White paper

VECTRA®

Detect insider attacks in real time

VECTRA®

TABLE OF CONTENTS

Many people steal from their workplaces. But there's a big difference between pocketing some pens and sticky notes, and walking out the door with source code, strategic marketing plans, financial or health information, credit card data, or a fat list of customer contacts.

In some cases, employees or contractors are acting maliciously, intent on destruction, misuse, corruption or theft. They may take high-value information with them to their next job, feeling they should be the rightful owners of their work product.

Or, more often, they are simply inattentive or negligent about their use of account credentials, opening the door to information theft by an external attacker.

A high-risk threat

Whatever the cause, insider threats pose a significant risk to organizations of all sizes and in all industries.

Insider threat cases make up 28% of all cybercrime and more than a third of organizations reported an insider cyberattack in 2013, according to a U.S. State of Cybercrime Survey from the Computer Emergency Response Team at Carnegie Mellon University.

And 32% of affected organizations said that the damage caused by insider cyber attacks was greater than outsider attacks. The result is an annual $2.9 trillion loss from employee fraud around the world.

Understanding the insider threat risk profile

Insider incidents may be intentionally planned and executed, or the result of negligence, and may transpire over weeks or months.

In a malicious insider attack, a disgruntled employee may direct his anger against the organization as a whole or against specific coworkers. For example, Chuck works as a systems administrator at a national retail chain and was recently denied a promotion he thought he deserved.

Mary, with whom he has had a long-simmering feud, was promoted, and in retaliation, he steals Mary's account credentials and uses them to steal customer credit card numbers from secure internal systems and sells them on an illegal online market.

The theft of millions of cards is discovered, and the retailer faces significant financial and reputational damage.

In this scenario, Chuck, the malicious insider, figures out how to steal the account credentials, using personal knowledge or Web searches to sleuth out his coworker's passwords, and then experiments with different methods to steal the credit card information.

Once he's found a workable method, he goes into execution mode, stealing and using Mary's credentials to download credit card data. Because he is an employee, he can simply download them to his laptop and walk out the door. The final step is escape or evasion, where Chuck deletes all of the digital footprints that could lead back to him.

Theft can also occur due to an outside attacker relying on an employee's moment of inattention or negligence. Stan works at large hospital and in his spare time is building a social network for patients with diabetes.

Stan builds a prototype on his own external Web server, and wants to test it using real data. He copies the hospital's internal database to Dropbox, and loads it to his personal Web server for testing.

Unfortunately, Stan's Web server is poorly secured and is quickly compromised, and patient data is exposed to the public. Without proper oversight, Stan's good deed turns into a major breach of protected health information, resulting in HIPAA violations for the hospital.

Detecting insider threats today

Detecting insider and targeted threats today requires skilled security analysts, a hefty digital tool bag, and a tremendous amount of time. IT security operations already have an overwhelming workload.

It includes protecting their organizations from increasingly sophisticated and successful external threats, developing strategic security plans, ensuring regulatory and industry compliance, and training workers in security best practices.

Figure 1: Today's insider threats are detected after a breach and investigators perform time-consuming forensics that may not uncover the culprit.

Insider threat detection often relies on the post-breach forensics, such as monitoring and recording sufficient amounts of information to enable litigation. A better, more proactive approach involves real-time detection as threats happen or before they occur. This is highly desirable over sifting through the debris of a disaster.

Many security operations teams write queries for security information and event management (SIEM) systems to find clues to possible insider incidents. This involves correlating mountains of information collected by security products such as firewalls and data leak prevention.

Finding meaningful information among many petabytes of data is like looking for the proverbial needle in a haystack that grows larger every day. Because of the manpower required, this approach is often used only after an incident has been reported.

Taking action against insider threats requires close collaboration among human resources, IT and legal departments. But before human resources and legal can get involved, they need tangible evidence of insider threat behavior, and IT needs the ability to gather that evidence.

Legal may then be able to provide information about ongoing investigations and legal procedures. Otherwise, with nothing to go on, human resources and legal can't provide information proactively and insider threats will continue to cause damage, as they remain undetected.

A new approach to detecting insider threats

Vectra provides real-time insight into all threats – whether insider, targeted or opportunistic – by applying a combination of data science, machine learning and behavioral anlysis.

The Vectra X-series platform provides comprehensive insight into potential insider threats by putting an organization's high-value assets at the center of real-time investigations of insider and targeted attacks.

Vectra provides continuous monitoring of all internal network traffic across all operating systems, applications and devices. Based on the monitored traffic, communities of users, devices and high-value data assets are constructed, reflecting the organization's actual network behavior. Unusual connections, data exchanges and changes in community membership become visible and traceable.

Vectra then identifies and prioritizes risks, placing behavior anomalies in context with an organization's high-value assets.

