OVERVIEW

Organizations today must learn to cope with constant infiltration. Keeping cyber attackers out of enterprise IT environments has become extremely difficult and, in some cases, impossible because custom-crafted attacks can easily circumvent traditional threat detection tools and exploit inherent weaknesses in modern networks. Infiltration, however, does not need to result in data theft and other forms of business damage, especially if organizations become adept at detecting and responding to attacks early.

Detecting attacks before they result in harm requires security teams to reduce their reliance on passive forms of threat detection, such as alerts from signature-based scanning tools. Instead, organizations must actively hunt for intruders by constantly scouring their IT environment for subtle signs of malicious or suspicious activity. Finding these early signs of problems requires organizations to cultivate new capabilities in data analysis and incident response.

Cultivating new capabilities, however, can be prohibitively difficult for security teams pinched by staffing shortages and overwhelmed by the scope of ever-expanding applications, infrastructures, and threats. The challenge most security teams face is how to prioritize which problems to address, given the constraints they have—distinguishing the most serious threats from the myriad of nuisance threats.

The challenge is addressed by Intelligence Driven Security, an information security strategy that delivers the visibility, analytical insights, and corrective actions needed to help organizations mitigate the risk of operating in a digital world. Intelligence Driven Security enhances the speed and effectiveness of cyber threat detection and response by:

• Providing visibility into digital activity within logs, the network and at end points
• Using advanced analytics from diverse data sources to uncover hidden threats and to guide decisions on how best to mount a targeted, effective response
• Utilizing signature-less malware detection on networks and endpoints
• Empowering security teams to be more effective through efficient processes, workflow automation, threat intelligence, and education

To achieve Intelligence Driven Security in threat detection and response, organizations should advance their capabilities in four areas:

1. Network and endpoint monitoring that is constant and comprehensive, including capabilities such as full-packet capture and behavior-based threat detection on hosts
2. Advanced analytics techniques that can sift through massive amounts of information, such as network traffic, in near-real time to spot suspicious behaviors and accelerate investigations
3. Malware analysis using methods that don’t rely on file signatures and go straight to the actual behavior of executables, whether collected on the network or endpoints, to detect hostile activity
4. Incident detection and response practices that align security personnel, processes, and technologies to streamline and accelerate workflows so security operations teams can spend less time on routine tasks and more time defending high-priority assets and addressing the riskiest threats
A CONSTANT STATE OF COMPROMISE

Most organizations’ IT environments have been infiltrated by outside parties. In many cases, attackers have established a persistent presence. That’s not alarmist; it’s a reality created by a different breed of attacker taking advantage of today’s hyperconnected networks.

Today’s most dangerous attackers aren’t part-time activists or moonlighters looking to make mischief or a statement. They’re professionals looking to make money. They’re nation-states looking to advance their strategic agenda. And they enjoy many advantages.

Increasing interconnection among IT systems and applications has brought new efficiency and opportunities for organizations. Networks are open to more partners and supply chains to facilitate ever-more collaborative business processes. But attackers also exploit that openness by targeting vulnerabilities in the value chain, making the weaknesses of less secure participants a collective weakness. Meanwhile, the virtualization and outsourcing of IT infrastructure and applications offers efficiency advantages that have become impossible to ignore. But moving to the cloud also moves critical IT functions off-premises, often in a range of locations with varying policies and procedures for information security.

Today’s interconnected IT environments are harder to defend and offer many more places for intruders to conceal their activities. Combined with the fact that many attackers modify malware to escape detection by traditional signature-based scanning tools such as anti-virus software, firewalls and intrusion detection systems, and it’s clear to see that infiltration has become the new norm. The question is how well organizations can adapt to this constant state of breach.

Stretched security teams can no longer focus exclusively on preventing infiltration. They must balance attack prevention—an impossible goal—with complementary competencies in attack detection and remediation. Today’s organizations may be vulnerable to infiltration, but that doesn’t mean that data theft or business damage is inevitable. Organizations must proactively identify and neutralize the threats inside their IT environment before attackers achieve their objectives. The best way to do this is by leveraging Intelligence Driven Security, a strategy for solving today’s most serious and sensitive security challenges.

