Tasks

**TASK 1**

**Kevin Mitnick**

A seminal figure in American hacking, [Kevin Mitnick got his start as a teen](http://www.cnn.com/SPECIALS/1999/mitnick.background/). In 1981, he was charged with stealing computer manuals from Pacific Bell. In 1982, he hacked the North American Defense Command (NORAD), an achievement that inspired the 1983 film [*War Games*](https://www.imdb.com/title/tt0086567/?ref_=nv_sr_srsg_0). In 1989, he hacked Digital Equipment Corporation's (DEC) network and made copies of their software. Because DEC was a leading computer manufacturer at the time, this act put Mitnick on the map. He was later arrested, convicted and sent to prison. During his conditional release, he hacked Pacific Bell's voicemail systems. Throughout his hacking career, Mitnick never exploited the access and data he obtained. Although Mitnick ultimately went white hat, he may be part of the both-hats grey area.

**Anonymous**

Anonymous got its start in 2003 on [4chan message boards](https://en.wikipedia.org/wiki/4chan) in an unnamed forum. The group exhibits little organization and is loosely focused on the concept of social justice. For example, in 2008 the group took issue with the Church of Scientology and begin disabling their websites, thus negatively impacting their search rankings in Google and overwhelming its fax machines with all-black images. In March 2008, a group of "Anons" marched passed Scientology centers around the world wearing the now-famous Guy Fawkes mask. As noted by [The New Yorker](http://www.newyorker.com/magazine/2014/09/08/masked-avengers), while the FBI and other law enforcement agencies have tracked down some of the group's more prolific members, the lack of any real hierarchy makes it almost impossible to identify or eliminate Anonymous as a whole.

**Adrian Lamo**

In 2001, 20-year-old Adrian Lamo used an unprotected content management tool at Yahoo to modify a Reuters article and add a fake quote attributed to former Attorney General John Ashcroft. Lamo often hacked systems and then notified both the press and his victims. In some cases, he'd help clean up the mess to improve their security. As [Wired](http://www.wired.com/2010/05/lamo/) points out, however, Lamo took things too far in 2002, when he hacked The New York Times' intranet, added himself to the list of expert sources and began conducting research on high-profile public figures. Lamo earned the moniker "The Homeless Hacker" because he preferred to wander the streets with little more than a backpack and often had no fixed address.

**Albert Gonzalez**

According to the [New York Daily News](http://www.nydailynews.com/news/world/soupnazi-hacker-albert-gonzalez-nerdy-life-sex-guns-drugs-article-1.394977), Gonzalez, dubbed "soupnazi," got his start as the "troubled pack leader of computer nerds" at his Miami high school. He eventually became active on criminal commerce site Shadowcrew.com and was considered one of its best hackers and moderators. At 22, Gonzalez was arrested in New York for debit card fraud related to stealing data from millions of card accounts. To avoid jail time, he became an informant for the Secret Service, ultimately helping indict dozens of Shadowcrew members.

During his time as a paid informant, Gonzalez continued his in criminal activities. Along with a group of accomplices, Gonzalez stole more than 180 million payment card accounts from companies including OfficeMax, Dave and Buster's and Boston Market. [The New York Times Magazine](http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html) notes that Gonzalez's 2005 attack on US retailer TJX was the first serial data breach of credit information. Using a basic SQL injection, this famous hacker and his team created back doors in several corporate networks, stealing an estimated $256 million from TJX alone. During his sentencing in 2015, the federal prosecutor called Gonzalez's human victimization "unparalleled."

**Matthew Bevan and Richard Pryce**

Matthew Bevan and Richard Pryce are a team of British hackers who hacked into multiple military networks in 1996, including Griffiss Air Force Base, the Defense Information System Agency and the Korean Atomic Research Institute (KARI). Bevan (Kuji) and Pryce (Datastream Cowboy) have been accused of nearly starting a third world war after they dumped KARI research onto American military systems. Bevan claims he was looking to prove a UFO conspiracy theory, and according to the [BBC](http://news.bbc.co.uk/2/hi/technology/4761985.stm), his case bears resemblance to that of Gary McKinnon. Malicious intent or not, Bevan and Pryce demonstrated that even military networks are vulnerable.

