SIEMPLIFY
THREATNEXUS™

ThreatNexus for the Financial Services Industry

Global Bank Relies on ThreatNexus as the backbone of its Security Operations

For obvious reasons financial institutions are natural targets for attacks, often bearing the brunt of hackers focus. According to the Global Economic Crime Survey conducted by PricewaterhouseCoopers LLP, threats to the industry are rising and 41% of bank leaders are fairly sure they will experience an attack in the next 12 months. Security budgets to battle cyber crime often top a billion dollars annually for large banks. Yet higher budgets haven't necessarily translated to more security.

Everyone in the industry intuitively understands that breaches are unavoidable. While preventing attacks will always be critical, the goal has shifted to locating and terminating breaches as quickly as possible to mitigate damage. Yet with existing tools, it is becoming harder and harder for security teams to successfully prevent and remediate breaches.

For one of our large Global Banking customers, the status quo was unacceptable and turned to Siemplify. "ThreatNexus is the primary tool our analysts rely on to manage the entire threat lifecycle. Our entire SOC team no longer has to navigate multiple tools and systems to investigate and mitigate cyber threats" -- CISO, Global Financial Institution.

Business Challenges

- Pressure to demonstrate ROI from existing SIEM and other security tool investments
- Board level confidence in security footprint
- Visibility to security landscape
- Challenges staffing SOC with sufficient analysts

Technical Challenges

- Drowning in a sea of alerts
- Time to investigate and remediate threats on the rise
- Analysts overwhelmed with growing case loads
- No unifying solution that connects disparate tools and data silos

SIEMPLIFY ROI

- On average a 5 to 1 consolidation of alerts (an effective 80% reduction in alerts to investigate)
- Immediate reduction in time to investigate from hours to minutes
- Tripling of analyst caseload capacity

CUSTOMER ENVIRONMENT

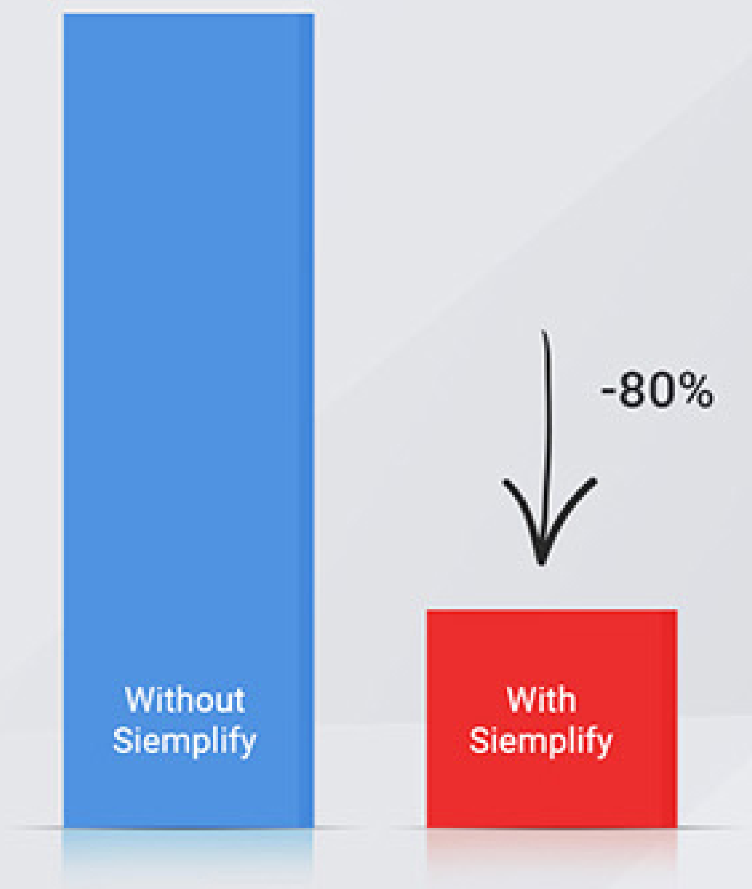
Like any large enterprise, this banking customer faces a broad range of security threats. From a security perspective, they must protect not only their internal operations but perhaps more importantly the thousands of critical customer accounts.

As such, the customer ran a 24 x7 monitored Security Operations Center staffed with multiple shifts. They employed a patchwork of the classic stack of security tools ranging from multiple end-point and network detection systems, ArcSight for log repository, and various Intelligence tools.

