ENDPOINT SECURITY SURVIVAL GUIDE

A Field Manual for Cybersecurity Professionals

★ ★ ★

Office of Cybersecurity Preparedness

TW-BRESSG16

tripwire®

INTRODUCTION

During the past decade, attackers have demonstrated incredible creativity in adjusting to changes in the security industry. Each time security vendors create a new type of "lock" to protect enterprise assets and data, the criminal underground builds a new set of lock picks in the form of malware to help them circumvent the new controls.

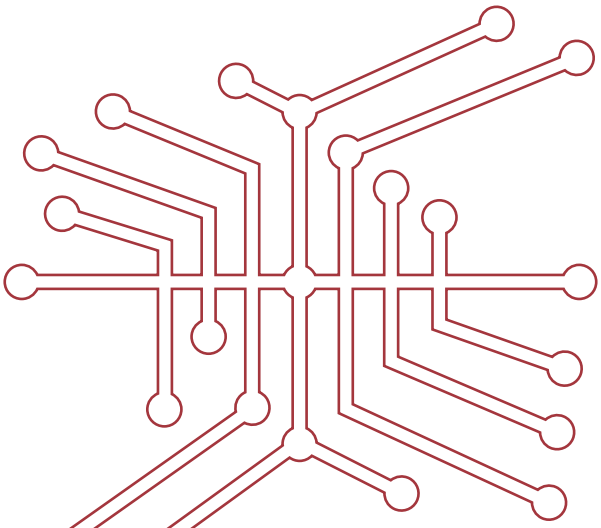
A proactive cybersecurity defense is the best strategy for protecting your business against cyber threats. In the past, security approaches have focused on understanding attacks to stop cybercriminals from accessing corporate networks and systems, but this approach has become less effective. Endpoint Detection and Response (EDR) is a new, proactive approach that focuses on behavior that indicates an attack is underway rather than just indicators of compromise (IoC). In this way, it helps you protect your network against zero-day threats and a wide range of emerging threats. It also reframes the security problem so you're not just focused on keeping the bad guys out. Instead, you're also working to quickly detect intrusions, minimize cyber attackers' abilities and reduce the potential damage they can cause if they do get in. This is a subtle, but critical, shift in strategy that works to disrupt criminal activities. Even if attackers do manage to breach your network, EDR helps make sure they leave empty-handed.

EDR relies on the deployment and active management of key security controls for your business-critical assets. These controls provide crucial information that allows endpoint incidents to be quickly detected, identified, monitored and handled.

This guide delves into the implementation and maturation of each control. It provides an overview of how to build an effective EDR program through robust implementation of these six key controls:

1. **Endpoint Discovery**
2. **Software Discovery**
3. **Vulnerability Management**
4. **Security Configuration Management**
5. **Log Management**
6. **Threat Detection and Response**

These controls represent a consolidated security foundation that are common across many security frameworks, and are necessary for the implementation of an effective EDR program. This guide breaks down the implementation of each control into three phases that progress from the basics to a robust, mature implementation that delivers the information necessary to support an EDR program and effectively combat cybercrime.



Terms Used in This Field Guide

To help simplify the process of implementing and optimizing the six key security controls for EDR, the guide uses the following phrases to identify each phase of implementation, broken down into manageable steps:

BOOT CAMP

This is basic security hygiene. Every security program, regardless of time, budget and skill set should implement at least the basics for each control. Implementation of each control at this level is a prerequisite to advanced training.

ADVANCED TRAINING

If you have dedicated security resources that allow you to go beyond the basics, you should consider adding these advanced capabilities for each control in order to improve visibility and reduce security risks.

COMBAT READY

This term describes the most mature security programs, and expands the implementation of each control to provide the information and visibility necessary to support a robust EDR program.

This field guide describes a sequential, cumulative process of implementing and improving foundational security controls. Keep in mind that skipping a procedure will make each subsequent procedure more difficult to implement—and less effective. For example, it makes sense that building an accurate hardware and software inventory will make hardening configurations more effective. If you miss hardware or software assets in your inventory—and as a result they are not securely configured—your organization's security posture will be weaker, and subsequent controls required for an effective EDR program will be less effective.