Intelligence Driven Threat Detection and Response

Intelligence Driven Security helps organizations neutralize cyber threats before they cause significant problems. The strategy delivers the following capabilities:

- Unprecedented visibility into networks and their end points, capturing and parsing enormous amounts of security relevant data.
- Sophisticated analytics to sift through the data, identify anomalies and then alert organizations of potential problems tied to its information assets
- Activation of incident response processes to make threat investigation and remediation much more efficient and effective
Intelligence Driven Security stops cyber attacks before damage is done

Applying the Intelligence Driven Security strategy to incident detection and response means organizations should cultivate capabilities in four interrelated areas that are critical to discovering, investigating and responding to advanced attacks:

1. Network and endpoint monitoring
2. Advanced analysis of security-related data
3. Malware identification and analysis
4. Incident response and breach remediation

**NETWORK AND ENDPOINT MONITORING: SEE EVERYTHING**

Faced with constant streams of data moving over the network, the temptation—and until recently, the only option—has been to focus data collection and analytics on select problem areas. Security teams often collect and analyze logs from critical systems, but this log-oriented approach to threat detection leaves many blind spots that sophisticated adversaries can exploit.

Intelligence Driven Security aims to eliminate blind spots by providing comprehensive visibility both on the network and on endpoints such as servers and employees’ computers.

Comprehensive visibility on networks and endpoints

Intelligence Driven Security solutions use logs as one of many data sources, but they achieve far greater visibility by also incorporating network packet-capture capabilities. Full network packet-capture means recording, parsing, normalizing, analyzing, and reassembling all data traffic at every layer of the network stack. As network traffic is captured, it’s analyzed and tagged to facilitate subsequent threat analysis and investigation. Capturing and tagging network data enables security analysts to reconstruct users’ sessions and activities to understand not just basic details such as what time or to which IP address specific data packets were transmitted, but exactly what information was sent in and out and the resulting damage. Full packet collection and session reconstruction help organizations detect security anomalies and reconstruct security incidents with certainty and detail so they can investigate their losses and remediate problems faster and more effectively.
Intelligence Driven Security solutions also provide deep visibility into activities on endpoints, including servers and laptops. To detect suspicious endpoint activity that could indicate malware and other threats, solutions must analyze both what is happening in a computer’s memory and what is stored on the physical disk. By comparing running processes to files on disk—without relying on intervening operating systems and hypervisors, which may themselves be manipulated by malware—organizations gain insight into whether endpoint executables and processes are legitimate or have been maliciously injected. A deep, x-ray view of endpoints and automated detection of suspicious activity is crucial for identifying and investigating threats faster.

Real-time data collection and parsing

Security data such as logs, network packets, and endpoint activities are collected from diverse sources, parsed, and stored in a way that makes the information easy to centrally search and analyze. For example, effective network packet collection systems parse and tag data traffic as it’s getting collected for subsequent indexing, storage, and analysis. Internal security data and visibility are further enriched with threat intelligence from external sources. External threat data enables organizations to learn from others’ experiences to enhance their own threat detection capabilities.

Deployment wherever monitoring is needed

When visibility is urgently needed, such as when an organization is in the middle of an actual incident investigation, ease and speed of deployment are critical. Network and endpoint monitoring tools can often be up-and-running wherever they’re needed within a few days. This would include installing equipment with full packet capture capabilities at the organization’s main network ingress and egress points, as well as capturing data traffic to and from IT systems handling intellectual property and other high-value information. Software agents that scan for malware activity on endpoints can usually be pushed out to them within hours, depending on the size and scale of the implementation.