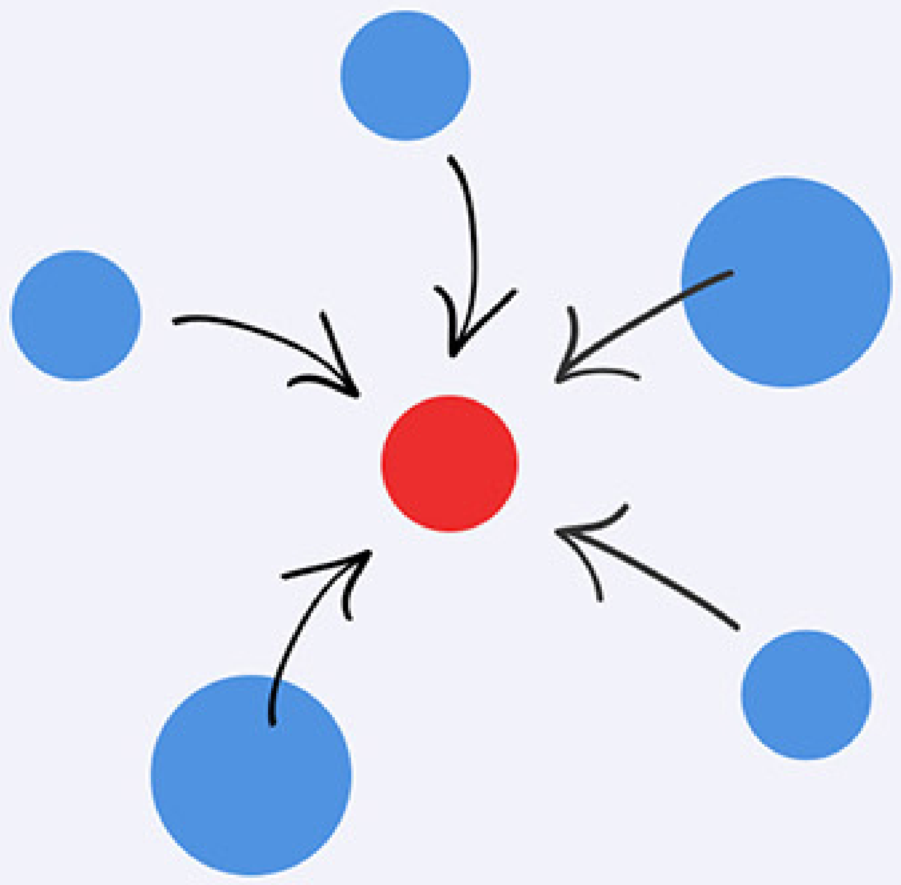
Yet the bank was unhappy with the visibility, investigation capabilities, and growing fear of rising dwell times in their environment and ineffective response. SOC management was under increasing pressure to seek a solution. With few alternatives the bank contemplating building their own next-gen investigation and response tools...until meeting Siemplify.

THREATNEXUS ROI

By leveraging Siemplify ThreatNexus this banking customer realized immediate productivity and security gains.