After you read this guide, you should be able to accurately evaluate your organization's implementation of each control and understand what you need to do to improve the efficacy of each control.

ENDPOINT DISCOVERY

You must know your hardware to defend it.

Keeping track of your endpoints is essential work that facilitates hardware and software management, license compliance, regulatory compliance and, most critically, security.

The principles of asset discovery are:

A **Removing security blind spots:** It's difficult to create a complete picture of your enterprise network endpoints all at once, but breaking down the process into stages makes it more manageable. You can start with the systems and processes that already exist in your organization. These inputs are likely to be spreadsheets, or some out-of-date network diagrams, or notes stored in the desktops or brains of your IT staff.

B **Standardization now will save time later:** Standards, like the NIST Specification for Asset Identification[1], are useful for identifying endpoints using information you already know about them. With a common format you will be able to share asset information between tools and groups that may not "speak the same language," such as tool sets like IT Service Management (ITSM) and Security Information and Event Management (SIEM), or IT and OT.

C **You really can't get out of doing this:** Before you can defend your network against an enemy, you need an accurate picture of yourself and your environment.

While third-party management of endpoints can be an attractive option, no one knows your business and the value of your data and systems the way you do. One of the first steps an attacker targeting your network will take is building an inventory of potential targets connected to your networks. Attackers do this as part of a process of discovering your weaknesses, because those are the easiest places to attack. To defend your endpoints, you need to know where your weaknesses are, so you can fix them before the enemy uses them to attack you. There's no way to find all of the weaknesses in your network if you don't first have an accurate list of your assets.

Impediments to Discovery

These things can trip you up:

1 **Segregated networks:** In larger organizations, endpoints are usually located across a global collection of multi-segmented networks, physically secured areas, and behind data diodes that prevent unauthorized access. Appliance and cloud-based options that deploy data collectors on remote and segmented networks can be useful for endpoint discovery in segregated environments.

2 **Proprietary protocols:** Not all networks support traditional IT protocols[2]. Some endpoints, like Industrial Internet of Things (IIoT) devices will speak proprietary protocols that are not IP-based.

3 **Fragile as an autumn leaf:** Scanning some types of endpoints, such as IIoT devices, can result in disrupted service. Passive discovery and asking around may be the only ways to inventory these devices safely without affecting availability or reliability.

BOOT CAMP

Establish a baseline of your endpoints

1. **Collect information from existing records:** Ask for all of the network maps, Excel sheets of endpoint assets, sticky notes and other odds and ends of information that comprise your system of record.

2. **Scan you network:** After gathering tribal knowledge about what people think is on your network, it's a good idea to find out what's actually on your network using an automated discovery tool to scan it. Use a commercial product (e.g. Tripwire® Asset Discovery[3]) or free networking tool (such as Nmap[4]), to start mapping your network.

3. **Passive Discovery:** Use a commercial product, such as Lumeta IPSonar[5], or a free tool, such as Kismet[6], to map the endpoints, including wireless access points.

4. **Reduce your addressable IP space:** Make sure your organization is using the fewest number of IPs possible, and make sure those IPs are within the private address space[7].

ADVANCED TRAINING

Refine your endpoint asset inventory

5. **Use logging from DHCP**: If you are using DHCP, you can collect these logs to keep a record of the endpoint MAC addresses on your network.

6. **Acquiring new hardware:** Endpoint inventory should be a documented part of the business process associated with inventory and control. Make the addition of new hardware and removal of old part of an ongoing endpoint inventory process. Once per quarter, or more often if possible, use endpoint discovery scans to identify unauthorized endpoints that could be a vector for attack.