ADVANCED ANALYTICS: UNCOVERING HIDDEN THREATS

The unprecedented visibility created by an Intelligence Driven Security strategy does much more than capture the forensic data needed to re-create cybercrime scenes. It creates new opportunities to be far more proactive and predictive in threat detection, so organizations can prevent serious breaches and business damage. Intelligence Driven Security systems enable novel approaches to analyzing and reporting on user, machine, and resource behaviors—learning what behaviors are normal for a particular system, user, or resource and then finding and alerting on subtle signs when something is amiss.

Intelligence Driven Security systems incorporate the following principles:

Single, integrated platform for security monitoring and analytics

Intelligence Driven Security operations centralize the monitoring, detection, analysis, investigation and reporting of anomalies and incidents. Analysts can pivot through terabytes of log data, metadata and re-created network sessions with just a few clicks. Because details on both networks and endpoints are available through a centralized system and single console, analysts don’t need to toggle among different security tools and applications. Queries leverage this integration, saving analysts considerable time and effort. This means investigations that once took days can now be handled in mere minutes.
Technology integration is what makes this high degree of efficiency possible. The analytics platform must work with a variety of tools generating security-related information about servers, networks, endpoints and other vital IT systems. Metadata parsing and management consolidate events, logs and network data from many sources so they are all accessible for centralized analysis, alerting and reporting.

This integration extends beyond internal systems to the consumption of external threat intelligence. Intelligence feeds that can be ingested directly by the analytics platform, including open-source community intelligence, APT-tagged domains, blacklists, and suspicious proxies, are critical to providing timely detection of security issues.

Timely analysis of Big Data

Intelligence Driven Security systems capture and analyze massive amounts of rapidly changing data from multiple sources, pivoting on terabytes of data in real time. Security-related analysis is stratified to enable different types of detection. For example, data can be captured and analyzed as it traverses the network. This type of “capture time” analysis identifies suspicious activities by looking for the tools, services, communications and techniques often used by attackers without depending on logs, events, or signatures from other security systems. Examples of this capture time analysis includes the detection of non-browser software programs running HTTP, protocols over non-traditional ports, and executables embedded in PDF files.

Additionally, these sophisticated tools can detect subtle signs of attack by correlating events that seem innocuous in isolation but that are problematic when strung together. Analytical techniques fuse internal inputs from various sources using metadata. These advanced detection mechanisms also act as trip-wires that can provide early warning of potential infiltration. Processing of these information flows happens as they occur, meaning suspicious activities are spotted while there’s still time for security teams to stop attacks in progress.

With Intelligence Driven Security systems, security operations teams can also perform batch analysis on huge volumes of historical security data. Such data are needed not only to fulfill most companies’ data retention and audit requirements but they are also invaluable in uncovering adversarial tactics that may have taken many months to execute and may even be ongoing. For instance, batch analysis of security data archives can help uncover previously overlooked cyber-attacks in which illicit data was transmitted only sporadically in small, stealthy streams over weeks or months. These types “low and slow” attack techniques are hard to spot when they are occurring, because they are designed to seem innocuous by taking cover under existing processes and communication streams. These techniques usually become suspicious only when executed in a particular pattern over a specific window of time. Detailed, automated analyses of security data archives can discover attackers in the midst of establishing a foothold, as well as reveal information losses those organizations may not even realize they sustained. Oftentimes, batch analyses of security data can uncover treasure troves of information about attacker techniques and indicators of compromise that security teams can use in the future to detect similar attacks. Perhaps more importantly, batch analysis techniques help organizations learn what is “typical” within an IT environment so that future deviations from normal—which often indicate problems—can be identified and investigated as they arise.
Detection based on behaviors, not signatures

Intelligence Driven Security systems monitor the IT environment for signs of unusual behaviors—of people, applications, infrastructure, and communications—not just for explicit indicators such as previously identified malware signatures or blacklisted IP addresses or domains. Sophisticated attackers can circumvent such telltale, static monitoring approaches by modifying lines of code, by provisioning a new virtual machine in a public cloud, or by registering a new Internet domain as a command-and-control or drop site. It’s much harder, though, for attackers to circumvent security monitoring systems that are watching for unusual patterns and behaviors. Sooner or later, hostile malware or users must do something unusual that breaks with system norms, and that is when Intelligence Driven analytic systems will find them.

