REAL-TIME SECURITY ANALYTICS

An Overview White Paper

NEAL HARTSELL

VICE PRESIDENT, MARKETING

JULY 2012

Introduction

The network security market needs a breakthrough – a disruptive, revolutionary approach that changes the game against the bad guys. Our solution specifically addresses the widening security risk gap driven by virtualization, consumerization, cloud computing, social media and enterprise mobility. We call it **Real-time Security Analytics**.

Less and Less Control leads to More and More Hacker Opportunity

Network users demand anytime, anywhere, any-device connectivity – and freedom to comingle personal and professional environments like never before. As a result, network infrastructure and information asset protection faces daunting challenges that are accelerating in a manner that trends towards less and less IT control. At the same time, modern hackers – operating independently or within organized global crime rings; highly motivated, equipped with sophisticated tools, and willing to patiently use protracted entry and exfiltration techniques – are persistently setting traps for employee missteps, checking for doors left ajar, and copying the house keys at an alarming rate. The elephant in the room is not *will* you be hacked, but *how bad* is the hack that already occurred, or is likely in progress.

Traditional Security Necessary, but Insufficient

Traditional security functions – firewall, intrusion prevention, anti-virus/spam/phishing, identity management, security event management, etc. – will remain core to the defense-in-depth approach used by financial institutions, enterprises, government agencies, critical infrastructure utilities, higher education, and healthcare. No one would suggest otherwise. However, it is abundantly clear these products alone are proving ineffective at detecting, understanding, and stopping dangerous multi-stage attacks being executed by modern cyber-criminals in pursuit of financial assets, intellectual property, telemetry control, and/or state secrets.

Simply put, traditional network security suffers from several shortcomings:

- First, in-band rule/signature-based products like anti-virus and intrusion prevention systems can only react to the known bad – and further – only on the direct network connection in which they are inserted. They are surgical and fast – but have no peripheral vision and no long-term, stateful memory of contextual attack activity.
- Second, security information and event managers (SIEMs) – despite broader visibility based upon their consumption of event and log data from multiple network sources – are 1) highly constrained by the amount of data that can be ingested and processed in real-time (or over any lengthy period of time), 2) only able to act only on what is written to a database post mortem and only if that data fits a rigid data structure model, 3) crippled by the inherent performance limitations of relational databases, and 4) painfully slow to build and execute anything beyond the simplest of investigative analytics.
- Third, policy-based devices like firewalls and identity-based products suffer from bit rot and configuration errors. For example, IT may (erroneously) fat-finger a firewall rule, and no one catches it. Later, this gets misclassified into active

directory, leaving a new vulnerability and ultimately leading to a dangerous breach point.

To the degree that any of the three product classes perform well, it is always in a 'lone wolf' fashion. There is no semblance of coordinated real-time knowledge sharing, decision-making and policy action. This forces security analysts into daily triage, against their better wishes. Protection falls short.

As a result, the risk gap continually widens. And a wider risk gap means your company could make the next security breach headline. Worse, you may have already been victimized and are just unaware.

As if these product shortcomings were not enough, public and private organizations alike will never be able to acquire or afford enough talented security staff. Meanwhile, security personnel are overtaxed with daily operational responsibilities just to keep traditional defense products up and running with the latest software. Further, employees will not be deterred from using the latest mobile device or third party cloud-based application. Budgets cannot cover the increasingly complex 'conga line' of security appliances. And clearly, hackers will not slow down, reduce in number, become less intelligent, or less motivated any time soon.

Fundamentally New Approach Required

A fundamentally new approach is required. We all know it. It is not a new thought. Yet the discussion usually ends quickly because of the 'hangover' of historical technology barriers. Here is a sample of what we hear:

- "No product can ingest, process, and retain useful information at a fast enough rate to give analysts a more comprehensive data set."
- "There are no truly good visibility tools that allow us to crawl big data quickly and effectively."
- "There is no easy way to write analytics beyond the ad hoc world in which we live."
- "Even if we could write the analytics, our event management product can't handle complex correlation algorithms. It would take hours to run – so they are simply impractical."

Therefore, a 'fundamentally new approach' gets dismissed as folly. Security practitioners are clearly in need of something new, not a faster version of a product they already own. It just couldn't be done...until now. This problem set is exactly what Click Security upends.

The Click Solution

The Click Security solution is built upon three key components: 1) a high-performance, memory-based real-time stateful data flow engine; 2) security intelligence encoded into Click Modules; and 3) a world-class security research agency, Click Labs. The engine is instantiated through Data Mining Units (DMUs) and Module Processing Units (MPUs). Click Modules are programming objects that receive data from predecessor modules, process that data against a security analytic, and perform an output action ranging from 'write results to a downstream click module' to 'invoke a specific human or machine action'. Click Labs

monitors the evolving threat landscape for its own module development effort, assists customers in becoming self-sufficient at writing their own modules as desired, and progresses Click's module development infrastructure enabling an increasingly open and independent crowd-sourced intelligence sharing model.

