Detecting “the Low and Slow (attack)” with XYGATE SecurityOne™

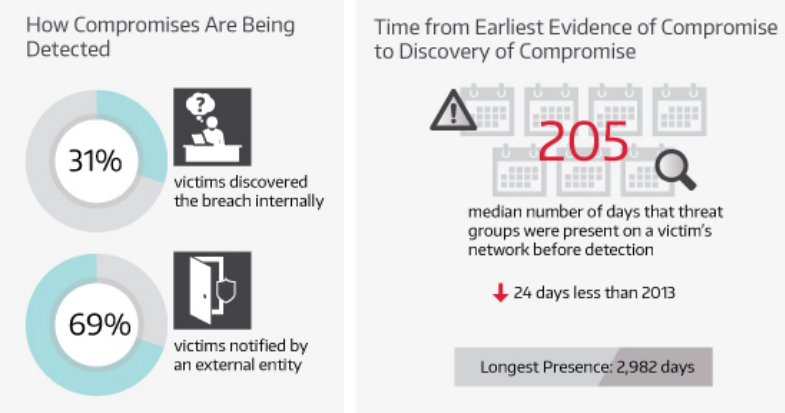
Security has been a lifelong passion of mine. Growing up, I constantly pushed the envelope of what was possible. This was strictly for “research” purposes of course. I would spend a lot of my time after school (and sometimes during school) seeing what systems I could gain access to, discovering obscure security “features”, using social engineering or exploiting just plain security negligence . This was for no other reason than self-satisfaction, to cure a little bit of boredom and, to obtain some online fame. It was fun. I felt cool. I WAS that kid in my parent’s basement, but as I was sitting in my parent’s basement banging away on my keyboard, I was pwning your tech! The dot-com bubble was just forming and n00bz didn’t stand a chance.

I look back at the wealth of experience gained from the need to alleviate boredom in my early life and wonder how trivial it would have been for someone to notice what I was doing and to shut me down, but in the late 90s, security wasn’t just an afterthought – it was virtually non-existent. No one was keeping an eye out whether the system was being used for anything other than for what it was originally intended.

MTTD in Today’s World

Fast forward twenty years and security is at the forefront of everyone’s minds, yet common security oversights of best practices and negligence are still very much part of today’s landscape. The Mean Time To Detection (MTTD) of a security incident is still close to 200 days. That translates to an attacker residing in your systems for nearly six months on average until someone notices, that is – if – someone notices. In my day, the issue was that no-one was tracking my activities – nowadays there is audit data being generated everywhere. The problem has shifted from not enough data to too much data.

Figure 1.[1]



In an era where everyone is used to, and in fact demands, instant gratification, and where we have a one hundred billion dollar plus cyber security industry providing the tools and solutions to satisfy that demand, MTTD is still nearly 6 months! We cannot underestimate the ability of criminals to stay ahead of conventional solutions by constantly adapting – allowing them to hide their malicious intentions or simply fly under the radar. These low and slow attacks have become the Achilles heel of organizations worldwide. The data breaches that will be announced next year are taking place right now, as you're reading this article. The attackers are already in the networks and systems doing their reconnaissance work, exfiltrating data, planning their next move – for months and years at a time, blending into the noise of everyday business users and operations. How can one detect these anomalies?

Data is King

We use data every day to gain insight, plan our next moves and run our organizations. Too little data and you're not getting the complete picture to make an informed decision. Too much data and you're overwhelming your staff and drowning in the noise to make any sense out of it all. Analyzing the vast amounts of data to detect pattern anomalies requires specialized knowledge and takes time. Attackers know this.

Traditional SIEMs and log management devices do what they do well. They aggregate data from multiple sources, report on the verticals you tell them to report on, and allow your auditor to put a tick in the PCI-DSS compliance checkbox for requirement 10.5.3. You would think that should make your CISO sleep better at night, but ticking the compliance box is all that exercise will allow you to do.

We are bombarded by marketing buzz words like "Big Data" and "Data Lakes"; how can we strip away the marketing buzz in order to introduce the concepts into our security strategy and use them to our advantage?

Hello Security Intelligence!

Security Intelligence and Analytics is the concept of collecting, normalizing and correlating the data that you already have access to from myriad systems and solutions that have been deployed in the enterprise. This minimizes the reliance on the human element in what is typically a time consuming exercise for highly skilled data scientists. Applying computer based algorithms and data analytics to the vast amount of data in order to detect valid security events introduces a new dimension to data intelligence that can be used for tracking security incidents **before** they occur, ultimately **reducing the Mean Time to Detection**. Potentially saving organizations millions of dollars and often more importantly – from appearing on the front pages.