For example, when it comes to detecting malware, endpoint threat detection solutions don’t look for “known bad” files; look for suspicious behaviors. By comparing what’s actually running in memory with what should be running based on the files residing on the local disk, malware detection tools are better able to identify discrepancies and get a direct, more reliable view of whether illicit code is present.

Intelligence Driven Security systems establish what “good” behavior looks like within an IT environment by monitoring and learning a variety of machine and human activities, from what ports on servers are typically used for outside communications to employees’ individual log-in locations and habits. Activities observed to be outside the norm are flagged for investigation by security analysts. If analysts dismiss an event as a false positive, security tools can “learn” from that experience and are less likely to flag future recurrences.

Scalable without performance penalties

Data collection and analysis are handled by a distributed computing architecture, not a monolithic, centralized, database. By spreading the workload among many computing nodes, organizations get faster results and a highly modular, scalable system. To enable data gathering and analysis in a new network segment or at a branch office, organizations simply add a new node. This modular, distributed system can scale linearly as an organization’s data analytics requirements increase, without a performance penalty or a big jump in cost.

MALWARE ANALYSIS: TRUST NOTHING

Hostile software that anti-virus researchers have already flagged as malicious isn’t generally the malware used in targeted cyber-attacks. Nevertheless, some security tools still purport to protect organizations by scanning their IT environments using the signatures of easily altered malware.

Intelligence Driven Security systems forego signature-based scanning because of its obvious ineffectiveness. Instead, it uses the “trust nothing” approach to malware detection that assumes all programs are hostile, all communications are suspect, every machine is polluted, and every operating system is corrupt.
Risk-aware malware detection

Advanced threat detection tools examine the behavior of machines, networks, and processes to determine whether they are or have been compromised by malware. Such tools do more than detect incidents; they assess risk and prioritize alerts for remediation. Files determined to be malicious may warrant a lower prioritization score if they’re determined to be “garden variety” malware that causes more of a nuisance than a true threat. Conversely, files that bear no outward signs of tampering may contain a custom-compiled executable designed to run only when it reaches certain systems or when a covert command is given. To uncover this type of dangerous, customized malware, advanced threat detection systems use a series of analytical techniques to rate the risk levels of suspicious files.

For example, an organization may set a rule requiring the security system to analyze every new executable coming into its networks. The malware detection system would then “sandbox” new executables, running them in a quarantined environment, recording everything they do, and elevating their risk score if suspicious behaviors are observed, such as changing registry settings or replacing operating system DLLs. Of course, legitimate software could also perform these actions: to integrate functions with existing software or to install a patch, for instance. But if the new executable demonstrates one of these behaviors along with initiating unusual network connections, then its overall risk score skyrockets.

Intelligence Driven malware detection correlates multiple factors to make probabilistic decisions about risk and presents prioritized alerts to human security analysts. It is ultimately up to these analysts to decide the severity of a threat, but their decisions are greatly accelerated and more accurate because of the background work done by their Intelligence Driven Security tools.

Centralized correlation of suspicious endpoint activity

Scan results from endpoints are sent to a central server where known and unknown files are identified and suspicious activity is flagged. Files (including processes, drivers, DLLs, etc.) are analyzed and suspect levels are assigned based on the behavior observed. File behavior can be correlated at a global level across the enterprise to show if the potential malware is active on one machine and dormant on another. Organizations also gain insight into how prevalent a particular file is across the environment. For example, if a particular file is found on thousands of machines across the enterprise, then it may be a standard IT application that can be filtered out of security analysts’ view during an investigation. On the other hand, if a malicious file is identified, organizations can quickly gauge the scope of the infection by instantly showing all other machines with that same malicious file.