**Jeanson James Ancheta**

Jeanson James Ancheta had no interest in hacking systems for credit card data or crashing networks to deliver social justice. Instead, Ancheta was curious about the use of bots—software-based robots that can infect and ultimately control computer systems. Using a series of large-scale "[botnets](https://usa.kaspersky.com/resource-center/threats/botnet-attacks)," he was able to compromise more than 400,000 computers in 2005. According to [Ars Technica](http://arstechnica.com/uncategorized/2006/05/6789-2/), he then rented these machines out to advertising companies and was also paid to directly install bots or [adware](https://usa.kaspersky.com/resource-center/threats/adware-pornware-riskware) on specific systems. Ancheta was sentenced to 57 months in prison. This was the first time a hacker was sent to jail for the use of botnet technology.

**Michael Calce**

In February 2000, 15-year-old Michael Calce, also known as "Mafiaboy," discovered how to take over networks of university computers. He used their combined resources to disrupt the number-one search engine at the time: Yahoo. Within one week, he'd also brought down Dell, eBay, CNN and Amazon using a [distributed-denial-of-service (DDoS)](https://usa.kaspersky.com/resource-center/threats/ddos-attacks) attack that overwhelmed corporate servers and caused their websites to crash. Calce's wake-up call was perhaps the most jarring for cyber crime investors and internet proponents. If the biggest websites in the world—valued at over $1 billion—could be so easily sidelined, was any online data truly safe? It's not an exaggeration to say that the development of cyber crime legislation suddenly became a top government priority thanks to Calce's hack.

**Kevin Poulsen**

In 1983, a 17-year-old Poulsen, using the alias Dark Dante, hacked into ARPANET, the Pentagon’s computer network. Although he was quickly caught, the government decided not to prosecute Poulsen, who was a minor at the time. Instead, he was let off with a warning.

Poulsen didn’t heed this warning and continued hacking. In 1988, Poulsen hacked a federal computer and dug into files pertaining to the deposed president of the Philippines, Ferdinand Marcos. When discovered by authorities, Poulsen went underground. While he was on the run, Poulsen kept busy, hacking government files and revealing secrets. According to his [own website](https://www.kingpin.cc/about/), in 1990, he hacked a radio station contest and ensured that he was the 102nd caller, winning a brand new Porsche, a vacation, and $20,000.

Poulsen was soon arrested and barred from using a computer for three years. He has since converted to white hat hacking and journalism, writing about cyber security and web-related socio-political causes for [Wired](https://www.wired.com/author/kevin-poulsen/), The Daily Beast and his own blog Threat Level. Paulson also teamed with other leading hackers to work on various projects dedicated to social justice and freedom of information. Perhaps most notably, working with Adam Swartz and Jim Dolan to develop the open-source software SecureDrop, initially known as DeadDrop. Eventually, Poulsen turned over the platform, which enabled secure communication between journalists and sources, to the Freedom of Press Foundation.

**Jonathan James**

Using the alias cOmrade, Jonathan James hacked several companies. According to the [New York Times](http://www.nytimes.com/2000/09/23/us/youth-sentenced-in-government-hacking-case.html), what really earned James attention was his hack into the computers of the United States Department of Defense. Even more impressive was the fact that James was only 15 at the time. In [an interview with PC Mag](http://www.pcmag.com/article2/0,2817,2164176,00.asp), James admitted that he was partly inspired by the book *The Cuckoo’s Egg*, which details the hunt for a computer hacker in the 1980s. His hacking allowed him to access over 3,000 messages from government employees, usernames, passwords and other sensitive data.

James was arrested in 2000 and was sentenced to a six months house arrest and banned from recreational computer use. However, a probation violation caused him to serve six months in jail. Jonathan James became the youngest person to be convicted of violating cyber crime laws. In 2007, TJX, a department store, was hacked and many customer’s private information were compromised. Despite a lack of evidence, authorities suspect that James may have been involved.

In 2008, James committed suicide by gunshot. According to the [Daily Mail](http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html), his [suicide note](http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html) stated, “I have no faith in the 'justice' system. Perhaps my actions today, and this letter, will send a stronger message to the public. Either way, I have lost control over this situation, and this is my only way to regain control.”