7 **Attach ownership and other meta-data:** Now that you know which endpoints are out there, you need to know who's responsible for them. This can be difficult, especially when this information is not written down. Use your security tool's metadata capabilities to track endpoint information such as endpoint owner, business purpose, risk, value and other key elements that help identify the business context of each asset. Identifying the endpoint owner is especially important in order to know who to partner with to improve the security of the endpoint. Ideally, this information will be incorporated across your security tools automatically using tags and rule sets derived from the configuration and profile of each endpoint. This approach dramatically reduces or eliminates manual data entry errors.

COMBAT READY

Electrify the fences, Automate, Alert, and integrate

8 **Electrify the fences:** Now that you've attached ownership to each endpoint, you should require the owners of endpoints to authenticate when using shared resources like wireless access points. This way only authorized devices and users are allowed to use secured networks.

9 **Automate:** Along with DHCP logs, use active and passive scans to update endpoint inventory to increase the accuracy and timeliness of data and alerts.

10 **Alert:** Start adding alerts for unauthorized/unknown devices so these can be quickly identified and either authorized or sequestered from the network.

11 **Integrate:** Look for ways to enhance and improve discovery accuracy by integrating and correlating inventory data across ITSM, SIEM, GRC and FIM tools.

SOFTWARE DISCOVERY

You must know your software to defend it.

Keeping track of your software assets is essential for a well-run enterprise and facilitates more effective software management, license compliance and, most critically, security. Nearly every regulatory compliance standard includes software inventory because attackers could exploit unknown or unnecessary applications. In addition, the mere presence of an application on an endpoint could be an indication of an attack.

The principles of software discovery are:

A **Attackers will find the weakest parts of your attack surfaces:** The bad guys love to find a juicy unpatched software package. Whether it's a server running an old version of SSH or Apache or a laptop with 5 year old Internet Explorer exploits are easy to find and use.

B **What you don't know can hurt you:** In terms of licensing and security, not knowing exactly which software is used on each endpoint can be expensive. When it comes time to pay for licenses of premium software, knowing the number of licenses you are paying for versus actual license usage may help you negotiate a lower maintenance renewal cost. Unknown or unnecessary software increases security risks because these installations are easier for attackers to misuse or exploit. If you don't need a specific software package on an endpoint, turn it off.

C

For lack of a backup the kingdom was lost: When a system fails-over during a planned outage, having an identical system to pick up the tasks is critical. Part of a comprehensive software inventory process is identifying backups. This makes recovery more successful and helps minimize repair costs.

BOOT CAMP

Lists and authorizations

1

Build a complete list: You can use an endpoint asset discovery or vulnerability management tool (like Tripwire Asset Discovery[3] or Tripwire IP360™[8]), Excel or a free database to document authorized software packages on each type of endpoint.

2

Scan you network: The same tools used for endpoint discovery apply here. You can use a commercial product, such as Tripwire Asset Discovery[3], or a free networking tool, such as Nmap[4], to identify open ports and services.

3

Roles endpoints play: A server usually doesn't need Microsoft Word, a workstation shouldn't be running a Web server, and accounting probably doesn't need Visio. For each department and business unit there should be a list of authorized software for each type of hardware device.

4

In security, less is more: "Perfection is achieved not when there is nothing more to add, but when there is nothing left to take away."[9] Reducing the number of authorized applications will make it easier to protect the remaining authorized software. Fewer software applications also mean there are fewer holes an attacker can squeeze through. There's also less software to patch, protect and monitor, which reduces resource requirements and false alarms.

ADVANCED TRAINING

Secure those systems

5 **File integrity monitoring and security configuration management:** Now that you have an accurate list of all the endpoints you have and the software applications they're running, the next step is to make sure they only change as authorized. To achieve this, you'll need to monitor endpoints to ensure the integrity of configurations and reduce "drift" from known good states. Catching and remediating unauthorized changes will maintain and improve your security posture and help identify a breach quickly. Products like Tripwire Enterprise have evolved to meet these needs by going beyond basic file integrity monitoring by including advanced capabilities like auto remediation and detailed change histories, along with the appropriate context/feeds necessary to differentiate good from bad change.

