White paper

Age of the Cyber Hunter

How a New Generation of Threats Changed the Cybersecurity Paradigm

rackspace®

Table of contents

Introduction

The newest generation of cyberthreats, known as advanced persistent threats (APTs), presents significant challenges to the security community and changes how we need to view, implement and manage security operations.

So what are APTs? According to Daniel Clayton, a former British intelligence officer who served as director of security operations at Rackspace, the phrase was coined by Western intelligence agencies in the 1990s. It described attackers capable of breaching data infrastructure through continuous targeting and then remaining within that infrastructure, undetected, to locate and access valuable information. Clayton describes modern APTs as "groups of individuals that have the resources and manpower to persistently target a company or organization 24 hours a day for as long as it takes to get the job done."

Prior to APTs, the cyberthreat landscape was composed almost entirely of automated, nonspecific threats — what Rackspace specialists call the "background radiation" of the internet. Those threats typically rely on a single technique that remains consistent across all platforms (DDoS, virus, Trojan, file-based, etc.). And you can defeat those attacks with universal, perimeter-oriented solutions (web application firewalls, intrusion detection and anti-virus software, etc.).

That remained the state of play until quite recently, and today's cybersecurity compliance standards reflect that earlier landscape — they're designed to protect against elementary threats. But beginning around 2011, more sophisticated, sustained attacks began proliferating globally.[1]

This reality has forced a paradigm shift in cybersecurity strategy. "The ability to persist has made the whole idea of prevention obsolete," Clayton says. Effective security now requires firms to assume penetration and continually scan their environments for malicious activity.

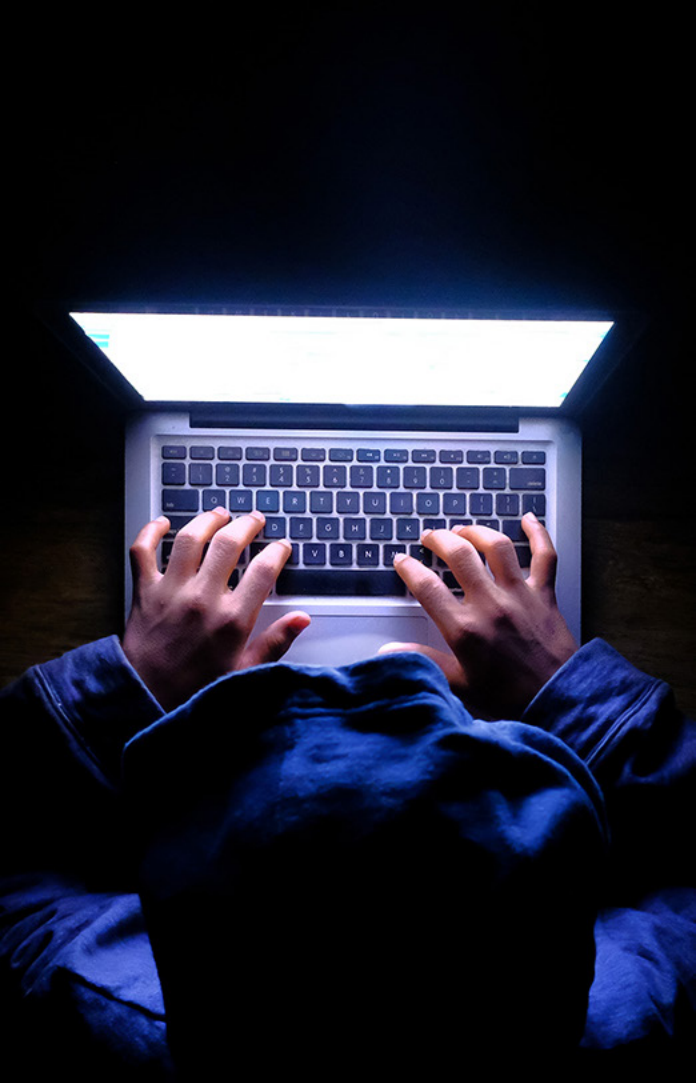
Let's take a closer look at today's APTs, and then we'll explore state-of-the-art techniques and technologies to detect and counteract them.

Understanding the Current Cyberthreat Landscape

Advanced Persistent Threats: Who's Responsible?

Many countries now engage in sophisticated hacking and cyberespionage. A few years ago, former U.S. Secretary of Defense Robert Gates warned that at least 15 countries engage in cyberespionage. The list wasn't limited to longtime adversaries like Iran, Russia and North Korea; it also included several allies. In fact, many national militaries now have cyberespionage divisions. According to Foreign Policy magazine, China's cyber army may comprise as many as 100,000 soldiers, and the country recently acknowledged that it had created specialized cyberwarfare units.