**ASTRA**

This hacker differs from the others on this list in that he has never been publicly identified. However, according to [the Daily Mail](http://www.dailymail.co.uk/news/article-2262831/Revealed-Aaron-Swartz-prosecutor-drove-hacker-suicide-2008-named-cyber-crime-case.html), some information has been released about ASTRA. Namely that he was apprehended by authorities in 2008, and at that time he was identified as a 58-year-old Greek mathematician. Reportedly, he had been hacking into the Dassault Group, for almost half a decade. During that time, he stole cutting edge weapons technology software and data which he then sold to 250 individuals around the world. His hacking cost the Dassault Group $360 million in damages. No one knows why his complete identity has never been revealed, but the word 'ASTRA' is a Sanskrit word for 'weapon'.

**TASK 4**

Information Leakage

**Description:**The web application may reveal system data or debugging information by raising exceptions or generating error messages. Leakage of system data or debugging information through an output stream or logging function can allow attackers to gain knowledge about the application and craft specialized attacks on the it.

### Frame Injection

**Description:** Improper validation of input parameters could lead to attackers injecting frames to compromise confidential user information. Frame injection is a common method employed in [phishing](https://www.upguard.com/blog/phishing) attacks

### URL Redirection

**Description:**While it's common for web applications to redirect or forward users to other websites/pages, attackers commonly [exploit](https://www.upguard.com/blog/exploit) vulnerable applications without proper redirect validation in place. This can lead to malicious redirection to an untrusted page.

### Missing Session Timeout

**Description:** Attackers may gain unauthorized access to web applications if inactivity timeouts are not configured correctly.

### Session ID Cookies Not Marked Secure

**Description:** If session ID cookies for a web application are marked as secure, the browser will not transmit them over an unencrypted HTTP request. Not marking them as such allows cookies to be accessible and viewable in by attackers in clear text.

### Sensitive Information Cached

**Description:** Browsers typically store a copy of requested items in their caches: web pages, images, and more. This creates a security gap for applications that store, process, and display sensitive data, since attackers gaining access to the user's browser cache have access to any information contained therein.

### CRLF (Carriage Return and Line Feed) Injection

**Description:** CRLF exploits occur when malicious content is inserted into the browser's HTTP response headers after an unsuspecting user clicks on a malicious link. Hackers will typically inject malicious code into the user's browser through the web application/server, making casual detection difficult.

**TASK 5**

1. **Dos/DDoS -**

Denial of Service where an attacker attacks by sending numerous service request packets overwhelming the servicing capability of the web server, resulting in crashing and unavailability for the users.

1. **DNS Server Hijacking -**

DNS Server Hijacking, is also known as DNS redirection, where an attacker modifies DNS configurations. DNS redirection's primary use is pharming, where attackers display unwanted ads to generate some revenue, and Phishing--where attackers show fake websites to steal credentials.

1. **DNS Amplification Attack -**

A DNS Amplification Attack happens when an attacker spoofs the lookup request to the DNS Server with the DNS recursive method. The size of the requests results in a Denial of Service attack.

1. **Directory Traversal Attacks -**

Directory traversal, also is known as Path Traversal, is an HTTP attack that allows attackers to access restricted directories and reveal sensitive information about the system using dot and slash sequences.

1. **Man in the Middle Attack -**

A Man in the Middle / Sniffing attack happens when an attacker positions himself between a user and the application to sniff the packets. The attacker's goal is to steal sensitive information such as login credentials, credit card details, etc.

1. **Phishing Attacks -**

A Phishing attack is a social engineering attack to obtain sensitive, confidential information such as usernames, passwords, credit card numbers, etc. It is a practice of fraudulent attempts that appear to come from a reputable source. Scammers mostly use emails and text messages to trick you in a phishing attack.

1. **Website Defacement -**

Website Defacement is an attack where an attacker changes the website/web page's visual appearance with their messages. SQL injection attack is mainly used in web defacement. An attacker can add SQL strings to craft a query maliciously and exploit the webserver.

1. **Web Server Misconfiguration -**

Web Server Misconfiguration is when unnecessary services are enabled, and default configurations are being used. The attacker may identify weaknesses in terms of remote functions or default certifications, and can exploit them. An attacker can easily compromise systems by some attacks such as SQL Injection, Command Injection.

1. **HTTP Response Splitting Attacks -**

HTTP Response Splitting is a straightforward attack when the attacker sends a splitting request to the server, which results in the splitting of a response into two responses by the server. The second response is in the hand of the attacker and is easily redirected to the malicious website.

