RisqVU Information Security Telemetry

EARLY THREAT DETECTION USING TELEMETRY DATA

- A SOLUTION TO TODAY'S RAPIDLY EVOLVING CYBER THREATS

PALADION
BETTER SECURITY OUTCOMES

EXECUTIVE SUMMARY

With the cyber attack landscape changing daily, network infrastructure needs to respond at a similar rate. True situational awareness in information security depends on a security approach that provides continuous monitoring using advanced techniques that combat the latest developments in cyber attacks. Paladion's RisqVu IST is the answer to this problem, providing users with an agent less telemetry based information security solution that addresses the constant advancements in cyber attacks. RisqVu IST also addresses the need for situational awareness, allowing for open communication and focus on the security posture of an organization.

TABLE OF CONTENTS

BACKGROUND

THE MODERN CYBER ATTACK

With the cyber attack landscape changing daily, network infrastructure needs to respond at a similar rate. True situational awareness in information security depends on a security approach that provides continuous monitoring using advanced techniques that combat the latest developments in cyber attacks. Paladion's RisqVu IT is the answer to this problem, providing users with an agent less telemetry based infrastructure security solution that addresses the constant advancements in cyber attacks. RisqVu IST also addresses the need for situational awareness, allowing for open communication and focus on the security posture of an organization.

THE CASE FOR SITUATIONAL AWARENESS

Situational awareness as it applies to information security is the means in which an organization understands its environment through constant, reliable, timely feedback about its security posture and a well defined strategy communicated across all channels to remediate problems. An organization should be able to predict and respond to an event and everyone in that organization should know his or her role in reacting to that event. This comes first with identifying who the enemies are and what tactics they are using.

HOW WE GOT HERE

Traditionally, vulnerabilities in software have been thought of as the prime weakness which can be exploited by attackers or malware. While defense techniques have evolved with vulnerability scanners and patch management, attackers have now de-vised techniques to exploit the weaknesses and insecure features of an entire operating system.

In the case of antiviruses and other threat prevention mechanisms, a defense was built by investigating signatures to counter threats. However, attackers devised another approach to conceal their signatures, relying on weaknesses in account security.In fact, some attacks are even able to turn off host based defenses altogether. The human aspect of network security often falls prey for social engineering attacks such as phishing, leading to their accounts being compromised. This technique is still one of the most powerful attack vectors in practice.

If we aggregate attack analysis over the last five years, it is apparent that modern day hackers consider multiple dimensions when devising attacks, while security solutions on the market are single-dimensional thereby addressing only a part of the overall problem.

ATTACKS AFFECTING IT INFRASTRUCTURE

MALWARE

Malware is a broad term that literally refers to any "malicious software" and includes viruses, trojan horses, ransomware, adware etc. Modern day malware, however, is developed as self-propagating programs which can automatically spread over a network. Malware deployment has two phases: entry and propagation.

To enter a corporate network, malware employs techniques like social engineering and file execution to find an entry point. The next phase necessary for success is propagation. Malware propagation refers to the method by which malware is transmitted to the device or system which it intends to infect. In the past, operating systems built defense capabilities to disallow malware to conduct further attacks. As a result, malware now follows more dynamic approaches to conduct attacks.

The obvious choice for any malware to propagate further would be to look for and wait for exploitable weaknesses in network interfacing components like file-sharing or a remote desktop. Therefore, it is important to continuously monitor for exploitable weak-nesses.

THE THREE DIMENSIONS OF INFRASTRUCTURE SECURITY

Modern day attacks on infrastructure like malware generally exploit one of three dimensions to further evade and propagate.

Those dimensions are vulnerabilities, insecure design and privileges. While vulnerabilities can be addressed through patch management, the other two require more tactful security measures..

Traditionally hardening of IT infrastructure has been done by turning off all insecure features, however, that can negatively affect the utility of the system. Therefore, turning off the system for regular business is a common practice. This problem has been exploited by malware developers and hackers. After a successful evasion they will turn on such features to conduct further attacks through lateral movement and then shut it down when the action is over.

In the case of privilege issues, modern day malware targets accounts for lateral movements through phishing. Once cyber attackers have gained entry into a corporate account, they will then look for account security weakness like a shared folder over a network or will even create a local user and add it to an administrator account. Cyber criminals will also look for "hanging accounts" which exist when an employee leaves an organization but there account is not deactivated.