But government militaries aren't the only source of APTs. Multinational organized crime syndicates, many with the tacit backing of national governments, now command vast resources. Examples include Japan's largest criminal syndicate, the Yakuza, and the Russian mafia, which has 10 semi-autonomous "brigades" and a governing council. Several years ago, research suggested that the rapidly maturing, multibillion-dollar cybercrime market might be larger than the global market for illegal drugs.[2]



APT Capabilities and Techniques

Plentiful resources and ever-decreasing computing costs enable cybercriminals and foreign militaries to deploy advanced, non-linear techniques, many of which we've never seen before. APT tactics include fileless malware (in-memory resident attacks), sophisticated social engineering based on government intelligence and zero-day exploits (no known digital signature).

That sophistication is problematic in and of itself, but persistence hugely compounds the problem. The ability to continuously attack a target may be the greatest weapon cybercriminals currently wield, partly because it exploits human fallibility.

"Now you've got an environment where someone is continuously probing your tools, sending phishing attacks, whatever it may be, and sooner or later, in most cases, if not all cases, somebody will click on something they shouldn't, somebody will misconfigure a tool, someone won't change a password or use a weak password," says Clayton. "Sooner or later, they'll find a way in."

But APTs pose problems beyond the inevitability of network penetration. Sophisticated attackers aren't interested in smash-and-grab jobs. Once they break into your environment, they want to stay there, undetected, acquiring maximum knowledge and extracting maximally valuable data. That's why many of the major security breaches of the last few years began with a spear phishing attack against a small set of users. The attackers stole credentials and used them to access an organization, reconnoiter the environment, pivot across the infrastructure, establish persistence and eventually exfiltrate data. By expertly mimicking the behavior of system administrators or users and only deploying native tools, attackers can remain in an environment for months, or even years.

Needless to say, traditional automated security tools at the perimeter won't detect attackers of this caliber.

What Can Be Done? Cyber Hunting and Advanced Remediation

The first step is conceptual: Accept that the most advanced adversaries you face will probably penetrate your network — they're likely inside already. The simple reality is that if a country's leaders believe it's in the national interest to break into your network, they'll find a way in.

When you accept the inevitability of a breach, you can refocus your resources on a more holistic approach that depends on proactive detection and immediate, preauthorized remediation measures.

Modern security providers deploy sophisticated technology and highly skilled analysts to actively patrol environments and locate anomalies. They focus not only on ingress (inbound traffic), but also on egress (outbound traffic) and lateral movement (internal network traffic). This technique is called "cyber hunting," and it can make your adversaries' work more complex, more expensive and more likely to fail.

Cyber Hunting: Proactive Detection of Advanced Cyberthreats

Definition of Cyber Hunting

Cyber hunting involves proactively analyzing all activity occurring in your network environment, and then contrasting it with normal activity to identify anomalies that indicate malicious action. This requires advanced tools that can gather highly detailed data sets — system data, network

infrastructure logs, application logs, raw event data from security tooling, etc. That data is then aggregated and dissected by a security analyst.

It's important to note that this kind of detection cannot be replicated by a tool or machine. Advanced analytics solutions and detection tools are critical, Clayton says, but "ultimately it's an analyst versus a hacker, each sitting in front of a monitor." The experience and discrimination of individual analysts allow them to pick out anomalies that would otherwise be dismissed as legitimate activity.

"What's powerful about threat hunting is that it pits human defenders against human adversaries," says SANS Institute security analyst Robert M. Lee. "The key is to find the right analysts and empower them."

Here are the key elements of a modern cyber hunt.

Intelligence Gathering

Understanding the Attacker Lifecycle

A model of the attacker lifecycle, or kill chain, guides most cyber hunting missions. With few exceptions, cyberattackers must accomplish certain objectives in a certain sequence in order to take control of an environment.

"We're looking for benign impacts of things we know cyberattackers like to do," explains Clayton. Attackers usually reconnoiter the target environment, he says, like burglars casing a house. You might not know whether your house is being cased, but you can keep an eye out for any empty coffee cups or cigarette butts left behind. And once a burglar is inside, he needs time. He knows he might not get everything done in a 7.5-hour shift, so he'll make keys to all the exterior doors. The cybercrime equivalent leaves digital traces.