6 **Whitelist profile:** An unauthorized port is a policy violation at best and an IoC at worst. Tripwire Enterprise[10] can identify ports and services running on endpoints and monitor for unauthorized port usage[11]. You can also trigger automatic alerts and remediation when an unauthorized service is present or running.

7 **Exception handling:** Every business or mission has some legacy applications and one-off proprietary items that are more difficult to secure. The owners of these endpoints may have access to critical information about their purpose and configuration, as well as the authentication and privileges needed to access them or make changes in an emergency. Make sure you know who owns these assets and how they are handled during audits. It's also crucial to identify the mitigating controls that can be used to secure them.

COMBAT READY

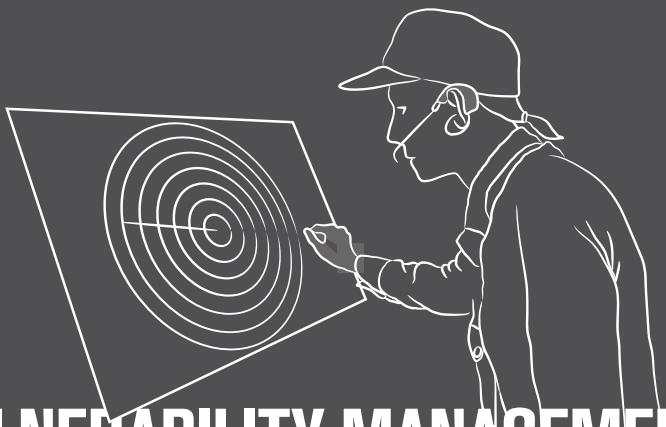
Electrify the fences, automate, alert, and integrate

8 **Electrify the fences:** Now that you know what should be running on each asset type, you can start identifying unauthorized applications. Just as with ports, unauthorized apps are a policy violation at best and an IoC at worst, so it's important to find them quickly. When your endpoint detection solution identifies an unauthorized application, it's important to investigate because it may be part of a breach. The good news: once you define "authorized" software applications, it's much easier to define "unauthorized" through process of elimination.

9 **Automate:** Your environment isn't static. You need to update your endpoint software inventory regularly using file integrity monitoring and whitelist profiling to keep it accurate. It's also smart to make sure old software is decommissioned and new software is carefully vetted to ensure compatibility and compliance with your policies. As your organization evolves, your endpoint population will change. These shifts need to be incorporated into a baseline that represents "known good" devices and configurations, which will help you identify "known bad" ones.

10 **Alert:** Start adding alerts when unauthorized software is found in your environment. Gateways, such as Palo Alto Networks' next-generation firewalls, can identify applications in use across gateways. Tripwire IP360[8] is excellent at inventorying applications installed on endpoints.

11 **Integrate:** Once you have individual security tools working reliably, look for ways to expand integration across your security stack. Integration across ITSM, SIEM, GRC and FIM can automate workflows, saving valuable time and resources. Integration can also make it possible to correlate information between security controls. This improves accuracy and timeliness of the information necessary to detect and respond to threats.



VULNERABILITY MANAGEMENT

Vulnerabilities and exposures are your enemy's allies.

Attackers benefit from the same innovations that drive digital business: automation, crowdsourcing, low cost cloud computing resources, big data, mobile, and social networks. All of these innovations can also be used to attack you. Worse, an attacker only needs to be successful once through any attack vector; meanwhile, you must remain ever vigilant. Somewhere, in the tangle of interconnected hardware and software packages running on your networks, are vulnerabilities that can be exploited given enough time and effort. Managing those risks continuously and in a timely fashion is crucial to security.

You may also face another challenge if your board of directors does not "get" security and has difficulty understanding the connection between risk reduction and vulnerability management. You will need to communicate your efforts in terms of risk reduction and potential impacts of breaches avoided.

The principles of vulnerability management are:

A **Highest risks first:** You need to work toward continuous vulnerability scans. They will provide you with up-to-date scan results from all the endpoints identified in endpoint and software discovery. These scans will find

and prioritize all the vulnerabilities across your network. Once located, you will be tasked with remediating the riskiest vulnerabilities quickly

B

Attackers are looking for the same things you are: They have access to myriad resources, and all they need to do is find a single vulnerability that can be exploited to get in. You must plug holes continuously to reduce your attack surface and limit security risk.