The only solution to this problem is to continuously monitor your IT infrastructure to detect compromising patterns and raise an alert when detected. Unfortunately, traditional host based compromise detection systems cannot keep up with the latest advances in cyber attacks.

THE PROBLEM WITH HOST BASED SYSTEMS

Most current compromise detection systems are host based and use an agent to regularly check for malware by matching file hashes. Modern day malware has evolved beyond this detection by instituting "polymorphic malware" and modern day attacks have evolved to override host based defense systems by turning them off.

THE PROBLEM WITH CURRENT CONTINUOUS MONITORING SYSTEMS

The most common continuous monitoring systems gather all possible data to create a "golden profile" which they will use to track deviations, flagging them for future investigation. Unfortunately, this category of systems uses considerable network bandwidth and disk space.

SOLUTION

RISQVU IST

RisqVu IST is a telemetry based information security software that analyzes the security posture of your IT infrastructure to provide immediate situational awareness of security issues. Without the need to install an agent, you can collect security posture measurements remotely and scan and monitor from both on-site and cloud based systems. IST also supports over 25 existing platforms, provides over 5000 types of measurements, and helps achieve regulatory compliance within your industry. While most infrastructures will have some part on premise and some on cloud, RisqVu IST can scan and monitor both seamlessly without any agent.

THE TELEMETRY DIFFERENCE

Telemetry based security systems are, by design, difficult to evade by social engineering attacks as compared to host based prevention systems. This approach uses inbuilt components like ssh server and power shell for collecting information on the current security posture of servers and desktops and then feedsit to the analysis engine to detect compromisable behavior and patterns.

RisqVu IST's core engine is an advanced telemetry system which can collect security posture measurements remotely without an agent. The so called “Plug-n-play” feature of RisqVu IST allows it to be installed seamlessly into an existing network.

Another key benefit of telemetry based approach is hassle free deployment. As there are no agents, only the scanning server needs to be installed and maintained. Agents consume significant power and memory which can slow down performance. A telemetry based agent-less approach reduces this overhead to a great extent leveraging inbuilt components of an operating system to only collect data while analysis of the collected data occurs on the server so that the target machine performance does not suffer.

In addition, RisqVu IST uses an analysis engine that turns your security into code. The primary task of the analysis engine is to look for unsafe conditions in the collected data using a primarily SPL script execution engine.SPL, or Secure Programming Language is a simple script based language and is easy to learn. The script based approach also helps to control output or observations. This kind of flexibility makes RisqVu IST a very good fit for an enterprise.

RisqVu IST USE CASES

COMPROMISE DETECTION

Hackers use malware to look for exploitable scenarios to penetrate which occur from insecure features of IT infrastructure. RisqVu IST detects these compromisable patterns and can detect malicious activities to prevent malware from exploiting scenarios in the first place. Use cases include antivirus not running, folder sharing with global access, checking for failed login accounts that don't exist or bad image name and process running.

ACCOUNT SECURITY

Modern day (more urgent) malware targets user accounts for lateral movements. Using phishing methods, cyber attacks gain entry into a corporate account and then look for weaknesses in account security. It is also a requirement of PCI DSS and ISO to check for issues in user accounts. RisqVu IST defends against advanced persistent threats and malware by frequent checks for the existence of hanging accounts, dormant accounts or resigned user accounts.

SECURITY APPS

During events like zero day attacks it is often necessary to launch countermeasures immediately. RisqVu IST allows specialists to respond via security apps. Powered by telemetry and analysis engines, it converts security to code.

CONFIGURATION ASSESSMENT

It is often necessary for users to assess the security of configurations applied to an IT infrastructure. RisqVu IST's telemetry engine collects required configuration and supplies it to the analysis engine which makes assessments on safe or unsafe conditions. In addition, RisqVu IST comes prepackaged with assessments that can be modified to fit custom requirements.

COMPLIANCE MONITORING

Due to multiple regulations, RisqVu IST can monitor compliance of IT infrastructure against regulations form PCI DSS or ISO. Users can either define compliance requirements or link to the existing security configuration assessments. The telemetry engine collects all required data from the target infrastructure and passes it to the analysis engine for assessment which decides on compliance or non compliance status. In addition, compliance can be monitored on a routine basis and the system raises alerts if there are deviations.