Understanding the attacker lifecycle helps focus and scope a cyber-hunt mission, because each stage involves distinct activities. The stages are:

1. **Initial reconnaissance:** Determine which businesses to target, which data to target within those businesses, evaluate existing security measures, etc.
2. **Exploitation:** Gain access to the environment via an exploit (spear-phishing attack, vulnerability in a web app server, etc.).
3. **Command and control:** Establish the ability to come and go freely to attain persistence in the environment (e.g., stealing passwords, installing back doors).
4. **Internal reconnaissance:** Locate the crown jewels by moving laterally through systems and mapping the digital geography.
5. **Exfiltration:** Extract valuable data.

Defining Normal Operations

The essential goal of cyber hunting is to detect anomalous activity; but doing so requires a complete, granular understanding of the environment in its healthy, active state. Companies commonly struggle with the process of mapping their own systems, but it's indispensable to cyber-hunting success. A comprehensive profile of your environment should involve an inventory of assets, an assessment of data criticality and a map of normal business-to-business communications.

While you're engaged in this process, look for any inherent vulnerabilities, and determine which digital assets would be most valuable to hackers and cybercriminals. Identify the technologies that make up your "attack surface." Address those vulnerabilities and erect additional safeguards to protect highly valuable data.

rackspace

Studying Your Adversaries

The better you understand your potential adversaries, the more effective the cyber hunting process will be.

Today's cyberattackers are extremely good at concealing themselves, so it's essential to develop an understanding of their objectives, motivations and tools — you want your cyber hunters to know what they're looking for. An experienced, well-equipped analyst armed with good intel should be able to detect an adversary's most subtle techniques.

To understand the kind of intelligence you'll need to collect, consider the following questions:

- Have any of your technologies been targeted? How and why?
- Take a look at the broader cyberthreat landscape — what do cybercriminals typically target in relevant threat verticals? What are their motivations? Which data types are most valuable to them?
- Based on current attack trends, attack vectors and adversary "chatter," which adversaries might attack your network? What are their preferred techniques?
- Identify reconnaissance methods adversaries are likely to use — are you equipped to detect indicators of adversary surveillance?
- How do your likely adversaries create and weaponize their campaigns?
- What are the capabilities of potential attackers? How advanced and targeted are they likely to be? How persistent?
- If you can generate detailed answers to these questions, you'll have a useful intelligence baseline for your cyber-hunting teams.

The Hunt

When you've completed your intelligence gathering, you're ready to hunt — to search the environment server by server and endpoint by endpoint for signs of adversary activity. Cyber hunts occur in two phases: detection and analysis. Intelligence insights inform and guide cyber hunts during both phases.

Detection

Detecting advanced adversaries requires tools that give back telemetry on all activity in an environment. As Travis Mercier, manager of the Rackspace Customer Security Operations Center (CSOC), explains, "You need to conduct a proactive analysis of all the data that's coming and going through an environment, as well as the data that's living inside a system day to day."

Your detection tools need to function at both the network and host levels. At the host level, this means a kernel-level agent, and at the network level, this means both in-line protection — a next-generation firewall (NGFW) — and network-intrusion detection. You'll also need a big data analytics (BDA) solution to correlate data and pick out what security experts call "indicators of compromise" (IOC) and "indicators of attack" (IOA). (For more information on the tools necessary for effective cyber hunting, see Appendix A.)

At the host level, you'll look for operating system behavior changes, including process creation, network activity, registry access, the creation/deletion/renaming of critical files and memory analysis. At the network level, you'll look at both incoming traffic and traffic moving laterally between computers.

Your BDA solution will apply heuristics to network and host data to correlate events and identify changes or deviations from normal patterns.

Analysis

Analysis by a skilled expert is crucial for determining whether an event flagged by analytics as potentially malicious constitutes an actual attack. To make this determination, analysts rely on a deep knowledge of the customer environment, relevant threat intelligence and their own security expertise, notably packet and malware analysis and host and network forensics. (For more information on the expertise cyber hunters should possess, see Appendix B.)

Generic vs. Targeted Hunts

Generic cyber-hunting missions seek out known tactics, techniques and procedures (TTPs) used by multiple adversarial groups, often in multiple industries. These hunts are guided primarily by the stages of the attacker lifecycle. Analysts begin by conducting a broad search aimed at a particular lifecycle stage (initial reconnaissance, exploitation, etc.). They can look for stage-specific identifiers, anomalies within a larger data set or a combination of the two. They must also determine the relevant time window. (Generic missions can be executed on cyclical rotations to ensure 24x7 coverage.)

The hunters then make a series of pivots on data returned, distilling it until an individual analyst can study it line by line. If analysis uncovers anything suspicious, the security team can shift focus laterally across the attacker lifecycle to establish corroborating evidence.

