VECTRA®

Minding the cybersecurity gap

Ontrex

Cybersecurity has become a boardroom-level discussion as organizations seek ways to stay agile while maintaining appropriate controls. Across all sectors of industry and government, organizations are working to protect their intellectual property, personally identifiable information (PII), public reputations, and in some cases, their very survival.

Cyber criminals are highly organized and well-coordinated. More than 895 billion data records have been stolen over the last decade, according to the Privacy Rights Clearinghouse. And those are only the data breaches that have been made public.

The cybersecurity gap

The cybersecurity gap exists between the time an attacker successfully evades prevention security systems at the perimeter and the clean-up phase when an organization discovers that key assets have been stolen or destroyed.

In the cybersecurity gap, an attacker has free reign in a compromised network for an average of 146 days, according to Mandiant. That's more than four months in which attackers have the freedom to spy, spread and steal.

In most cases, organizations are unaware that a network breach has occurred until after the damage is done. Mandiant has reported that 69% of organizations learned about their own security breach from law enforcement or another outside entity.

The risks of the cybersecurity gap are big and only getting bigger.

Failure to recognize the cybersecurity gap

Companies are investing more than ever in cybersecurity. Much of these investments are in prevention-based controls that are focused on stopping threats at the network perimeter.

In the prevention phase, Gartner forecasts that by 2017 organizations will spend more than $12 billion on the great wall of prevention machines – more than $9 billion on VPNs/firewalls, more than $1.2 billion on intrusion prevention systems, more than $2.7 billion on Web proxies[1] and about $500 million on malware sandboxes.

Ironically, the concept of a network perimeter has been in a steady decline since the use of mobile devices became widespread and organizations adopted BYOD. Yet security resources today are still focused on the perimeter, while the internal network is scarcely monitored for signs of active threats and nefarious behaviors.

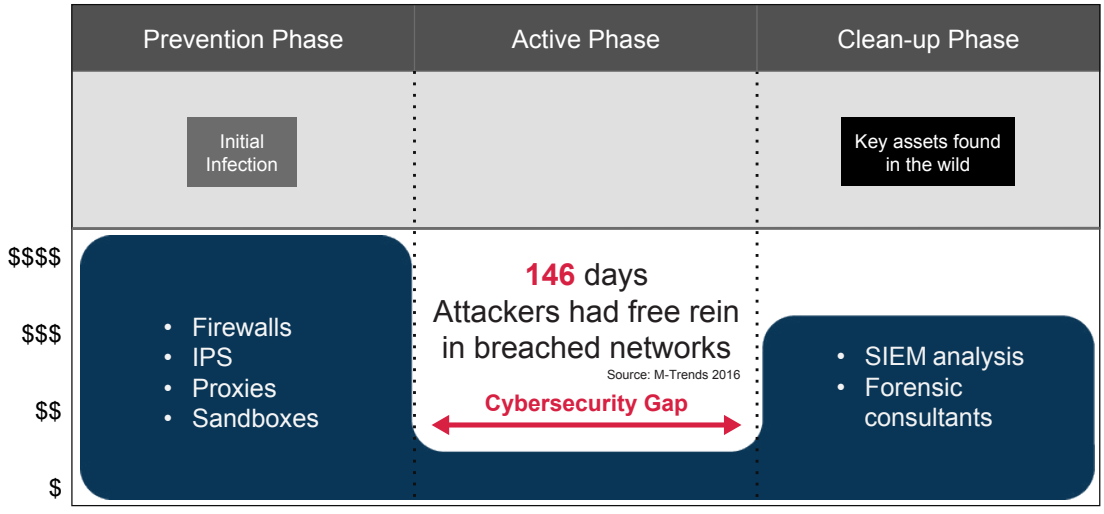

Figure 1: There's a dangerous cybersecurity gap between prevention security at the network perimeter and post-forensic analysis that occurs after an attack.

[1] "Forecast Analysis: Information Security, Worldwide, 2013-2019, 1Q15 Update, 28 April 2015, by Ruggero Contu, Christian Canales, Sid Deshpande and Lawrence Pingree, ID G00277265, © Gartner, Inc.

In the clean-up phase, organizations will invest nearly $2.2 billion on security information and event management (SIEM) tools, and even more on SIEM consultants and staff, according to the same Gartner 2017 forecast.[2] These systems collect logs from security and network devices and confirm known breaches reported by law enforcement or other outsiders.