1. **SSH Brute Force Attacks -**

Brute force is where an attacker uses trial and error to guess login info by submitting many passwords or paraphrases. In an SSH Brute force attack, the intruder brute forces the SSH tunnel to use an encrypted tunnel. The encrypted tunnel is for communicating between the hosts. Hence, the attacker gains unauthorized access to the tunnel.

**TASK 6**

IT security experts use the CIS Critical Security Controls Version 7 to establish digital security protections within organizations. With these defenses firmly in place, organizations can flush out most of the typical cyberattacks.

Here are the seven fundamental principles that serve as the bedrock of the framework.

1. The CIS Critical Security Controls Version 7 must address current attacks, emerging technology, and changing business requirements for IT.

As part of its core promise, the CIS Controls continually update and re-structure to reflect the presence of new cybersecurity tools and new threats as they happen.

1. There has to be more focus on authentication, application whitelisting, and encryptions.

The guidance for these essential topics is more precise, robust, and consistent across all CIS Controls.

1. The CIS Controls now have better alignment with other frameworks such as the [NIST Cybersecurity Framework](https://blog.rsisecurity.com/why-you-should-adopt-the-cybersecurity-nist-framework/). With more emphasis on multi-framework functionality, it offers better dynamics to companies.
2. Improvement of the wording of each sub-control has been prioritized. Each sub-control only has one “ask,” and the consistency of the syntax has been simplified.

The expert community worked tirelessly to clarify the intention of each CIS Control to be more user-friendly. Multiple tasks have been eliminated so that they can be measured, monitored, and implemented more efficiently.

1. A rapidly growing ecosystem of devices, products, and services from both CIS and the marketplace now has a better foundation set in place. The documentation is better since Version 6 made an effort to improve importing, tracking, and integrating the CIS Controls.
2. The layout and format have been bolstered with structural changes. And flexibility is prioritized so that various organizations can help keep the Controls adaptive and relevant to their industries.
3. With growth encouraged, there is now a system in place that will reflect the feedback of a global community of supporters, volunteers, and adopters. The CIS Security Controls Version 7 believes it is only as strong as the support that sustains it. The hope is to provide more guidance and resources for the entire cybersecurity community.

The CIS Controls V7 are now separated into three particular categories listed below:

* Basic (CIS Controls 1-6): All organizations must follow the key controls for essential protection against cyber threats.
* Foundational (CIS Controls 7-16): Companies must adhere to these best practices to have further security protection.
* Organizational (CIS Controls 17-20): These have more technical elements to boost a more robust cybersecurity system in place.

**Basic Controls**

* **CIS Control 1: Inventory and Control of Hardware Assets**

 All hardware devices within the network must undergo active management. This encompasses inventory, tracking, and correction. All devices must be authorized to screen unmanaged devices from gaining access to the network.

* **CIS Control 2: Inventory and Control of Software Assets**

 All software within the network must undergo active management. Companies must adhere to this basic control, including the proper inventory, tracking, and correction of authorized software, in order to avoid installing and executing unmanaged software.

* **CIS Control 3: Continuous Vulnerability Management**

 New information must be continuously acquired, assessed, and taken action so that vulnerabilities are identified and remediated. The objective is to minimize the window of opportunity for cyber attackers.

* **CIS Control 4: Controlled Use of Administrative Privileges**

 There must be proper supervision of the tools and processes used for the active management of hardware and software. Administrative privileges on networks, computers, and applications must be adequately managed.

* **CIS Control 5: Secure Configuration for Hardware/Software on Mobile Devices, Laptops, Workstations, Servers**

 The security configuration of servers, workstations, mobile devices, and laptops must be implemented and established using a rigorous configuration management and change control process. The active management of this security will prevent attackers from tampering and exploiting vulnerabilities.

* **CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs**

 Audit logs of events are essential to monitor, understand, troubleshoot, and detect attacks. There must be a system in place for its collection, management, and analysis.

**Foundational Controls**

* **CIS Control 7: Email and Web Browser Protections**

 The window of opportunity of cyber attackers using email systems and web browsers must be minimized so that human behavior cannot be manipulated easily.

 One of the popular types of cyberattacks is phishing, a fraudulent attack wherein cybercriminals try to acquire critical and sensitive data such as usernames and passwords through spam emails or text messages. The modus operandi uses a disguise as a trustworthy organization such as a bank or a government agency to scam employees into providing necessary information.