C

Fix vulnerabilities that jeopardize the mission: CVSS provides a useful mechanism for prioritizing vulnerabilities in a standard way that is easily understood between different people, departments and organizations. Advanced vulnerability management tools, like Tripwire IP360[8], include more granular scoring mechanisms that provide predictive "heat map" capabilities. These tools identify areas of highest risk on your network. These are the places where a successful attack is most likely to disrupt business or operations.

BOOT CAMP

Scans and more scans

4

Scan frequency: Run vulnerability scanning tools against all inventoried systems to identify endpoint weaknesses that could be leveraged during an attack. While many organizations strive for continuous scanning, significant investments in scanning infrastructure may be required to complete assessments within scan windows. Also, remember that human resources are required to respond to the findings.

Choose a scan frequency target that is realistic based on the resources available to you. For example, weekly assessments may be a stretch goal for one organization, but not frequent enough for another. You may also want to increase the frequency of scans on more critical endpoints or Internet-facing systems.

Prioritize the findings from your scans and deliver them to the system owners, summarizing the findings for management. Include risk scores to quantify risk severity and prioritize remediation based on criticality. Tripwire IP360[8] is an excellent product for internal assessment, and Tripwire PureCloud[12] is very effective for assessing Internet-facing endpoints, as granular scoring based on business context information is a key deliverable.

5 **Patch, harden, repeat:** Obviously, identifying these issues is only useful if you are fixing them. Some issues will be addressed using a patch management business process, and others will require a mitigating control or configuration change. Regardless, this will be a continuous process.

6 **Report cards:** Continuous scans will allow you to quickly identify trends in the data that will indicate how well your vulnerably management program is performing, as well as where risk is increasing or decreasing. They will also help justify resource allocation. Communicate all of these things in your reports. Tripwire's reporting products generate risk report cards to help illustrate security posture trends.

ADVANCED TRAINING

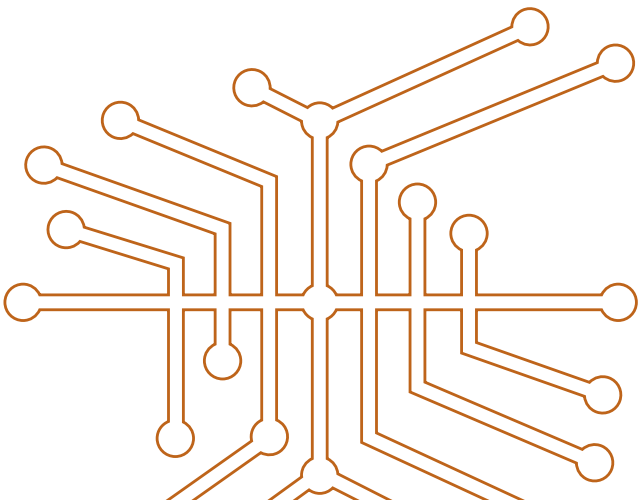
Develop your security intelligence

7 **Security intelligence sources:** Just like you, attackers are looking for ways to make their job easier and do more with fewer resources. The availability of attack kits and frameworks can make it easier for attackers to gain access to your network by automating complex processes. These tools allow less skilled attackers to execute successful attacks. Therefore, your vulnerability risks may increase as new automated attacks become available. Subscribe to vendors who provide frequent updates to

policy content, device and application detection and vulnerability detection rules. Leverage information regarding exploit kit availability and potential impact to prioritize investigation and response, especially in places where an attack is most likely to occur or will cause the most disruption

8 **Do deeper scans:** Perform scans in authenticated mode either with an agent or by providing your scanner with administrative credentials. Credentialed assessments take longer to run than uncredentialed assessments, but the additional information that is gathered dramatically improves discovery and assessment accuracy.