USE CASES

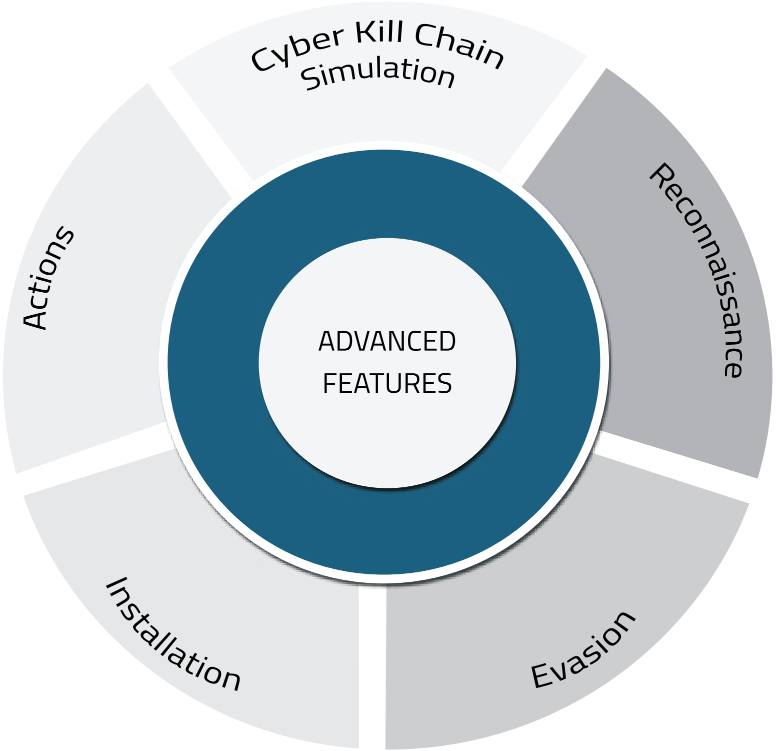
VULNERABILITY ASSESSMENT

Scanners are needed to determine multiple vulnerabilities. RisqVu IST is integrated with multiple scanners to conduct vulnerability assessments that can be pulled in for further assessment. This includes PCI DSS vulnerability management requirements and ISO 27001 technical control requirements.

SITUATIONAL AWARENESS MADE SIMPLE

Since situational awareness is a necessity to understanding infrastructure and assessing potential problems that may occur, RisqVu IST's situational awareness dashboard allows end users to drill down from their mission requirements and address security issues present in the infrastructure to involve the decision makers. With this picture available, leaders can gauge negative situations which are prevailing in their environment ultimately facilitating decision making.

ADVANCED FEATURES



CYBER KILL CHAIN SIMULATION

Risqvu IST has the capability to correlate and map all of your IT infrastructure security issues to create and implement a cyber kill chain. A cyber kill chain is a plan of attack which predicts that malware will follow a pattern to achieve its goal. The stages of the cyber kill chain include:

Reconnaissance

This is the stage in which attackers attempt to gather data of your IT infrastructure to craft an attack.

Evasion

In this stage, attackers or malware will exploit certain weakness to invade your infrastructure. The attack can range from vulnerability exploitation to a social engineering attack.

Installation

After a successful evasion, the malware seeks to install itself. Malware will persist in your disk with stealth so that antivirus and other defense mechanisms are unable to detect it.

Actions

From this phase malware will try to conduct actions like communicating with the mother server, attempting to collect data and propagate further.

When RisqVu IST aggregates your infrastructure security issue data and maps it to various phases, it is able to create a simulation. This simulated output can provide actionable insight and valuable context to your security issues.

ARCHITECTURE

The core of RisqVu IST is its three engines: a Telemetry engine, Analysis Engine and Discovery Engine and all other modules are built leveraging features from these three engines. First, the telemetry engine collects security related data from a wide variety of infrastructure such as operating systems, databases, web servers and routers. Next, the analysis engine executes analysis logic over the collected data to identify security issues. Finally, the discovery engine can discover Live IPs and raise alerts upon unmanaged assets in a network.

These three engines collaborate to provide a unified IT infrastructure security framework. Apart from core engines, the framework also establishes a communication channel between host machines and a server.