However, SIEM tools require a significant time investment by highly-sought-after and highly-skilled security analysts to manually research, correlate and prioritize logs in order to find and stop an active attack.

Prevention alone isn't enough

Organizations have focused first and foremost on preventing attacks, but the prevention-only strategy is no longer enough to detect today's highly-sophisticated attacks.

Gartner has been advising clients since 2013 that "Prevention is futile in 2020. Advanced targeted attacks make prevention-centric strategies obsolete."[3]

A prevention-centric approach has one imperfect chance to identify a threat before it sneaks past the perimeter into the network. It has only microseconds to match traffic to a signature of known malware, compare the URL to a reputation list, or observe code in a sandbox. Zero-day threats fly by undetected, ready for their first victim.

In concealment, attackers can operate with impunity on the internal network, with plenty of time to spy (internal reconnaissance) and spread (lateral movement) within the network, and then steal assets (exfiltration) at their convenience.

They change tactics and morph their malware by remote control. They stay silent until the moment is right. Then they communicate covertly using normal network protocols as a mask and hide in everyday applications like webmail.

They also encrypt their communications and use hidden tunnels, making it impractical or even impossible for most organizations to detect and analyze. Attackers are hiding in plain sight – and it's working.

Detecting cyber attacks is a painstaking, manual process

It's impossible to prevent every attack. And that makes it critically important to detect in real time and mitigate active threats that get inside networks. By stopping an attack in progress, it's possible to stop their spread and reduce the risk of data loss.

Gartner advises: "In response to advanced attacks that circumvent or avoid specific protection technologies, CISOs are having to shift the emphasis of their security programs from detection and blocking to detection and response."[4]

But today's trusted tools don't make it easy or efficient for security teams to detect and respond quickly to threats.

Quite the opposite: A security strategy based on prevention drains IT resources. Experienced security analysts and outside consultants may need weeks to properly tune a firewall or IPS so that it is operationally effective. Day-to-day, security teams must manually validate, correlate and prioritize dozens of alerts.

Isolating a newly discovered threat can result in a tedious day of sifting through mountains of data and making sense of logs from security appliances and network devices. It's a job for highly skilled and highly patient analysts.

Such expert analysts are outside the budget reach of most midsized companies, and while large organizations might be able to afford them, there simply aren't enough experienced professionals to fill the open positions.

The cybersecurity skills gap

Based on a survey of CISOs, IT analyst firm ESG found that information security has been the most commonly reported skills shortage for four years. And the SANS Institute found that incident response skills would be in high demand in the next two years as organizations try to mitigate and prevent increasing cyber attacks.

In addition to traditional security roles, data scientists are highly sought-after as security team members. This is due in part to increased reliance on data science for everything from getting more value out of SIEMs to building custom behavioral models to detect insider threats.

In fact, CIO.com recently surveyed more than 500 CIOs and found that data scientists and security staff topped the list of skills shortages.

Not surprisingly, the high demand for these rare skills has made cybersecurity analysts and data scientists some of the most highly paid positions in IT. A recent report from Glassdoor found that the average salary for a data scientist was $118,709 compared to $64,537 for a trained programmer.

The most qualified data scientists demand even higher salaries. An analysis by recruiting firm Burtch Works found that the median salary was $175,000 for top individual-contributor data scientists.

---

[2] "Forecast Analysis: Information Security, Worldwide, 2013-2019, 1Q15 Update, 28 April 2015, by Ruggero Contu, Christian Canales, Sid Deshpande and Lawrence Pingree, ID G00277265, © Gartner, Inc.

[3] "Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence," 30 May 2013, by Neil MacDonald, Gartner, ID G00252476, © 2015 Gartner, Inc.

[4] "Cool Vendors in Security Intelligence, 2015," 24 April 2015, by Ray Wagner, Laurence Orans, Avivah Litan, Lawrence Pingree, Anton Chuvakin, Jeremy D'Hoinne, Craig Lawson, Oliver Rochford, ID G00275655, © 2015 Gartner, Inc.

Of course, salary is just one portion of the fully loaded cost of an employee, which will be much higher. However, this comparison of salaries gives a view into the premium associated with security and data science talent.

Automated threat management – A security analyst in software

Automated threat management helps organizations detect and respond to active threats in real time, closing the cybersecurity gap between prevention and post-forensic clean up.