Prioritized alerts to accelerate malware investigation and remediation

To minimize the burden on security analysts, an Intelligence Driven approach to malware detection learns from previous scan results and a baseline of the environment to automatically flag unknown, suspicious files. Before scan results are presented to analysts, they’re checked against a global repository of items that analysts have previously investigated and whitelisted, meaning the files can be trusted. Trusted files are removed from scan results to quickly eliminate clutter for security analysts.
Endpoint threat detection consoles do not just present a list of scan results; they also prioritize prospective problems so analysts can identify which should be investigated first. To speed investigations, the endpoint threat detection console provides rich details about prospective problems. For instance, it correlates suspicious behaviors about a file (e.g., a driver, a process, a DLL), and then reveals what's known about the file (e.g., file size, file attributes, MD5 file hash) through static and heuristic analysis. Security analysts use the tools and information in the console to determine if the file is malicious, and should be blacklisted, or non-malicious, and should be whitelisted. If an item is deemed malicious, all occurrences of the problem across the entire IT environment can be instantly identified. Then, once a remedy is determined, the security operations team can perform any necessary forensics investigations and/or clean all the affected endpoints.

INCIDENT RESPONSE: FAST, FOCUSED ACTION

The growing size and complexity of IT environments have increased the scope of vulnerabilities, but that doesn’t mean all potential entry points present an equal risk. When a true attack or incident is suspected, security teams must act fast to cut off attackers within their IT environment and mitigate the damage. Doing that requires planning, staff training and, sometimes, outside assistance.

Practice and planning for effective breach readiness

Well-prepared security teams know what the organization's valuable information assets are and which systems, applications and users have access to them. Awareness of these parameters help security analysts narrow their field of investigation during a breach so they can address problems faster and with greater confidence.

Security operations teams should conduct breach readiness assessments and remediation drills to improve the speed and efficacy of their reactions to cyber attacks. As part of these assessments, security teams take inventory of the high-value IT assets that must be protected, review workflows for investigating and remediating incidents and evaluate areas for improvement. Proactive planning and practice compels organizations to map their security policies to their business priorities and regulatory requirements. It enables organizations to progressively improve their capabilities in threat detection, management and response. It optimizes staffing and skills on the security operations team so that scarce resources are deployed to maximum effect. It also provides targeted training to improve the incident response skills of security personnel.

Data-driven incident response for faster, better results

Security operations teams often find potential evidence of an infiltration or breach, but must initiate an investigation to understand the cause. Often organizations explore potential causes without success for weeks or even months. When that happens, it helps to bring in people with specialized expertise and tools in incident response (IR). IR specialists can deploy technologies that capture activity on networks and endpoints in key segments of the IT environment. Based on the scans, analyses and supplemental information these technologies generate, experienced IR professionals can usually pinpoint where and how security breaches are occurring and shut down ongoing cyber attacks much faster than organizations can do on their own.
Intelligence Driven Threat Detection & Response

Consolidated context to speed investigations

Intelligence Driven Security solutions collect a rich assortment of background and supporting detail to aid in incident investigations. Alerts from multiple security monitoring systems are aggregated into a single security management console, from which analysts can drill down to see data sources, affected machines, and other incident-related information with a few clicks of the mouse. The security management console also integrates with enterprise risk management software to provide contextual information on the business criticality of identified incidents and affected systems. Priority ratings are assigned to each incident based on the information assets at stake, the risks posed to the organization, and the seriousness of the security issue. Taken together, this supplemental information helps analysts investigate incidents more thoroughly, accurately, and quickly.

Additionally, Intelligence Driven Security systems ingest information from external sources to enrich the organization’s internal security data. The security analytics platform and management dashboard identifies, aggregates, and operationalizes the best sources of intelligence and context from inside and outside the organization to accelerate the analysts’ decision making and workflows.

CONCLUSION

Intelligence Driven threat detection and response helps organizations achieve predictably high standards of security despite today’s rapidly escalating and unpredictable threat environment. Intelligence Driven threat detection relies on gaining full visibility into networks and endpoints and applying advanced data analytics techniques to uncover malware without using hashes or signatures exclusively. Intelligence Driven threat response is led by experienced security personnel who are aided in their work by advanced security analytics and management tools. These tools greatly improve the speed and accuracy of security investigations by providing complete context around incidents from within a single management console and by prioritizing potential problems for further evaluation.