In addition to the unified security framework there are three scanning engines. An Account Security Scanner is responsible for assessing issues related to accounts in various hosts. A Security Configuration Scanner assesses issues related to insecure features of your IT infrastructure. Finally, a Vulnerability Scanner assesses issues related to software bugs in the infrastructure.

In the top zone we have a monitoring framework which leverages scanning engines and enables continuous monitoring for all scanners as well as an engine dedicated to compromise detection and one devoted to compliance monitoring.

MANAGING YOUR SECURITY OPERATIONS

Manage Remediation

Whether its account security or security configuration scanning, the result will always be a list of issues which needs to be quickly remediated. After remediation, you will have to verify by rescanning to assure a closure. This complete workflow is available in the remediation tracker of RisqVu IST where you can create, assign, close and verify tickets.

Manage Exceptions

RisqVu IST allows you to create, manage and track time based exceptions. Whether an exception is time limited or permanent, asset based or subnet based, security practitioners are often required to subdue an alert on specific hosts. For example, it might be necessary to allow a legacy system to use a custom port since it cannot be changed. With RisqVu IST, you can create time based exceptions that will produce an alert when it has expired rather than while it is still active.

Manage Your Scan Schedules

With hundreds of IT infrastructure components, it becomes paramount to effectively manage scheduling for all of your scans. To avoid peak business hours and avoid network traffic overhead, it is ideal to run a scan during non business hours with alerts to its beginning and completion. With RisqVu IST, you can define multiple frequency levels to automatically initiate scanning and designate "blackout hours" to easily define times when scanning should not take place.

Manage Alerts

Alerts are pivotal to security management systems since they define triggers to actionable cases. RisqVu IST allows you to easily create alerts for various trigger points so thatonce a trigger point is detected, email based notification alerts are sent immediately. Alerts are omnipresent in all modules of RisqVu IST.

RisqVu IST can also be integrated with any third party incident management systemso that certain high risk alerts, including compromise detection patterns, can be pushed for incident response.

Manage Compliances

"Auditonce, complyall" is the mantra by which RisqVu IST's compliance engine works. You can manage your policies and map them to compliance requirements from one place. In effect, one scan can generate results against various compliances, thereby easing compliance management to a greater level.

CONCLUSION

IT infrastructure will always remain the weakest link in information security after humans so it is paramount that organizations plan for adequate controls to keep risks under acceptable levels. New age attackers have evolved to mix and match issues from various dimensions and hence countermeasures need to evolve accordingly.

RisqVu IST addresses these problems by using multi-dimensional security assessment. Attackers don't rely on a single dimension so the defense also needs to counter on all dimensions including the use of insecure features, account security and vulnerabilities. Only when cyber security takes on cyber attacks on a level playing field will an organization truly be secure.

PALADION

BETTER SECURITY OUTCOMES

ABOUT PALADION

Paladion Networks is a specialized partner for information risk management providing end-to-end services and solutions in the US, Europe, Asia and the Middle East. Paladion is rated and has been recognized and awarded by Gartner, Asian Banker and Red Herring, amongst others.

For over 15 years, Paladion has been actively managing information risks for over 700 customers. Paladion provides a complete spectrum of information risk management comprising of security assurance, compliance, governance, monitoring, security analytics and security management services to large and medium-sized organizations. Paladion is also actively involved in several information risk management research forums and has authored many books on the same. With a staff of over 800 dedicated security experts, Paladion has 6 Security Operations Centers (SOCs) across the world.

Head Office: Bangalore: Shilpa Vidya, 49 1st Main, 3rd Phase, JP Nagar, Bangalore- 560078
Phone : +91-80-42543444, Fax : +91-80-41208929
Abu Dhabi: +971-55-9891227, Bangkok: +66 23093650-51, Doha: +974 33559018, Dubai: +971-4-2595526, Jakarta: +62-8111664399,
Kuala Lumpur: +60-3-7660-4988, London: +44(0)20 7148 7475, Mumbai: +91 022 33655151, Riyadh: +966 (0) 11 4725163, Stuttgart:
+49-711-7224-9626, Toronto: +1-416-273-5004, Virginia: +1-703-8713934, Muscat: +968 99383575 (Business Associates)
sales@paladion.net | www.paladion.net