* **CIS Control 8: Malware Defenses**

 Malicious code can spread and execute if there is no existing installation control at multiple points in the organization’s digital environment. The company can optimize automation to help with the rapid updating of cyber defense, data gathering, and corrective action.

* **CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services**

 The operational use of ports, protocols, and services on networked devices must be managed actively using tracking, control, and correction protocols. This minimizes the available vulnerabilities that can be exploited by cyber attackers.

* **CIS Control 10: Data Recovery Capabilities**

 Data recovery is essential for the overall security of an organization. There must be a proven methodology for the timely recovery of data using processes and tools to back up vital information. Without a system in place for data recovery, the long-term operations of a company can severely suffer. When crucial data is gone forever, it can have damaging implications to a company’s reputation and output.

* **CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches.**

 Organizations must enforce a rigorous configuration management and change control process of network infrastructure devices. When actively managed, this security configuration can prevent attackers from vulnerabilities and exploitations. These serve as the first line of defense of an organization. When these are left vulnerable, cyberattackers can easily exploit these weaknesses with impunity.

* **CIS Control 12: Boundary Defense**

 There must be a focus on security0-damaging data when monitoring the flow of information across networks. Detection, prevention, and correction are vital processes in this Control.

**Organizational Controls**

* **CIS Control 17: Implement a Security Awareness and Training Program**

 There must be a program in place to identify specific knowledge, skills, and abilities essential in defending the organization from cyber-attacks. This must be assessed across all functional roles in the organization, especially the business’s mission-critical designations. An integrated plan must assess, determine gaps, and remediate through awareness programs.

* **CIS Control 18: Application Software Security**

 Whether in-house or acquired, the software must have a robust security life cycle to prevent security vulnerabilities.

* **CIS Control 19: Incident Response and Management**

 A reliable incident response infrastructure must be implemented and developed to protect the organization, particularly its reputation. This includes defined roles, plans, training, management oversight, and communications. The flow of the response must begin with discovering the attack and must commence with damage control, eradication of the attacker’s presence, and the restoration of network integrity.

* **CIS Control 20: Penetration Tests and Red Team Exercises**

 Simulating an attacker’s objectives and methodology can help the organization prepare and test its defensive strategy strength. This should cover all aspects, including the technology, the policies, and the personnel.

**TASK 12**

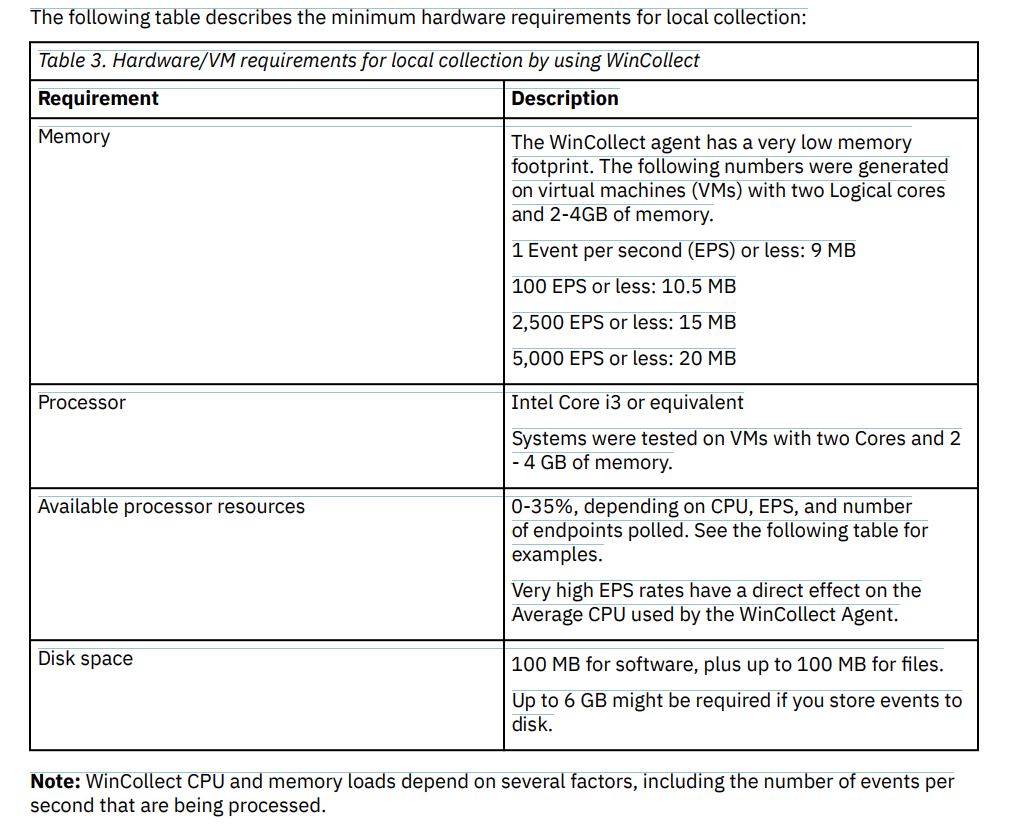
WinCollect is a Syslog event forwarder that administrators can use to forward events from Windows logs to QRadar.