Intelligence Driven Security enables unprecedented efficiencies in threat detection and response, because it optimizes how an organization’s security personnel, processes and technologies work together as a whole. Tools are integrated to enhance security analysts’ visibility and understanding and to enable centralized analysis and reporting. Tools also guide investigative workflows and remediation processes based on proven procedures and the organization’s policies. By supporting security teams with a harmonized set of tools and processes, organizations can minimize the time that security analysts must spend on routine processes and free them up to focus on neutralizing high-priority threats. The end result is stronger, more agile security that not only helps organizations overcome their top security threats but also operate in the digital world with greater confidence.
INTELLIGENCE DRIVEN THREAT DETECTION AND RESPONSE
SOLUTIONS FROM RSA

RSA® Advanced Cyber Defense Practice provides a holistic range of solutions to help clients protect their organizational mission, drive operational efficiencies and evolve with a dynamic threat environment. Targeted attacks often focus on the theft of critical assets and data and utilize techniques that bypass traditional defenses. RSA helps organizations enhance their existing security capabilities and implement countermeasures designed to prevent cyber adversaries from achieving their objectives. Services offered by RSA include gap analysis, maturity modeling, cyber threat intelligence, infrastructure hardening and security operations development and automation. Services are designed to help organizations converge their technical and operational capabilities into a unified security program that aligns with risk management priorities and business objectives. RSA emphasizes the preventive measures required to protect the organization while also providing incident response and remediation services to reduce breach exposure time and to mitigate attacks.

RSA® Education Services provide training courses on information security geared to IT staff, software developers, security professionals and an organization’s general employees. Courses are taught by security experts from RSA’s Advanced Cyber Defense Practice and combine theory, technology, and scenario-based exercises to engage participants in active learning. The current curriculum covers topics such as malware analysis and cyber threat intelligence. RSA Education Services also offers a workshop on addressing advanced threats such as APTs. Courses are designed to deliver the maximum amount of information in the shortest period to minimize staff downtime.

RSA® Enterprise Compromise Assessment Tool (ECAT) is an enterprise threat detection and response solution designed to monitor and protect IT environments from undesirable software and the most elusive malware—including deeply hidden rootkits, advanced persistent threats (APTs) and unidentified viruses. RSA ECAT automates the detection of anomalies within computer applications and memory without relying on virus signatures. Instead of analyzing malware samples to create signatures, RSA ECAT establishes a baseline of anomalies from “known good” applications, filtering out background noise to uncover malicious activity in compromised machines. The RSA ECAT console presents a centralized view of activities occurring within a computer’s memory, which can be used to quickly identify malware, regardless of whether a signature exists or if the malware has been seen before. Once a single malicious anomaly is identified, RSA ECAT can scan across thousands of machines to identify other endpoints that have been compromised or are at risk.
**RSA® Security Analytics** is designed to provide security organizations with the situational awareness needed to deal with their most pressing security issues. By analyzing network traffic and log event data, the RSA Security Analytics solution helps organizations gain a comprehensive view of their IT environment, enabling security analysts to detect threats quickly, investigate and prioritize them, make remediation decisions, take action, and automatically generate reports. The RSA Security Analytics solution’s distributed data architecture collects, analyzes, and archives massive volumes of data – often hundreds of terabytes and beyond – at very high speed using multiple modes of analysis. The solution also ingests threat intelligence via RSA Live about the latest tools, techniques, and procedures in use by the attacker community to alert organizations to potential threats that are active in their enterprise.

**RSA® Security Operations Management** helps analysts detect and respond to security incidents and data breaches more efficiently by providing a centralized orchestration layer for security investigations that integrate people, process, and technology. The solution aggregates and connects security systems and processes to furnish an integrated context for incident response. It also helps security teams track and report on their key performance indicators. The RSA Security Operations Management framework is built on industry best practices for incident response and breach management.