Meeting Transcript

Meeting: CloudShield Inc - Security Platform Demo

Date: December 16, 2024 | 10:00 AM PST

Platform: Google Meet

Participants:

- Rachel Martinez (Account Executive) - rachel.martinez@ourcompany.com
- David Kim (Solutions Engineer) - david.kim@ourcompany.com
- Jennifer Walsh (VP of Engineering) - j.walsh@cloudshield.com
- Marcus Thompson (Security Architect) - m.thompson@cloudshield.com
- Lisa Chen (CTO) - l.chen@cloudshield.com

Transcript

00:00:12 **Rachel Martinez**

Good morning everyone! Thanks for joining today's demo. I'm Rachel, your Account Executive, and I have David here who's our Solutions Engineer. We're really excited to show you how our platform can help CloudShield with your security monitoring needs.

00:00:34 **Jennifer Walsh**

Thanks Rachel. We've got our CTO Lisa and our Security Architect Marcus here as well. We've been evaluating several solutions and yours came highly recommended by our network.

00:00:52 **Lisa Chen**

Yes, I actually heard about you from the CISO at Meridian Financial. She mentioned you helped them reduce their incident response time by over 60%. That's exactly what we're looking for.

00:01:15 **David Kim**

That's great to hear! The Meridian implementation was actually one of our more complex deployments. Before we dive in, can you tell me a bit about your current security stack and what specific challenges you're facing?

00:01:38 **Marcus Thompson**

Sure. We're running a hybrid environment - about 60% cloud on AWS and Azure, and 40% still on-prem in our data centers. Our biggest pain point is visibility. We have Splunk for log aggregation, but correlating events across environments takes forever. Our mean time to detect is around 4 hours, which is way too long.

00:02:15 **Jennifer Walsh**

And from an engineering perspective, we're spending too much time on manual triage. My team is drowning in alerts - probably 500+ per day - and most of them are false positives. We need something that can actually prioritize real threats.

00:02:42 **David Kim**

Those are exactly the problems we were built to solve. Let me share my screen and show you the platform. What you're seeing now is our unified dashboard. Notice how we're ingesting data from AWS CloudTrail, Azure Activity Logs, and on-prem sources all in one view.

00:03:08 **Lisa Chen**

That's a clean interface. How does the data ingestion work? We have strict data residency requirements - everything needs to stay within the US.

00:03:25 **David Kim**

Great question. We offer fully isolated deployments in US-East and US-West regions. Your data never leaves those boundaries. We're also SOC 2 Type II and FedRAMP Moderate certified, which I know is important for your government contracts.

00:03:52 **Marcus Thompson**

What about the ML component? How does your threat detection actually work under the hood? I've been burned by 'AI-powered' solutions that were basically just rule engines with fancy marketing.

00:04:18 **David Kim**

Ha! I appreciate the skepticism. Our detection engine uses a combination approach. We have about 2,000 pre-built detection rules based on MITRE ATT&CK framework, but the ML layer sits on top to learn your environment's baseline behavior. Let me show you a real example...

00:04:48 **David Kim**

See this alert here? It detected an unusual API call pattern from a service account at 3 AM. Traditional rules would have missed this because each individual action was legitimate. But our behavioral model flagged it because this account normally only operates during business hours and never accesses S3 buckets.

00:05:22 **Jennifer Walsh**

That's impressive. How long does it take for the system to learn a new environment? We can't afford weeks of tuning.

00:05:38 **David Kim**

Typically 48 to 72 hours for the baseline. But you start getting value immediately from the rule-based detection. The ML models improve continuously - we see accuracy increase by about 15% per month for the first quarter.

00:06:02 **Lisa Chen**

Let's talk about integration. We have a homegrown ticketing system and we use PagerDuty for on-call. Can you push alerts and create tickets automatically?

00:06:22 **David Kim**

Absolutely. We have native integrations with PagerDuty, ServiceNow, Jira, and Slack. For your custom ticketing system, we offer a robust REST API and webhook support. Actually, let me show you our automation builder...

00:06:48 **David Kim**

This is our playbook editor. You can create automated response workflows without writing code. For example, this playbook automatically isolates a compromised EC2 instance, captures a memory dump for forensics, and creates a ticket - all within seconds of detection.