There are significant innovations in data science, machine learning and behavioral analysis, that, when combined, make it possible to automate real-time threat detection and response.

Automated threat management detects all phases of an active cyber attack, including command and control, internal reconnaissance, lateral movement, data exfiltration, and botnet monetization.

Automation is the only way threat management can scale with the rapid increase and diversity of modern cyber attacks. It's not humanly possible to analyze massive volumes of alerts and logs to find the breadcrumbs of threats that make their way inside networks.

Having automated threat management software working throughout a distributed network is like having a top-shelf security analyst at headquarters and every remote location – except it works around the clock, watches all traffic and never takes a vacation.

Focus on attack behaviors

Advances in behavioral analysis make it possible to detect threats that are known or unknown, encrypted or in the clear, or even when the traffic payload can't be inspected. Attackers adapt their tactics – change malware or create a new domain, for instance – but their malicious behaviors are always observable.

Combining behavioral analysis with machine learning reveals the telltale signs of an attacker's actions across every phase of the kill chain. Using advanced techniques, automated threat management determines if an attacker is communicating covertly through hidden tunnels, hiding communications in everyday applications, using remote access tools to remotely control an attack, or even using encryption or obfuscation techniques.

Analyzing traffic as it crosses the perimeter is not enough. IT needs visibility into all network traffic – across the internal network and in the data center in addition to traffic out to the Internet or cloud and back. Automated threat management identifies attackers who perform internal reconnaissance inside a network, spread malware, escalate privileges, and accumulate data to steal.

It's a game of numbers – the more traffic that's monitored, the greater the chance of detecting an attack in progress. With data science, machine learning and behavioral analysis, automated threat management enables detection and response that scales.

Automated threat management simplifies forensics when an incident occurs because it has the original packets in which the threats were detected. In contrast, SIEMs can miss key pieces of an attack because they rely on information from security products that failed to detect the threat in the first place or might only have analyzed a fraction of overall network traffic.

Real-time detection for real-time organizations

An organization's security controls must keep pace with customers, constituents and business partners. Forward-thinking security teams are moving to real-time, automated threat management to stop active threats in progress – before they cause irreparable damage.

Proactively neutralizing threats and keeping valuable data safe is a whole lot better than getting a call from the FBI to report that your organization's has fallen prey to a cyber attack and your data is for sale on the commercial darknet market.

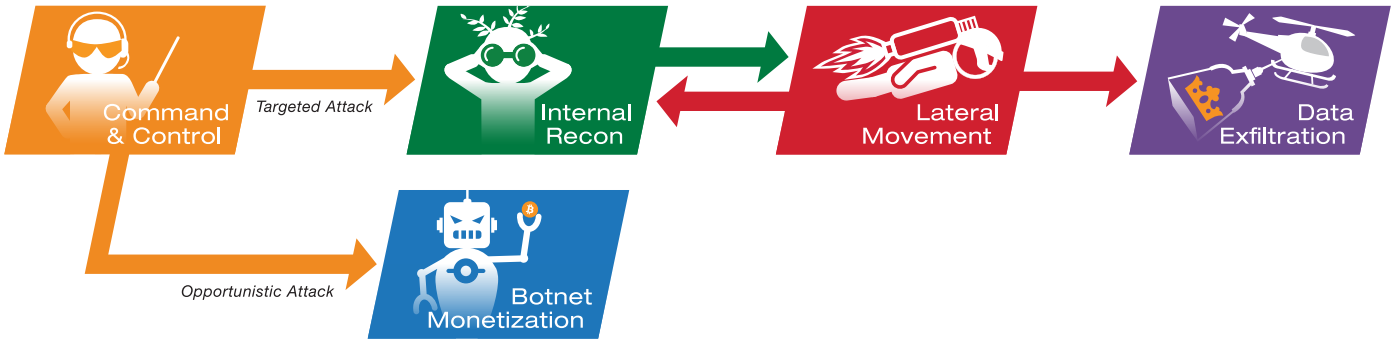

Figure 2: There are multiple phases in an active cyber attack and each is a perilous link in a complex kill chain that gives attackers the opportunity to spy, spread and steal from inside a network.

VECTRA
Security that thinks®

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

Ontrex
Ontrex AG
Haldenstrasse 23
Brüttisellen Zürich Switzerland 8306
+41 44 83510 00
www.ontrex.ch