At the highest level, the Click solution performs the following unique functions:

- **Actor-Based Information** – First, sensors take in any type of network telemetry data – logs, events, flows, etc. and pass that data to protocol decoders which decode the protocols and automatically convert today's 'haystack' of arcane event-level data into 'actor-based' information. Our belief is that no analyst should have to spend time preparing data for analysis. Using Click Modules to automatically create actor-based information means every event, every log, every flow is tied to a human or machine identity for you, fundamentally changing the start point of an investigation – and saving vast amounts of time and frankly, frustration.
- **Unknown Threat Precognition** – Second, since the system is able to capture, associate and correlate all network telemetry automatically, we reveal high–anomaly count actors and high-priority anomaly actors *before* you start your investigation – in fact, without you asking the first question. That means we are tying together events of interest on our own – we do not need to wait for the analyst to start with the usual "I wonder if there is any suspicious activity today, and if not readily apparent (meaning a set of screaming alerts), how and where should I start looking?" No detective begins looking for clues to a crime until they have been notified an incident has actually occurred. We turn this around. We see anomalous activity in the haystack, find it, filter it, correlate it and present it to you *before* a network breach has realized its full lifecycle.
- **Automated, Interactive Visualization** – Third, we fully automate the process of interactively visualizing the data in different ways – rows/columns, graphs, parallel coordinates, etc. Click Security's powerful protocol decoder, core, augmentation, analysis, and action Clicks let you rapidly pull any data and programmable action into a Dynamic Workbook – where it can be manipulated with ease. That means all data - ranging from live to months old, if not longer. And perhaps best of all, state information associated with protocols, connections, etc., is fully preserved – enabling you to correlate as many actor and incident parameters as you need – *in real-time*.
- **Automated Module Creation** – Once you've run to ground an unknown threat through the above advanced anomaly detection and investigation capabilities, our solution enables the Dynamic Workbook you created along the way – essentially a new binding of Click Modules – to be captured as a new Click. Your valuable time and energy is no longer left to a folder of screen shots, remnants of scripts, notes and thoughts. The process you used to filter down to records of interest, augment with additional contextual data, and decide what action should be taken upon reoccurrence – all conveniently built by selecting and integrating existing atomic-level modules – can now be packaged and named as a new module, then automatically pushed to persistent run time. Simple and complex Clicks alike can be created – including whatever remediation you choose to invoke, whether it be 'alert me', 'create a case for the help desk', 'collect more history around this actor', or 'impose an automatic IPS or Firewall action against this user, session, IP address, etc.' – and set into action, thus increasingly automating the multiplicity of tasks

faced in the 'daily grind'.

Automated Investigation | Automated Lockdown

These system capabilities drive value in two distinct, but interrelated ways. Security analysts are given powerful 'data to information' conversion, fast and intuitive interactivity, and an ability to easily codify their expertise for continuous leverage going forward. We call this **Automated Investigation**. Automated Investigation is about freeing the analyst to do what they are trained to do with greater speed, prioritization and accuracy – which today is impeded by slow, clumsy, archeological tools.

By extension, this same analytics engine can run a growing set of Click Module analytics on behalf of the security analyst - achieving an increasing level of **Automated Lockdown**. At the outset, "lockdown" is a term that sends shiver up an analysts' spine. Fortunately, we completely understand. But, we also know that manual intervention where unnecessary, and constant reinvention of the 'analytic wheel' through repeat scripting, are productivity killers that you cannot afford. Automated Lockdown is not a loss of control. It is the freedom to delegate a designed action to a system that can do that with speed and accuracy – further freeing the analyst to move on to the next unknown incident.

The ability to comprehensively policy-allow and -disallow virtually all traffic, users, apps, devices, etc. from a central point – and give you investigate and lockdown control over unknown, suspicious, and anomalous activity within your IT environment is the power of the Click solution.

Breakthrough Technology

We haven't met a security department yet that doesn't want a product capable of automating these critical functions. But we regularly encounter security-savvy practitioners who believe this to be a lofty – if not unachievable – objective due to inherent hardware, software and data storage performance limitations:

- They are well aware RDBMS-based products first - collect, second - write to a big disk somewhere, and third - query after the fact. This is too slow.
- They are well aware that these products have only a limited notion of state – which breaks down rapidly if, for example, the server operating system is complex, and that writing a script to capture and correlate state is next to impossible.
- They are well aware that to maintain a persistent window of network activity beyond just a few minutes is unthinkable.

This is why Click Security built a radically different – indeed breakthrough – platform to pull this off. A real-time, stateful data flow engine capable of unprecedented performance and scalability underpins the Click Modules. This engine operates entirely within memory – allowing it to run large numbers of persistent Click modules against massive real-time machine data. It is *game-changing*.

The combination of Click Modules and a ground-breaking engine are fundamental to a Real-time Security Analytics solution. Scope of actor information, the number of analytics that can run concurrently, real-time responsiveness, or analytic accuracy would be unachievable

otherwise. But there is a third key ingredient to our solution – Click Labs. Security analytics is not just a game of big data, mathematical equations and a fast engine. Knowledge and experience with the evolving threat landscape, network and application environment, and limitations of current tools are required to really develop powerful, effective analytics. Some enterprise security teams have this ability, time and budget, but many do not. That is why we have Click Labs. You never have to build the first module on your own, if you so choose. Click Labs is adding new analytics continuously. If you want assistance in matching the power of our solution to your network environment, Click Labs operates in that capacity as well.

Summary

Putting Click modules, the Click engine, and Click Labs by your side lets you scale security intelligence and interactive visibility into unknown threats like never before. Deploying Clicks that can operate in real-time with persistence provides network lockdown the dramatically shrinks the risk gap.

But, seeing is believing. A demonstration will show you why we believe this can change your view of the future of network security.

Click Security
www.clicksecurity.com
sales@clicksecurity.com
+1 512 637 8500