WinCollect can collect events from systems locally or be configured to remotely poll other Windows systems for events.

WinCollect is one of many solutions for Windows event collection.

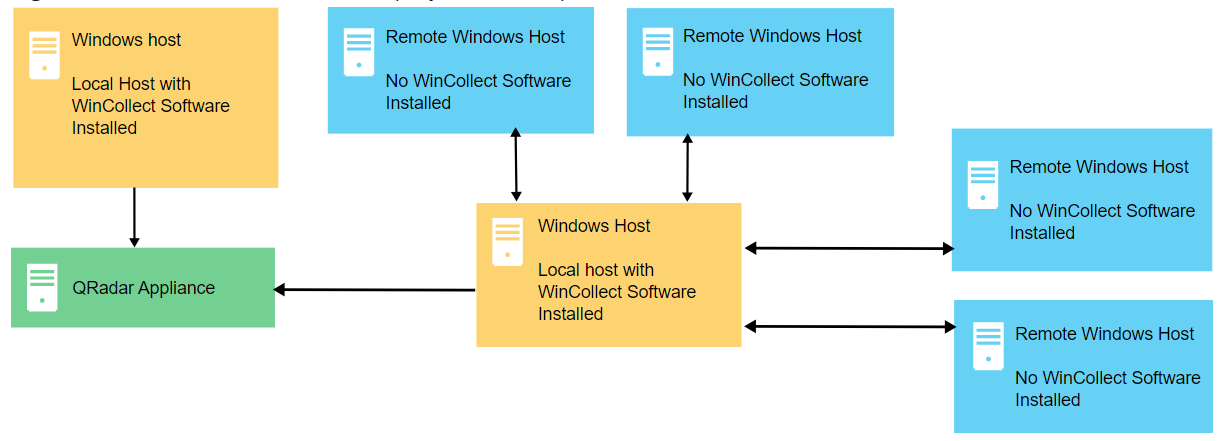
**How does WinCollect Work?**

WinCollect uses the Windows Event Log API to gather events, and then WinCollect sends the events to QRadar. Note: Managed deployment is not supported in QRadar on Cloud environments. Customers who use IBM QRadar on Cloud must use stand-alone WinCollect agents.



**StandAlone deployment**

If you need to collect Windows events from more than 500 agents, use the stand-alone WinCollect deployment. A stand-alone deployment is a Windows host in unmanaged mode with WinCollect software installed. The Windows host can either gather information from itself, the local host, and, or remote Windows hosts. Remote hosts don't have the WinCollect software installed. The Windows host with WinCollect software installed polls the remote hosts, and then sends event information to QRadar. To save time when you configure more than 500 Windows agents, you can use a solution such as IBM Endpoint Manager. Automation can help you manage stand-alone instances.



Stand-alone WinCollect mode has the following capabilities:

* You can configure each WinCollect agent by using the WinCollect Configuration Console.
* You can update WinCollect software with the software update installer.
* Event storage to ensure that no events are dropped.
* Collects forwarded events from Microsoft Subscriptions.
* Filters events by using XPath queries or exclusion filters.
* Supports virtual machine installations.
* Send events to QRadar using TLS Syslog.
* Automatically create a local log source at the time of agent installation.

**Setting up a stand-alone WinCollect deployment**

For a stand-alone deployment, follow these steps:

1. Understand the prerequisites for stand-alone WinCollect, which ports to use, what hardware is required, how to upgrade.