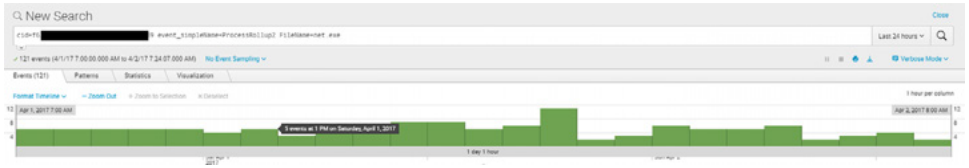
Targeted hunts focus on specific areas and behavioral signatures highlighted by threat intelligence: likely targets (because of perceived value or perceived vulnerability), digital indicators of adversary TTPs, etc. Analysts map potential indicators onto stages of the attacker lifecycle, allowing them to home in on particular data sources likely to reveal IOAs and IOCs, or anything else of relevance given the intelligence matrix.

Cyber Hunting in Practice

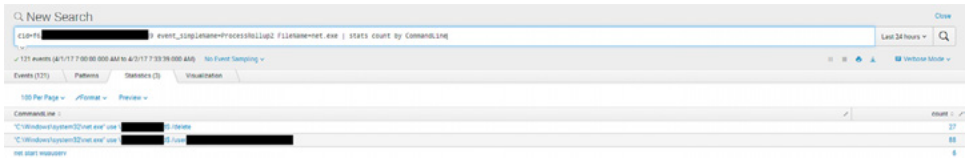
Rackspace senior security analyst Justin Ibarra offers the following examples of cyber hunting, based on his experience overseeing hunt missions at CSOC.

1. Privilege Escalation via Net Command Usage

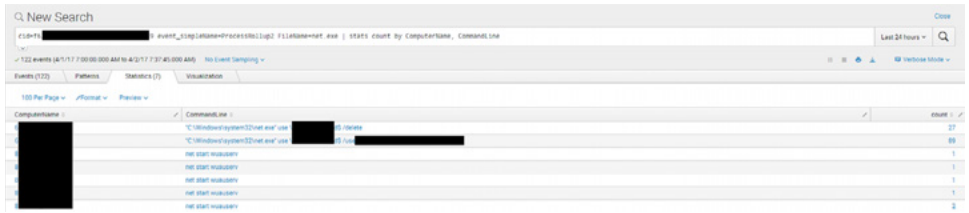
This is a generic cyber-hunting mission focused on potential malicious activity within the exfiltration phase of the attacker lifecycle. We're limiting the search to a single customer, and looking for all process-creation events executing the net command within the previous 24 hours:



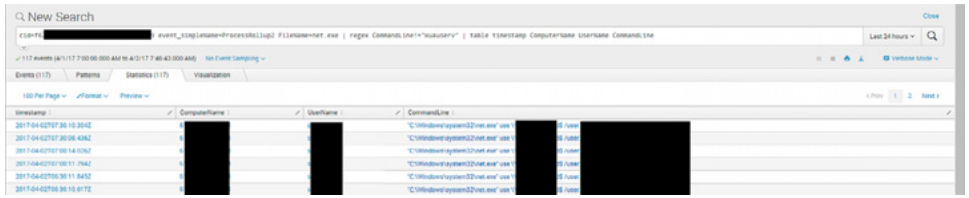
The search has returned 121 results. This is a manageable number of events for an analyst to investigate, but we can cull them further by filtering out normal activity based on established baselines:



Across the customer's entire environment, we can see that the 121 events are comprised of only three unique commands. Breaking this down further by individual system yields additional insight:



Based on previously documented baselines and our map of normal operations, we can determine that the wuauserv activity is expected, and rule it out. (Wuauserv stands for Windows Update AutoUpdate Service.) We can dig further into the net use commands:

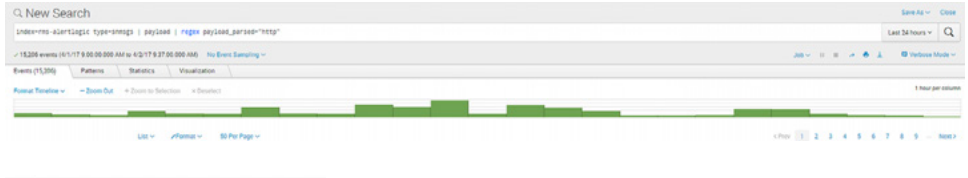


The results (truncated for brevity) reveal activity within specific time frames. We can compare it with the normal, expected activity within the respective systems, either by comparing it to baselines or verifying it with the customer.

If there were any suspicious results we could not legitimize, we would further contextualize the activity — e.g., identifying what the user is executing shortly before and after, discovering which other processes are running, looking into parent-child process relationships. We would then compare the suspicious activity to other data sources to enrich these findings, and shift our focus to other phases of the attacker lifecycle for further corroboration.