9 **Use your SIEM with Network Intrusion Prevention System (NIPS) logs:** One of the core use cases behind the development of correlation engines is the need to correlate the vulnerabilities on an endpoint with active exploits on a network. Combining information from multiple sources increases the usefulness and accuracy of the information. Take advantage of this technology by bringing your scan information and the logs from your network intrusion prevention systems into your log management tool. Tripwire Log Center[13] and its integration with Tripwire IP360[8] and Cisco FirePOWER NGIPS[14] is an example of this technology in action.



COMBAT READY

Automate, Alert, Integrate

10 **Automate patching:** Where possible, deploy automated patching software to keep system software up to date. Manual efforts will not scale in most organizations due to the explosive growth in the number of vulnerabilities and the endpoints they impact.

11 **Limit time frames of scans and alert on discrepancies:** You can detect unwanted reconnaissance by defining the times of day when authorized access is allowed and by looking for it in events of interest that occur outside normal business hours in your SIEM or log manager. Tripwire Log Center[13] can help with this type of behavioral detection.

12 **Integrate scan results into risk systems:** Consolidating risk data from multiple sources provides a more accurate view of enterprise risk, which allows you to manage risk and demonstrate improvements in security posture. GRC, network visualization and pure-play risk management tools can all take a role. Consolidated risk data makes it possible to "percolate" risk scores up to business owners of high-risk endpoints. You should include factors like potential exploit impact, exploitability and attack vectors in these reports. For example, data from Tripwire products integrates with a wide range of other security products[15] to automatically consolidate risk information.

SECURITY CONFIGURATION MANAGEMENT

Default configurations are built for maximum availability and rarely for security.

Hardening default configurations will mitigate many security issues on endpoints. Further, any prescriptive compliance policy will already have out-of-the-box guidance on these first steps, so this is a logical place to start.

The principles of security configuration management:

A **The right settings will evolve over time:** There are millions of ways to configure systems. The right mix of security, availability and performance often requires ongoing adjustments, unless you standardize on a legacy platform[16] where that never changes. Don't laugh — it's a viable option.

B **Security policy, like the endpoints, need to be reassessed periodically:** Even after you have tuned the finest configuration settings over countless meetings, there will come a time when the business or mission changes, software is updated, or new exposures are detected. Then policies will need to be re-tuned and all endpoints checked against them. This is typically done in conjunction with preparation for annual IT audits, but it should be done anytime there is a significant business change.

C **Unnecessary services and ports are dangerous:** Use applications and services identified during software discovery to start trimming back on things that aren't required by the business. Unneeded web servers, unauthorized file sharing applications, media players and unused programs are examples of applications that should be found and then turned off.

D **Users and their access:** User credentials have become a new target in today's threat landscape. Hackers frequently go after accounts and credentials that are enabled, but not closely monitored or actively used. Since these accounts and credentials are legitimate, hackers can easily evade detection because their activities appear to be part of business as usual.

Attackers use numerous techniques to steal employee credentials so they can gain access to corporate systems and networks. Sophisticated phishing campaigns can trick even the most skeptical users into entering their credentials on fraudulent websites. Advanced malware enables cybercriminals to capture employee credentials as they're entered on an infected endpoint. What's more, cybercriminals don't even need to try to obtain corporate credentials directly from employees. Reuse of corporate credentials on third-party sites is so high that some criminal groups focus on stealing login credentials from social networks and other consumer websites, knowing there's a good chance they'll obtain credentials that will give them entry into corporate systems.

Another concern is disgruntled insiders. Accounts that aren't deactivated after employees leave can be misused by both insiders and external actors. For example, a disgruntled terminated employee with remote access to company systems has the potential to cause a lot of problems.

BOOT CAMP

Leverage standardization

1 **Standard Operating Procedures (SOPs)**: Standardize a set of procedures for hardening your hardware platforms and software. The goal of these procedures is to provide enumerated settings that any system administrator can implement. Validating your procedures against security best practices (e.g., CIS Critical Security Controls[17]) can also make it easier to standardize your operating procedures. All organizations have exceptions: the CEO may insist on using a Mac or marketing requires new editing software. Make sure that exceptions to standard configurations are noted along with ownership and an expiry period, after which the exception must be reviewed and reapproved.