2. Install stand-alone WinCollect agents on the Windows hosts.

3. If you want to add new log sources to your agent or modify existing log sources, install the WinCollect stand-alone configuration console.

4. Configure the destination where the Windows hosts send Windows events.

5. If you want to use the stand-alone WinCollect agent to collect events from other devices using remote polling, create a credential in the WinCollect stand-alone configuration console, so that WinCollect can log in to the remote devices.

6. If you want to add additional log sources to the stand-alone WinCollect agent, do so using the WinCollect stand-alone configuration console.

**TASK 13**

The **Local Security Policy** (secpol.msc) of a system is a set of information about the security of a local computer. It allows you to control various security policies and settings on your Windows 10 computer, functioning like the Group Policy editor (gpedit.msc) that is designed to control settings on multiple computers in a domain from a central location.

According to Microsoft, the Local Security Policy information includes:

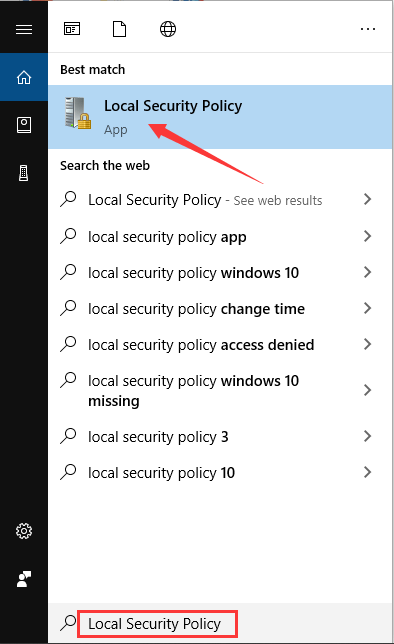
* The domains trusted to authenticate logon attempts
* User accounts may access the system and how
* The rights and privileges assigned to accounts
* The security auditing policy

**4 Methods to Open Local Security Policy**

**Note:** Local Security Policy utility is not available in Windows 10 Home and you can access it in Windows 10 Enterprise, Pro, and other higher editions. Besides, it requires administrative privileges to open Local Security Policy Windows 10.

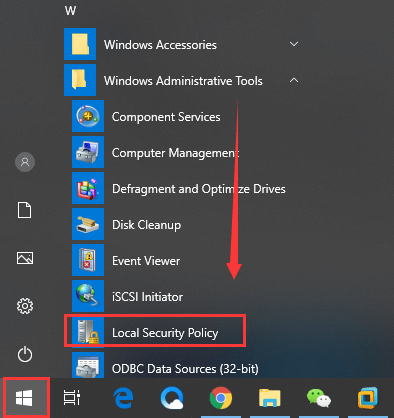
#1. Use Windows Search

* The easiest method to find a certain application is using Windows Search. You can also find Local Security Policy in this way and open it.
* Just press **Windows**+ **S** to open **Search** and type **local security policy** in the editable box. When the application appears in the search results, you can open it by clicking it.



#2. Use Start Menu

* Alternatively, you can also find Local Security Policy in the Start menu.
* You need to click the **Start** button to invoke the menu where all the applications on your computer are listed here. Then, scroll down to locate **Windows Administrative Tools**. Expand it and you will see the **Local Security Policy**. Just click it to open it.



[[](https://www.partitionwizard.com/partitionmanager/win10-start-menu-not-working.html)](https://www.partitionwizard.com/partitionmanager/win10-start-menu-not-working.html" \t "_blank)

#3. Use Secpol.msc Command

* There’s a command **secpol.msc** that you can use to open Local Security Policy Windows 10 quickly.
* Just press **Windows** + **R** to open **Run** window, input **secpol.msc** and click **OK** to open the console of Local Security Policy directly.
* Besides, you can also use this command in Command Prompt or Windows PowerShell to open the application.

#4. Use Local Group Policy Editor

* If you cannot open Local Security Policy using the methods below, you can try accessing it in Local Group Policy Editor. This doesn’t open a standalone console of the application but can allow you edit all the provided security settings.
* To do that, you just need to invoke **Run** window, input **gpedit.msc** and click **OK** to open **Local Group Policy Editor**. Go to **Computer Configuration** > **Windows Settings** > **Security Settings**. Now, you can configure local security policies in this module.