Case Reduction



5

Avg Aggregated Cases

00:00:02:11

Avg. Sneak Peek Query Time

4.6

Avg. Number of Entities in Case

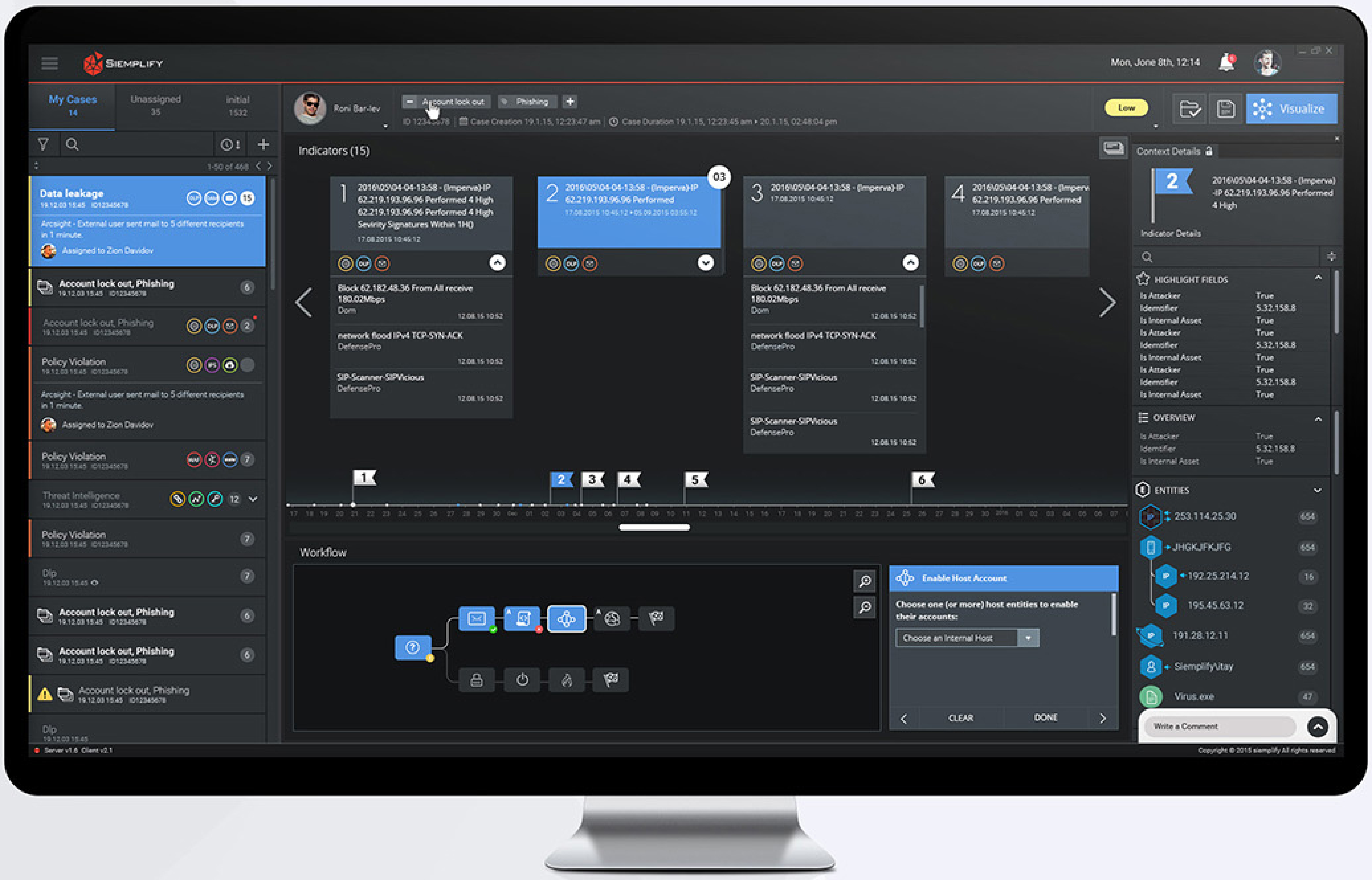
To learn more about Siemplify ThreatNexus and give it a test drive visit www.siemplify.co

SIEMPLIFY, ANSWER FOR THE INTELLIGENT SOC

The extreme proliferation of attacks taking place all the time had shown that breaches are unavoidable; the goal became to locate and terminate attacks in as little time as possible to keep damages to a minimum. Yet the ability to investigate and respond to attacks as fast as possible is hinged upon achieving full visibility across the SOC.

Siemplify ThreatNexus ingests all data from all tools across the SOC, allowing analysts to quickly understand the context behind events in order to build a true end-to-end perspective. The graphical interface grants in-depth insights into events as they take place and helps analysts understand their significance in a fraction of the time. ThreatNexus becomes the hub for all information and allows analysts to collaborate in ways previously impossible.

By bringing data from patchworked sources together, all intelligence becomes actionable. Analysts can proactively search for and organize threats across their environment, which means threats can be triaged and solved faster than ever before.



By grouping truly significant events, alerts, and related threat indicators into cases, Siemplify ThreatNexus eliminated 80 percent of the case-load and provided complete context to analysts yielding enormous benefits.

BOTTOM LINE

Evolving away from the fragmented SOC of yesterday to the actionable, intelligent next-generation SOC that will take your institution into the future requires a holistic solution. Security operations teams can no longer afford the time lost with security data operating in a separate silos, and ThreatNexus enables our customers to easily and proactively unite existing security tools and data to shift from detection to response.

To learn more about Siemplify ThreatNexus and give it a test drive visit www.siemplify.co