2 **Use secure gold images**: New systems should be rolled out with standard security settings included in master images. If a system is compromised, it's often faster and easier to replace it with a known secure image instead of taking the time to manually remediate the endpoint. Make sure the deployment of these updated systems is ticketed, so the change is documented and related information is available to system owners and responders.

3 **Legacy software:** One of the most important considerations for your security posture is the selection of tools and applications that are allowed to run in your environment. Many attacks take advantage of older vulnerabilities that may exist in the OS and/or software being deployed. It's important to check the manufacturer for updates and patches and the overall security readiness of legacy software. Be sure to note any potential vulnerability that may need to be mitigated using other means besides patching. Choosing a standard set of applications will also allow you to detect anomalies and unauthorized installations during your periodic software audits.

4 **Monitor "who" has access:** Administrative and system accounts, which can be used for auditing or creating correlation rules, should be carefully monitored. Set up automatic alerts that will flag any unauthorized activity connected with these accounts. Set policies that require users to change their credentials often, and test users with unscheduled security awareness training.

5 **Use secure communications:** Unencrypted communications and credentials can be intercepted and reused by an attacker, so make sure remote protocols are secured using strong encryption. If strong encryption isn't available for your application, then you should seriously consider removing it from the "authorized" list or take other mitigating steps to harden this asset. These might include isolating it from other networks and endpoints and severely restricting its access.

ADVANCED TRAINING

Monitor ALL the things!

6 **Monitor everything for changes**: Now that you've clearly identified what a secure baseline system configuration should look like for each asset type, monitor all systems for changes against that baseline. Tripwire Enterprise[10] can make sure business-as-usual changes are automatically promoted, and that authorized not-business-as-usual changes are ticketed and reconciled.

7 **Monitoring all the things (including OT):** IIoT devices can be a challenge because OT hardware often uses proprietary protocols. Talk to your SCM vendor about their capability to work with your IIoT vendors. Don't be surprised if monitoring of IIoT devices is achieved indirectly through IT systems (database queries, configuration files or command line interface at HMI) or through the simple expedience of event logs.

8 **Set alerts for administrator accounts:** Set up an alert for any time "administrator" or "root" accounts are used, as well as to automatically link the chain of events where they logged in from, what account was used to get to the system, etc. Monitor network events and trigger alerts when bogus or blacklisted IPs are detected. Alerts should also be issued on combinations of network and system events that could be unauthorized or indicative of a compromised system.

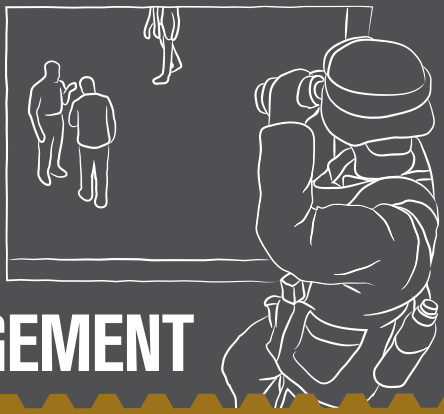
COMBAT READY

Automate, alert, and integrate

9 **Integrate to analyze**: Send alerts on unauthorized changes to ticketing systems as incidents and to SIEMs for security incident handling and correlation. Automate the detection of ports and services, as well as for new users.

Since multiple, conflicting polices can apply to a particular user and endpoint combination, you can also monitor Resultant Set of Policy (RSoP) to calculate the cumulative effect of multiple policy settings on Windows endpoints. RSoP is the group of policy settings in effect for a specific user. Wherever possible, reconcile these changes automatically. Tripwire Log Center can aggregate logs from all egress points and alert when that should be restricted to using proxy connections but are not are detected.

Tripwire Log Center can act as the receiving SIEM/log analytics system and correlate events. This can help save costs when forwarding to a SIEM product that's licensed based on amount of data processed.