2. Exploitation Leveraging a Software Vulnerability (CVE-2017-5638)

Here we'll take a look at how anomalies in a data set can reveal malicious activity. We're searching for event data to identify all unique request and response HTTP headers. We won't restrict our search to a single customer in this case; we want to encompass a larger, more diverse data set:

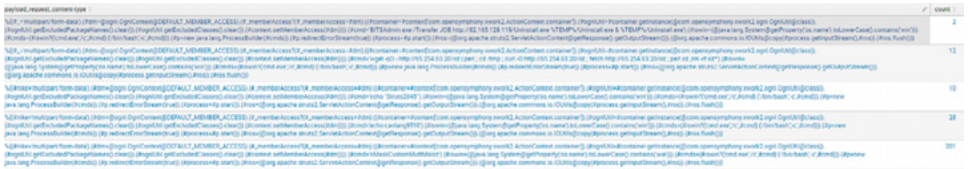


i	✓	Field
>	☑	payload_request_accept
>	☑	payload_request_accept-encoding
>	☑	payload_request_accept-language
>	☑	payload_request_connection
>	☑	payload_request_content-length
>	☑	payload_request_content-type
>	☑	payload_request_cookie
>	☑	payload_request_full_url
>	☑	payload_request_host
>	☑	payload_request_protocol
>	☑	payload_request_resource

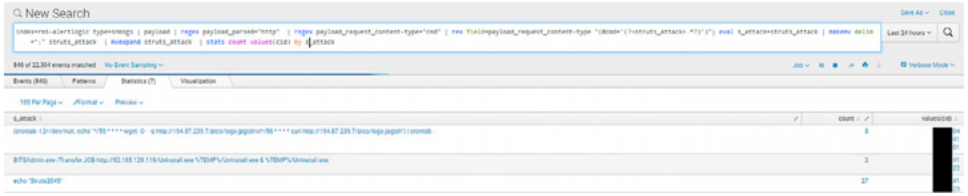
A partial list of results shows that we've captured over 50 unique HTTP headers. We can now look for certain outliers in the respective headers — significantly higher or lower occurrences of a value, for example, or even significant differences in the length of the values themselves.

As we browse through the top values, we notice something interesting in the request packet's content-type header: two entries are far longer than the rest, and one has a very high occurrence rate.

To appreciate how much of an outlier this is, we can examine all unique values. We find some repeating patterns within the value itself, and a review of the RFC reveals that this is anomalous activity. We now know, of course, that this is the attempted exploitation of CVE-2017-56381 targeting Apache Struts, but this process shows how it might have been detected prior to its discovery and disclosure.



We can now pivot on this data to extract all the attempted malicious command-line activity by the targeted customer within the Apache Struts vulnerability, so we're able to search our host-level data for verification that the commands were not successfully executed.



Response and Remediation

Preparation, Expertise and Technology

The Value of Preapproved Action

While early detection of adversary activity is critical, it's equally critical to respond immediately — within hours, ideally. Otherwise, you may squander the valuable temporal advantage gained by your cyber-hunting team.

The remediation effort begins long before an incident occurs. At Rackspace, we start gathering intelligence as soon as we assume responsibility for an environment. We run simulations of all relevant TTPs to understand how attackers might attempt to penetrate, compromise and persist in an environment. We then design countermeasures to neutralize attacks as soon as they occur.

To ensure we can respond immediately, we present our TTP findings and countermeasures to clients as soon as we've completed them, giving them time to study and approve defensive tactics in advance of an attack. When an attack is detected, our security teams can log straight into the compromised environment and respond, taking time away from the adversary, interrupting reconnaissance, and preventing a pivot to exfiltration and other damaging activities.

Response-Specific Expertise and Technology

It's important to understand that remediation skill sets are distinct from cyber-hunting skill sets. Cyber hunters develop hypotheses about the methods and targets of potential attackers, and then locate evidence of malicious activity; but they don't necessarily have expertise in blocking attacks and removing adversaries. You may or may not want your cyber hunters to assume responsibility for incident response; you should make the decision based on their level of training and expertise. For example, incident response specialists will have experience in containment and forensic data gathering. Cyber hunters may or may not have those skills.

You'll also want to make sure your responders have the latest technology. Automated remediation platforms can help remove adversaries rapidly and accurately, and they're capable of engaging in multiple corrective actions at the same time. For example, automated solutions can simultaneously deny a connection, disable a process related to that connection and destroy the file executing the process. That ability is particularly valuable during large-scale attacks, when the response effort may need to scale rapidly to neutralize malicious activity in diverse parts of an environment.