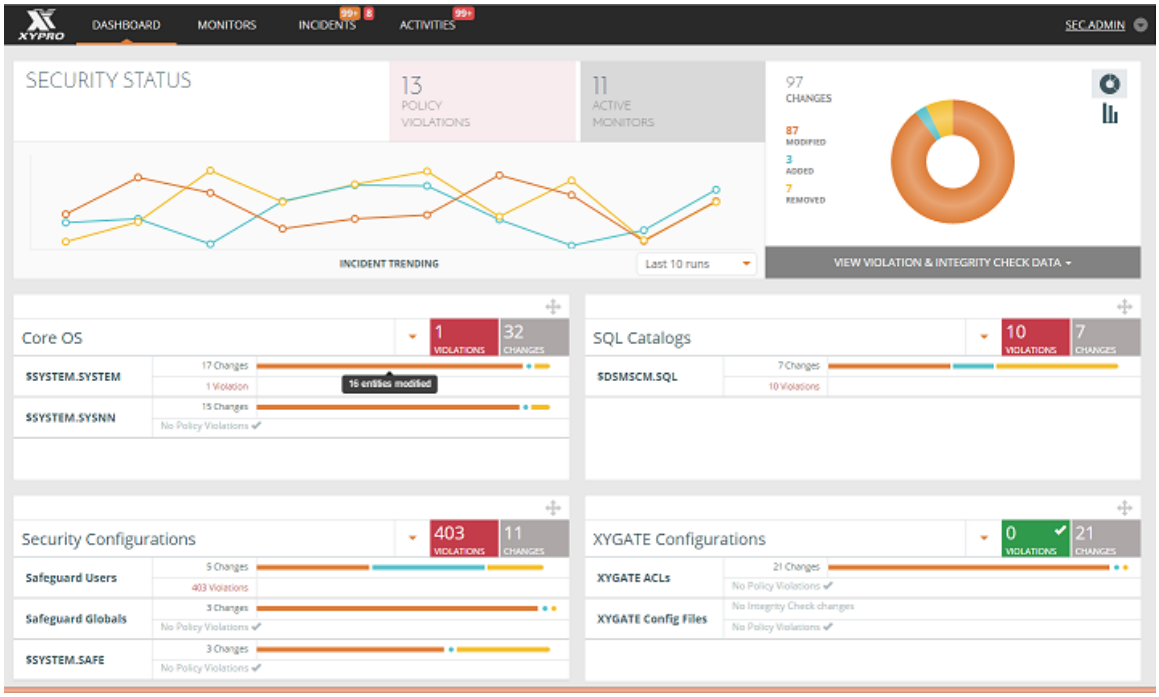
Security Intelligence algorithms and analysis techniques take the data sets that are already being generated from disparate sources in your enterprise, such as security audits, application logs, network flows, vulnerability management, configuration data, keystroke logs etc… It slices and dices that data, pivots the data and ultimately correlates the common elements between these unrelated sources while adding a layer of context to the correlation based on specific indicators of compromise for that system. You have now armed yourself with a proactive method to track anomalies and detect security events important to your environment, while separating the noise from the actionable data.

This real time correlation and contextualization of data sources enables notifications to security analysts of the anomalies that are being measured on a system as they're occurring. Say for example commands are being issued on a system that are not typical of the user issuing them. By recognizing this and correlating that activity with suspicious network flow and additional sources of data, security intelligence algorithms can detect and alert that something is happening on the system that is outside of what is normal for the given environment. This powerful concept provides meaningful interpretation of the data, allowing security practitioners to have the upper hand in detecting suspicious activity before you've reached the tipping point.

XYGATE SecurityOne™ – Security Intelligence and Analytics for the NonStop

Mission critical systems like the HPE Integrity NonStop Servers house an organization's most valuable applications and assets and must be protected against a variety of threats. Although the NonStop has unique security features not typically seen on other enterprise systems, it is still at risk from insider and outsider threats, misuse, non-compliance and security breaches. As systems grow larger, faster and more economical, the amount of data generated, and thus put at risk, exponentially increases. Keeping track of what is happening to that data and those systems becomes a very expensive and inefficient exercise for system operators. Without proactive control and visibility into their NonStop infrastructure, organizations expose themselves to greater risk. Current solutions do not provide the specialized NonStop security intelligence and contextualization to paint the correct picture for this purpose.

XYPRO is proud to announce XYGATE SecurityOne™ . A brand new product that provides a comprehensive, single pane of glass approach to control and contextualize NonStop security through policy management, data protection and security analytics. The result? Meaningful reduction in the Mean Time to Detection.



XYGATE SecurityOne™ introduces an intelligence platform never seen before for the HPE Integrity NonStop Server. Leveraging existing native HPE NonStop security information, all of the XYGATE suite's extensive security data information and extensive new functionality, XYGATE SecurityOne™ incorporates multiple NonStop security intelligence data feeds into a single, easy to use, browser interface for a single-view visibility of your NonStop Systems' security.

Using our patent pending technology, XYGATE SecurityOne™ gathers data from multiple, disparate NonStop server sources and uses specialized security intelligence algorithms to correlate, contextualize and analyze events. For example, combining application data, user behavior, file operations, network data, command input and other sources to paint a detailed security incident picture in real time for the NonStop, enabling security operators to hone in on and detect security events before they culminate into an "incident". XYGATE SecurityOne™ draws your attention and alerts you to the items you need to be aware of, allowing you to effectively prioritize your response and countermeasures.

With its summary/detail dashboards and customizable, easy to use browser interface, XYGATE SecurityOne™ enables you to manage security configurations, harden your system security based on NonStop best practices, measure and enforce compliance and policies on a global level, take the guess work out of audit and forensic investigations, intelligently analyze your NonStop security data and much more.

The value of security intelligence and the way it takes the human effort involved in data analysis, contextualization, correlation and pattern matching and automates it cannot be underestimated. This complex analysis allows for efficient and effective processing of security data so your security team can make quicker, informed decisions on events that are relevant to them. This in turn yields additional benefits by reducing operational costs, simplifies management, enhances security and increases response times. This is why Security Intelligence and Analytics have one of the highest perceived ROIs compared to its cost.

Organizations recognize the value of intelligence based on data analysis in other parts of their business strategy, like marketing – security intelligence is no different. Being able to leverage the data you already have access to through automated analysis empowers your organization to quickly and efficiently deal with the threats that are constantly evolving.

[1] Source: MANDIANT M-Trends 2015: A VIEW FROM THE FRONT LINES

Steve Tcherchian
CISO and Product Manager, XYGATE SecurityOne™
XYPRO Technology