**Scott Register**

That is the best harvesting. If you think about the answers to those and then you go to your bank or whatever and there's a list of 10 questions, it's a pretty good mapping. What was your first concert? What street did you grow up on? That - just please don't answer those.

**Mike Spanbauer**

We've got a few minutes for questions. We've got a microphone here. We'd love to hear from the room. There's no way we can cover all topic.

## *Audience Q&A*

**Unidentified Male**

How is GDPR going to affect your ability to map and track, especially considering where you guys are based?

**Mike Spanbauer**

Oh, GDPR. Obviously, the new act here, in the EU and governance. So anyone on the panel want to take the first crack at the impact?

**Paul Ferron**

Well, I mean, GDPR is very interesting from my point of view. I think it's a tremendous opportunity, actually, because it provides some of the attention and coverage that is overdue. There's a lot of stuff we should be doing already that we're not doing, for whatever reason - time and cost are the most obvious ones. I think GDPR provides an opportunity to do this well.

But it is difficult to see how it will play out from that perspective and what we can share, what we can't share. In the end, it comes down to if it's not tracked back to a particular person then that's okay, but what does that mean is still something that needs to be quantified.

**Laurance Dine**

Yes, that's fair. I don't know if we know exactly what technologies will be employed to provide for the governance controls that are required to achieve the mandate. So we'll see.

**Scott Register**

I think one thing I'd just add quickly, Laurance earlier mentioned having the baseline and so you know if things are different now than yesterday. Anything that forces people to maintain an audit trail is good. Independent of what technologies are deployed or how it impacts us directly. Anything that forces that is a good thing.

**Mike Spanbauer**

Okay. Another question.

**Unidentified Female**

I would like to ask you how to know that a behaviour is abnormal when you say that very often that abnormal stay for a long time inside an enterprise, so it becomes the normal situation at the end. So how to know that the abnormal is - the normal situation is the abnormal situation that you have for years, because you have been attacked years before and someone did put a lot of things inside and just listen to what happen inside your network. How to know that?

**Laurance Dine**

That's the golden question. If we knew the answer to that, we'd all be - you wouldn't need us up here, really. The reality is you have to pay attention. And that is what it is.

If you - when we respond to these types of incidents, and we're looking through information, it is literally, trying to pull together that little line from all the different sources that you have. And if you don't have all the sources, you may miss the one thing that was actually going to trigger it off.

Now, the way that comes back to you is, bad guys have to use tools. And if you know what the tools are, you know what to look for. So there are certain things that give indications to us that there may be bad people in there. And that can give you clues and then you have to follow all the data back. This is why it's an industry, because it takes time to actually do the investigation into what's actually happened.

So there is no one, single answer to that question.

**Guy Franco**

Sure, yes. Just to add to what Laurance just said, we can't just rely on user behaviour to find those attackers. It takes a lot of means and of course audit trails helps a lot. Once you detected where the malicious action started, to see what else got compromised.

But user behaviour won't solve this problem. It's a bunch of technologies that actually solve it, either on the end point, on the network level, watching about communication going outside. So if you combine all this stuff, you might have better chance to find. Not just rely on user behaviour.

**Paul Ferron**

Yes, and maybe start talking to the marketing companies, because they have it down. They know me really, really well.

**Mike Spanbauer**

Tracking, yes.

**Josh Appelbaum**

I think it's two things - tools and workflow. So tools having the ability to detect anomalies, but an anomaly does not mean that it's a malicious behaviour. So that gets into the workflow aspect of it. And really, the second piece, you have technologies, but then you have human knowledge.

So you're going to have to have the human review of anomalies to really understand, this may have been anomalous, but that wasn't malicious. So it's blending of technology and humans and taking the technology and moving that into work flow.

**Mike Spanbauer**

We need to get the machines, big response, but we're not there yet.

**Unidentified Female**

Okay, I am [unclear]?

**Mike Spanbauer**

Maybe.

**Josh Appelbaum**

This whole panel, I think, on machine running and AI, later, maybe we can go into more depth.

**Mike Spanbauer**

Indeed. So as you can tell, we're all quite passionate about the topic, there's no perfect - we'll get better with every day. I think we're improving and learning. But it's very hard.

So I want to thank my panel for definitely contributing today and chiming in, and the audience for participating. So thank you, all.

**Scott Register**

Thank you.

[end]