A Day in the Life of a Seasoned Security Analyst: Transforming Cybersecurity with 360Sequrity Solutions

By Shantanu Bhattacharya

Founder, CEO & CTO

A Day in the Life of a Seasoned Security Analyst: Transforming Cybersecurity with 360Sequrity Solutions

Let me take you on a journey through the eyes of Alex, a seasoned security analyst at **SecureBank**, a global financial institution. Alex's team is responsible for protecting sensitive customer data from increasingly sophisticated cyberattacks. Every day is a battle, but this one is about to be different.

The Old Normal: A Day of Chaos

Before implementing 360Sequrity solution, Alex's days were a blur of stress and frustration:

- **8:00 AM**: Alex logs in to a flood of alerts—thousands of them, most irrelevant. Sifting through the noise feels like finding a needle in a haystack.
- **10:30 AM**: An alert signals a possible privilege escalation. Is it real? Alex spends hours investigating, only to find it was a false positive.
- **1:00 PM**: Lunch is interrupted by another alert. This time, it's a legitimate breach attempt, but the delay in detection means the attacker has already exfiltrated data.
- **7:00 PM**: After a long day, Alex leaves the office, knowing tomorrow will bring more of the same—overwhelming alerts, late detections, and the constant fear of missing a critical attack.

The day ends for Alex without any hope of handling situation better. **Alex is afraid, at this rate, a burnout is not much further from eventuating.**

The Transformation: A New Era Begins

Fast forward to today. **SecureBank** has implemented 360Sequrity's advanced cybersecurity solutions, and Alex's day looks entirely different.

8:00 AM: Starting with Clarity

Alex logs in to a streamlined dashboard. The flood of irrelevant alerts is gone, replaced by a handful of high-priority incidents.

- **Why?** Advanced 360Sequrity analytics, using signals from the network with certainty, without probabilistic AI techniques, have filtered out the noise, presenting only actionable threats.
- **Impact:** Alex feels focused and confident, knowing the system has their back.
- **The 360Sequrity Difference:** Most existing solutions use AI as it can process high number of signals in a jiffy. However, the problem is, it requires extensive training after installation in the network for it to be relevant and useful. Even thereafter, it is probabilistic at best – with false positives and negatives, with very devastating consequences. 360Sequrity, on the other hand, identifies the important and relevant signals to monitor and does that with certainty, eliminating probabilistic approach.

10:00 AM: Early Detection in Action

An alert comes in: a new admin account is attempting to access sensitive data from an unauthorized device.

- **What happened?** The system's behavioural analytics flagged the unusual activity just three days into the attacker's campaign—191 days faster than the industry average.
- **Alex's Response:** With detailed insights provided by the system, Alex quickly isolates the account and blocks the device.
- **The 360Sequrity Difference:** Current solutions largely rely on using IP and MAC addresses for identifying and authenticating devices – a well-known failed method as IP and MAC addresses can be easily spoofed. 360Sequrity generates and assigns unique identity to devices and other entities resulting in much accurate identification of the device. So, the device authentication is more meaningful and certain, resulting in more accurate and actionable signal.

1:00 PM: Blocking Sophisticated Attacks

During a routine check, Alex notices an attempted lateral movement by the attacker.

- **How?** The solution's multi-layer authentication denied access because the software instance didn't match the authorized configuration.
- **Impact:** The attacker is thwarted at every turn, unable to access critical data even with admin privileges.
- **The 360Sequrity Difference:** When a data is accessed using a software instance not authorized by the network administrator, 360Sequrity can detect and block it. Most solutions do not have this factor when authenticating data access. The software access control is limited to the user authentication provided by the author of the software, and has nothing to do with authorization by the network administrator. 360Sequrity verifies authentication result from user account, device used and the software used. Even attempt to access data using privileged account is declined as the other multi-layered authentications fail.

3:00 PM: Identity Protection at Work

The system detects that the attacker is using a hacked identity to try and escalate privileges.

- **What happens next?** The solution flags the identity as compromised and instantly replaces it with a new, secure one.
- **Impact:** The attacker is effectively locked out, with no way to leverage the stolen credentials.
- **The 360Sequrity Difference:** Due to the multi-factor and multi-layered authentication supported by 360Sequrity, as described earlier, use of hacked user credentials by hackers can be easily detected. This is unheard of in current solutions in the market.

4:00 PM: Decentralized Identity Saves the Day

Alex reviews the system logs and notices an attempted breach of the backend server.

- **Why didn't it succeed?** Even if the attacker had accessed the server, the decentralized identity storage meant they couldn't reconstruct the full identities.
- **Impact:** Sensitive data remains safe, and Alex feels a sense of victory.

- **The 360Sequrity Difference:** 360Sequrity uses sophisticated algorithm to bifurcate a generated identity. One part is stored in the backend server and the other part is stored with the identity owner. So, even if the attacker is successful in breaking all the security controls put on the 360Sequrity backend server, they still do not have access to the identities and hence the organization does not lose much.

6:00 PM: Wrapping Up with Confidence

As Alex prepares to leave for the day, they reflect on how different their job has become:

- No more irrelevant alerts.
- Breaches detected and blocked before they escalate.
- Recovery costs slashed by 50%.
- A team that feels empowered rather than overwhelmed.

The Bigger Picture: A Solution That Works for Everyone

Alex's experience is just one example of how our solution transforms cybersecurity operations:

1. **Rapid Detection**: Breaches are identified within days, not months.
2. **High Blocking Rate**: 96% of attacks are stopped in their tracks.
3. **Resilience**: Decentralized identity storage ensures that even sophisticated attackers can't make headway.
4. **Analyst Well-Being**: Reduced noise means a happier, more effective team.

The Takeaway

Our solution doesn't just protect data; it protects people—analysts like Alex who are on the front lines of cybersecurity. It makes their jobs easier, their work more meaningful, and their organizations more secure.

This isn't just a story about technology; it's a story about empowerment, efficiency, and peace of mind.

Thank you.