00:07:18 **Marcus Thompson**

Now that's what I'm talking about. Currently that process takes us 45 minutes minimum. Can you automatically block IPs at the firewall level too?

00:07:35 **David Kim**

Yes, we integrate with Palo Alto, Fortinet, and AWS Security Groups for automated blocking. We also have a human-in-the-loop option if you want approval before taking action on high-severity incidents.

00:08:02 **Rachel Martinez**

I want to jump in here because I know budget is always a consideration. Jennifer, you mentioned your team spends a lot of time on manual triage. Can you estimate how many hours per week?

00:08:22 **Jennifer Walsh**

Easily 60 to 80 hours across the team. We have 4 security analysts and they're basically doing nothing but alert triage right now. It's not sustainable and it's burning them out.

00:08:45 **Rachel Martinez**

Based on that, customers in similar situations typically see 70 to 80% reduction in manual triage time. That's essentially giving you back 2 to 3 FTEs worth of capacity. The platform would pay for itself in the first quarter.

00:09:12 **Lisa Chen**

What does pricing look like? We're processing about 50 TB of security data per month.

00:09:25 **Rachel Martinez**

For your volume and requirements, you'd be looking at our Enterprise tier. I can put together a detailed proposal, but ballpark we're talking $180K annually. That includes unlimited users, 24/7 support, and quarterly business reviews.

00:09:52 **Lisa Chen**

That's actually more reasonable than I expected. Some of the other vendors we talked to were quoting north of $400K.

00:10:08 **Marcus Thompson**

David, I have a technical question. What happens if your cloud service goes down? Do we lose visibility?

00:10:22 **David Kim**

Good disaster recovery question. We have local collectors that buffer data for up to 72 hours if connectivity is lost. When connection resumes, everything syncs automatically. We also guarantee 99.99% uptime in our SLA, and in five years we've never had a full outage.

00:10:55 **Jennifer Walsh**

One more thing - we're planning to adopt Kubernetes heavily next year. Do you support container security?

00:11:12 **David Kim**

Yes! We just released our container security module last quarter. It provides runtime protection for Kubernetes, image scanning, and we detect misconfigurations like overly permissive pod security policies. Want me to do a quick demo?

00:11:38 **Lisa Chen**

Actually, I think we've seen enough for today. I'm impressed. What are the next steps?

00:11:52 **Rachel Martinez**

Great question! I'd suggest a proof of concept. We can deploy in your environment for 2 weeks at no cost. That way your team can validate the detection quality and integration capabilities. How does that sound?

00:12:15 **Lisa Chen**

That works for us. Let's set it up. Jennifer, can you work with David on the technical requirements?

00:12:28 **Jennifer Walsh**

Absolutely. David, I'll send over our architecture documentation after this call. Fair warning - it's about 50 pages.

00:12:42 **David Kim**

Ha! No problem, I've seen worse. I'll review it and come back with a deployment plan within 48 hours. We can target starting the POC next Monday if that works.

00:12:58 **Marcus Thompson**

Quick question before we wrap - do you offer any threat intelligence feeds? We're currently paying separately for that.

00:13:15 **David Kim**

Yes, threat intel is included in Enterprise tier. We aggregate from 40+ sources including VirusTotal, AlienVault, and our own research team. We also have a feature where customers can share anonymized threat data - kind of a community defense network.

00:13:42 **Marcus Thompson**

That's a nice bonus. The threat intel alone costs us about $30K a year right now.

00:13:55 **Rachel Martinez**

Perfect. So to summarize - I'll send over the proposal and POC agreement today. David will review the architecture docs and provide a deployment plan. And we're targeting next Monday for POC kickoff. Anything else?

00:14:18 **Lisa Chen**

No, I think we're good. Thanks for your time today. This was one of the better demos I've seen - you actually showed us real capabilities instead of just slides.

00:14:35 **David Kim**

That's the goal! Looking forward to working with you. Feel free to reach out directly if any technical questions come up.

00:14:48 **Jennifer Walsh**

Will do. Thanks everyone!

00:14:55 **Rachel Martinez**

Thank you! Talk soon.

End of transcript - Generated by Google Meet