Keys to Adversary Removal

Degrading Operational Capacity

At Rackspace, we concur with cybersecurity experts at Endgame, who identify three capabilities adversaries must possess in order to remain operational in your environment:

- **Execution.** To control an asset and exfiltrate data over time, an attacker must have the ability to execute malicious code or commandeer tools already installed on the infected assets.
- **Command and control.** Attackers rely on automatic command-and-control communication between the compromised asset and remote systems. That line of communication might run through multiple compromised components.
- **Access.** To persist in a targeted system, adversaries need to maintain access, even if the vulnerabilities used to gain initial entry have since been patched. Common methods for preserving access include using stolen credentials and installing back doors.

As Endgame points out, successful remediation requires degrading each of these capabilities in a carefully coordinated manner. That may include the forensic removal of malicious files (to be turned over to malware reverse engineers), denial of illicit access, and suspension of malicious threads or processes. Remediation should always counteract persistence: identifying and dismantling back doors, imposing password changes to prevent continued use of compromised credentials, etc.

Avoiding Disruption

Incident response teams often have to stop attacks and remove adversaries without interrupting business operations. Interruptions can be extremely costly in terms of bottom-line dollars, customer satisfaction or brand reputation — or all three.

Sophisticated adversaries, however, conduct reconnaissance to identify critical business assets, and critical services and data within those assets. They can hide in memory to maximize disruption in the event of discovery.

To protect operational continuity, security teams need to design responses that only affect the compromised assets. Consider this hypothetical from Endgame: An adversary is executing a malicious thread inside an essential system process, and you want to avoid killing the process, which would bring down the entire system. Focus instead on stopping the thread itself. Depending on the nature of the attack, it might be necessary to take broad-spectrum measures like denying network access to a compromised component or taking it offline, but the more precise your response, the less disruptive it will be.

Security Operations Centers: The Future of Cybersecurity

SOCs: The Best Defense Against Advanced Threats

Now that we've explored the cyberthreat landscape and effective responses to advanced attacks, you might be wondering about the investment required to establish state-of-the-art cyberdefenses.

When your organization is subject to attacks by sophisticated cybercriminals 24x7x365, the best response is a trained and motivated defense force working out of a security operations center (SOC). This is particularly true for large enterprise environments requiring extensive monitoring and response capabilities. You can then augment your SOC security staff with teams focused on critical areas like defensive infrastructure, vulnerability management and compliance.

This is clearly the best defense against today's cyberthreats — enterprise SOC use is predicted to grow from 10 percent in 2015 to 40 percent in 2020[3] — but standing up an SOC is not a trivial task. Organizations need to carefully analyze risks and benefits before finalizing a security budget. Many face a difficult dilemma: They must defend against the most sophisticated adversaries without the resources required to build a top-tier SOC. They fall below what has been termed the "security poverty line."

Requisite SOC Costs and Expertise

Taking into account the people and tooling needed in all parts of the business, it's common to spend $3 million to $5 million for a modern security operation — much of which is a recurring annual expense.[4]

Enterprises capable of funding their own SOCs face another hurdle: a lack of qualified security analysts. At Rackspace, we estimate that a fully staffed, 24x7x365 SOC requires at least 17 security specialists at various ability levels. (For more on SOC staffing requirements and challenges, including a breakdown of necessary experience and expertise, see Appendix B.) With as many as 209,000 cybersecurity jobs unfilled,[5] we find that many of our customers struggle to staff their SOCs to even a fraction of this level.

Our customers also struggle to find good security leadership. The average tenure of a chief security officer is down to 18 months,[6] so even if organizations are willing to invest in building a security operation, they're finding it nearly impossible to retain someone for the duration of the project.

A lack of staffing can have a pernicious effect. Cyber hunting and advanced remediation are essential to effective cybersecurity, but understaffed SOCs end up spending much of their time on elementary "block-and-tackle" measures (vulnerability management, patching, etc.).

The Value of Managed Security Solutions

There is a way to avoid these obstacles and control costs while meeting highly ambitious security goals. Outsourcing cybersecurity to a managed security services provider is often more effective and cost-efficient than a DIY solution. Providers tend to have deeper security expertise and deploy more advanced technologies.

We built our CSOC to help you solve the toughest cybersecurity challenges out there, and Rackspace Managed Security can help you think through key cybersecurity issues for your business, both technical and financial.

Our CSOC offers best-of-breed security solutions and employs industry-leading experts to protect your environment 24x7x365. Our analysts can help with strategic planning for best-practice multi-cloud security, tactical day-to-day security monitoring, and threat analysis to deter, detect and respond to potential threats.