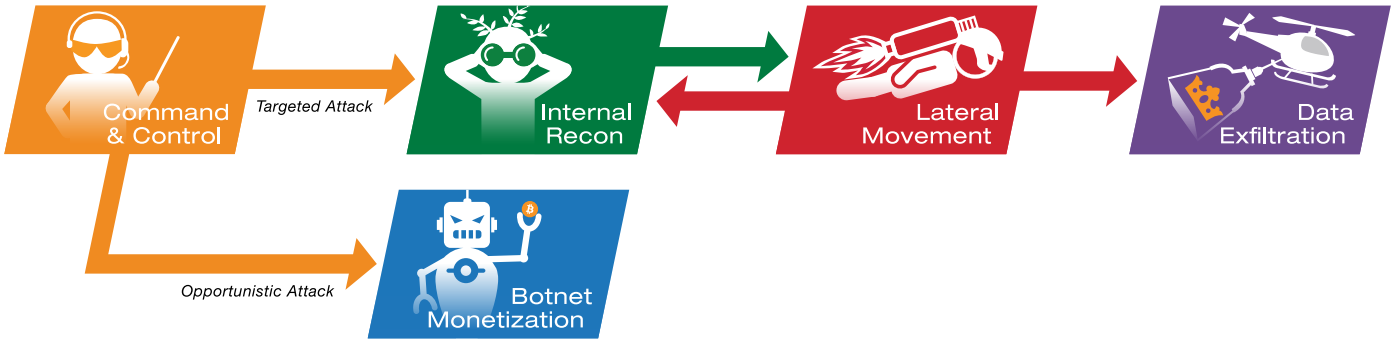

Figure 2: Vectra detects insider, targeted and opportunistic threats in all phases of the attack kill chain.

Whether an insider, targeted or opportunistic threat, Vectra detects all phases of an attack, including command and control, internal reconnaissance, lateral movement, and data exfiltration.

Inside attackers already have authorized access and may exfiltrate data by carrying it out on a laptop, a USB drive or other portable device, which is an activity that perimeter security can't detect.

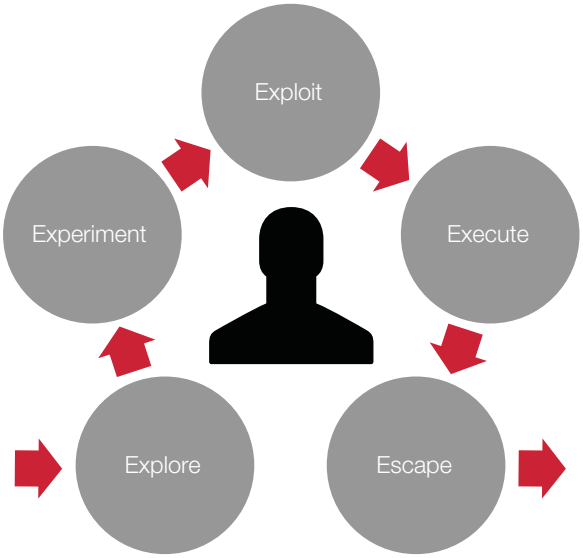

Figure 3: Phases of an insider attack.

Phases of an insider attack

In a malicious insider attack, an employee or contractor typically begins by exploring the environment to find weaknesses, and then experiments to find a successful method before finally executing the attack and then attempting to evade detection and ultimately escape.

If it is a case of willful negligence, the insider may simply open a door to an external attacker who plants malware that could be used to steal account credentials or data.

To detect insider threats, Vectra identifies the indicators and anomalous behaviors of an insider as they occur over weeks or months. The activities of an inside attacker are detected in the same way as a targeted attacker that has evaded perimeter defenses and is now inside the network.

Vectra can detect an insider performing reconnaissance activities, such as scanning ports on another internal host that may go undetected in the normal network chatter.

Additionally, Vectra detects the lateral movement of an inside attacker, such as a brute-force attack on another internal host into which he attempts to login to acquire stolen credentials.

Vectra also detects the accumulation of data from one or more internal hosts that the attacker may exfiltrate manually, such as walking out with the data on his laptop.

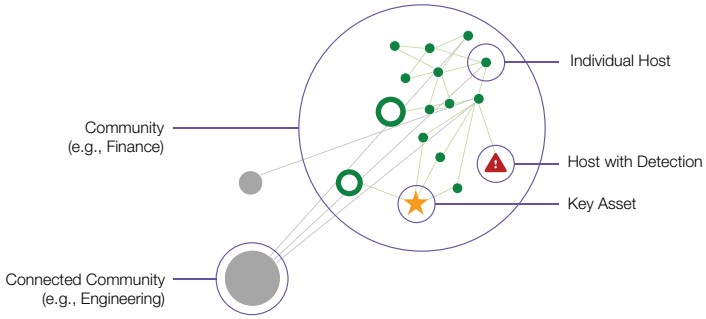

Figure 4: Vectra uses machine learning to identify host communities based on observed network traffic.

Putting key assets at the center of threat investigations

Vectra observes the behaviors of user host and server connectivity. Continuously monitoring the normal interaction of users and data servers exposes users and hosts that communicate in anomalous ways.

Vectra puts an organization's key assets at the center of real-time investigations of insider and targeted threats. It provides a dynamic visualization of communities so administrators can see at a glance how hosts typically communicate and interact.

This elegant representation vastly simplifies the complex relationships within communities, enabling administrators to spot potential dangers of malicious or negligent insiders and take action.

For example, Chuck's laptop, which normally only connects to hosts within the system administration community, is detected communicating with hosts in the finance community over the weekend and downloads massive files of credit card data.

With Vectra, the security operations team can see at a glance the new connections and anomalous behavior. A quick click on the host reveals any threat detections, and if needed, IT can investigate further.

In Chuck's case the security administrator will see that Chuck's machine connected to database servers last weekend, downloaded a large amount of data and his host subsequently sent an equal amount of data to an IP address registered to Dropbox.

Security that thinks™

It's time for security to get smarter. With Vectra, organizations of all sizes can easily identify the anomalous activities of malicious and negligent insiders, whether they are employees or contractors.

This enables security teams to detect and stop any attack – insider, targeted or opportunistic – while or even before it is in progress. Vectra protects an organization's high-value assets with security that continuously listens, thinks, remembers and anticipates the next move of an attack.

VECTRA®

Email info@vectranetworks.com **Phone** +1 408-326-2020 www.vectranetworks.com