Plainly stated, we have the resources and expertise to handle both "background radiation" and sophisticated, well-resourced APTs. And we can do so at an investment level that makes sense for most businesses.

To learn more, visit rackspace.com/en-us/security, or call us any time at 1-844-768-0280.

Appendix A: Requisite Technology for a Security Operations Center

Here are the technology tools your SOC will need to effectively defend against advanced cyberthreats.

Host-based detection tools

We recommend a kernel-level agent residing on each host. User-level agents will not be effective, as attackers can see services running on the host and disable them quite easily without detection.

The kernel-level agent provides telemetry back to the SOC, giving visibility into host behavior. At a minimum, the kernel-level agent should monitor:

- Host process creation
- Host network activity
- Host process/thread behavior (registry access, file access, file creation/modification, directory access)
- Host memory analysis (i.e., stack, heap)
- Host behavior correlation

Other features to look for are application whitelisting and blacklisting. Application whitelisting should be enabled in a detection-mode state, as this feature tends to generate many false positives. It's a best practice to have an SOC analyst investigate further to determine whether an indicator of attack or compromise is present.

Future endpoint technology should be able to model the ideal state of the host on which it is deployed and create an alert when behavior departs from that ideal state. For example, a Windows Active Directory domain-joined host exhibits certain behavior upon startup, logon, logoff and normal operation in terms of network connections, services started, event log entries and files accessed. This can be "learned" by the kernel-level agent, and alerts can be generated when certain behavior falls out of line with normal operation.

Network-based detection tools

At the network level, it's important to have both in-line protection and network intrusion detection/monitoring via a switch SPAN port or network tap, if possible. In public cloud environments, you may not have access to SPAN ports or network taps. In that case, in-line protection is essential. The in-line protection technology is known as a next-generation firewall (NGFW). The feature set for an NGFW, at a minimum, should include:

- Application visibility and control
- User visibility and control, integration with IAM
- IPS
- APT prevention
- Anti-malware
- Passive DNS
- Data filtering
- Policy control
- PFS-SSL offloading/decryption/inspection
- Exploit protection
- SaaS enforcement
- Logging and reporting
- VPN
- IPv6 support
- Next-gen networking support (i.e., NSX)

Whereas prior generation firewalls typically inspected Layer 3/4 traffic, the next generation firewall will also be responsible for Layer 7 (application layer) inspection of north-south (ingress-egress) network traffic, as well as east-west traffic (between Layer 3 VLANs).

The NGFW provides network information that can aid the analyst looking for changes in network traffic to correlate with the host detection discussed in the prior paragraph.

Network intrusion detection systems try to identify malicious actions like denial of service attacks, port scans and attempts to break into computers by monitoring network traffic. Network intrusion detection technology should have the following features:

- Ability to capture packets from the network interfaces
- An event engine to capture the packets and combine them into events that explain the performed actions
- A policy script interpreter to take action in case of suspicious or dangerous actions or to discard events not defined in the policy scripts
- Ability to run in high-speed (>10 Gbps) environments and capture without dropping packets or slowing down the traffic
- Next-gen (contextual) signature detection
- Pre-written policy scripts that can be used out of the box to detect the most well-known attacks
- Ability to customize policy scripts specific to your environment
- Ability to model network behavior to detect changes to known network traffic

If a network intrusion detection system can be deployed (it can be challenging to implement these features in the public cloud), it serves as an additional data point for SOC analysts.

Analytics tools

Finally, you'll need an analytics engine to correlate information from the host and network-level tools. This is known as security information and event monitoring (SIEM).

SOC response time after an attack often determines whether an attempted data exfiltration is successful. When correctly configured and monitored, SIEM software can play a significant role in identifying breaches in progress. SIEM requirements should be discussed and agreed upon before deployment, and the software should be correctly sized for the environment.

Companies often overspend on their SIEM implementation, because they fail to fully understand which problems they need to solve. At a minimum, a SIEM should be able to do the following:

- Integrate traditional log sources with other event sources (i.e., host-detection and network detection tools, NGFW)
- Include capabilities to support a security operations center
- Scale to large implementations
- Import and export content (rules, reports, trends)
- Include multi-value lists (active lists, watch lists) with expiration times on lists (expire after x number of minutes/hours) and event on expiration for state table usage
- Create custom log source feeds
- Aggregate and filter at the collector level (with selectable fields and summarization of fields)
- Reuse and move objects
- Summarize tables
- Provide health status monitoring
- Provide redundancy
- Scale at the correlation-engine level
- Integrate with a ticketing/workflow system
- Integrate with an existing configuration management database to pull asset tag information

Cloud-based SIEM-as-a-Service is gaining in popularity, but be aware that log data may contain personally identifiable information (PII) or protected health information (PHI). For example, the SIEM could alert on a file transfer and collect the data from the transfer in a log file. That log file could contain a social security number or a patient's private data. A separate privacy agreement with the cloud provider may be needed to ensure the data is handled appropriately.

Appendix B: Requisite Expertise for a Security Operations Center

The most valuable asset of any SOC is its people — the human analysts who detect and respond to threats. An SOC should have three levels of analysts, from level 1 to level 3. This classification is useful for hiring purposes and also provides the analysts with achievable goals. A fully staffed 24x7x365 SOC requires, at a minimum, 17 staff members — four level 3, four level 2 and eight level 1, plus a manager.

Every analyst should possess the following baseline skills:

- Understanding of continuous security monitoring and the cyber kill chain
- TCP/IP and common application layer protocols
- Packet analysis (i.e., tcpdump, Wireshark)
- Understanding of Windows, Linux and Mac architectures
- Data parsing skills (i.e., bash, grep, sed, awk, etc.)
- Familiarity with both basic IDS (Snort, Suricata) and next-gen IDS (Bro)
- SIEM analysis
- Indicators of attack and indicators of compromise
- Threat intelligence gathering
- Malware analysis
- Programming skills (C/C++, Perl, Python, PHP, Java)
- Host-based forensics
- Offensive and defensive tactics

Qualifications for the three analyst levels are as follows:

- **Level 1.** Analysts typically review IDS and SIEM alerts and logs, and perform analysis based on their findings. Their objective is to gain expertise — the more protocols, packets and events they view, the better. Most SOC analysts will be at this level.

- **Level 2.** Analysts specialize in one of the baseline skills. They spend time outside of normal event review and investigation refining their expertise. They will mentor junior analysts and improve the SOC's detection and response capabilities. Over time, they will begin creating signatures based on network events and malware analysis, and research the tactics, techniques and procedures of potential adversaries. They will also develop the skills needed to manually analyze data sources for indicators of attack and compromise.
- **Level 3.** These analysts have skills in all of the above areas, with at least two specialties. They are the SOC's thought leaders. Instead of reviewing events, they mentor other analysts, develop and provide training, and lead efforts involving more complex forensic investigations.

  They are also responsible for evaluating SOC tools and conceptualizing and developing new tools. They may serve as a liaison to personnel who manage the perimeter-centric tools to ensure that the SOC is receiving intelligence from those tools.

Professional Culture

Every SOC should promote a culture of learning. SOCs thrive on ingenuity and innovation, which are the products of motivation and education. SOC management should encourage and facilitate continuing education. Team building is also essential, and will require a commitment from every analyst. Analysts who trust one another and genuinely enjoy spending time together will be far more effective in detecting and responding to threats. And team cohesion helps promote a culture of learning.

Notes

1. Symantec, "Internet Security Threat Report: 2011 Trends," April 2012, https://its.ny.gov/sites/default/files/documents/Symantec-Internet-Threat-Report-Trends-for-2011-APR2012.pdf
2. RAND Corporation, "Markets for Cybercrime Tools and Stolen Data," March 2014, http://www.rand.org/pubs/research_reports/RR610.html
3. Gartner, "The Five Characteristics of an Intelligence-Driven Security Operations Center," Nov. 2015, https://www.ciosummits.com/Online_Assets_Intel_Security_Gartner.pdf
4. Rackspace Blog, "The Evolving IT Security Threat — A Primer," Sept. 2016, https://blog.rackspace.com/evolving-security-threat-primer
5. Stanford University Journalism Project, "Demand to Fill Cybersecurity Jobs Booming," March 2015, http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth
6. Rackspace Blog, "The Evolving IT Security Threat — A Primer," Sept. 2016, https://blog.rackspace.com/evolving-security-threat-primer

rackspace®

About Rackspace

At Rackspace, we accelerate the value of the cloud during every phase of digital transformation. By managing apps, data, security and multiple clouds, we are the best choice to help customers get to the cloud, innovate with new technologies and maximize their IT investments. As a recognized Gartner Magic Quadrant leader, we are uniquely positioned to close the gap between the complex reality of today and the promise of tomorrow. Passionate about customer success, we provide unbiased expertise, based on proven results, across all the leading technologies. And across every interaction worldwide, we deliver Fanatical Experience™. Rackspace has been honored by Fortune, Forbes, Glassdoor and others as one of the best places to work.

Learn more at www.rackspace.com or call 1-800-961-2888.

Rackspace-White-Paper-Age-of-the-Cyber-Hunter-SEC-14961 :: May 9, 2019