LOG MANAGEMENT

As the volume and sophistication of cyber threats increase, organizations must sift through mountains of data to detect anomalies and identify real threats.

The traditional approach of handling ever-increasing log and event data has been to rely on basic log collection utilities or expensive large-scale SIEM deployments.

The principles of log management are:

A **Log management is a core component of endpoint detection and response**. It provides convenient access to diagnostic information about events of interest, creates reports on your event data, serves as a historical catalog of log messages and events, and enables compliance with regulatory policies and industry standards.

B **Jack of all security trades:** To provide these benefits, zlog management systems collect log data from operating systems, applications, databases, IDS/IPS and network devices, such as firewalls and switches.

C **Answers the question, "What happened?"** It helps you better understand your environment, detect and prevent attacks. Also, malicious actors prefer to disguise their tracks by deleting or resetting logs to hide their activity. Detecting this is important for finding attacks.

BOOT CAMP

Know thyself

1 **First things first**: Turn your logs on. Every critical system has a log you can enable. In many cases, critical logs aren't enabled (by default or otherwise), so critical data is missing when detecting and responding to emerging cyber threats.

2 **Architect your log collection**: Know where your log data will be collected. In larger organizations, log data will be collect-ed from a worldwide network of connected devices distributed across geographically dispersed offices.

Creating a map and architecture of where your log data originates will enable you to fine tune your log data collection and storage architecture. During this phase, estimate the disk storage required to store "active" and "archived" log data based on its retention time. In most situations, there are regulatory guidelines you must follow. For example, you might be required to keep "active" log data available for 90 days and to retain "archived" data for 365 days.

Your map and architecture should, at a minimum, contain the locations of log data to be collected, the type of log data, expected daily log growth, the length of time the log data will be retained as "active" and "archived," and who has access to the it.

3 **Use secondary log managers**: By adding one or more secondary log managers to your environment you can distribute log management functionality to meet your organization's growing needs. The use of secondary log managers can improve performance while also giving you the ability to partition log data based on geography, business unit or business function.

4 **Reliably collect log data:** Each log contains unique data. When combined, the cumulative data will provide insights into emerging cyber threats. In the event of a breach, you will need all the endpoint data you can get your hands on: logs from network devices (such as firewalls, switches, IDS and IPS), all operating systems, databases, applications, servers and more. The collection process should ensure that if a system, device or other asset fails, you have 100% certainty that your log data is safe.

5 **Centralized Storage:** Because the data is easily accessible, centralized collection of logs and events is important for enabling fast investigations, forensics, and detection and response to endpoint threats. Good log management products like Tripwire Log Center can collect deep and detailed log data as well as endpoint event and network activity information, and store that information in a repository capable of large-scale data reporting and analytics.

Forensic investigations into how and why an incident occurred can benefit from a comprehensive archive of log data and events. When an investigation is underway, it's helpful to have log management tools that can adjust the length of time for archives, and enable the ability to dearchive log data for investigations or audits. It's also useful to employ a tool with high levels of compression to reduce storage demands, while simultaneously protecting logs from alteration.

ADVANCED TRAINING

Identify and alert

6 **Correlation Rules:** Identify emerging cyber threats with the identification of suspicious events based on correlation of system changes, weak configurations and vulnerabilities. Leverage products with drag-and-drop capabilities to quickly define and customize correlation rules for events and filter and detect anomalies, suspicious behaviors, changes and patterns known to be threats and IoC. In addition, you can correlate predefined patterns of malware behavior and exfiltration.

7 **Alerts:** When your logs match correlation rules, advanced log management products can identify suspicious events for quick review using trigger-specific alerts and actions. This reduces the need for specialized expertise and resources to create correlation rules in more complex formats.

COMBAT READY

Integrate, automate and investigate

8 **Integration:** Integrate your log management solution with a security configuration management product like Tripwire Enterprise[10] and a vulnerability management product like Tripwire IP360[8] to provide your organization with additional security and business context that will help prioritize the most critical threats.

Integrated log management systems can use correlation rules to detect and alert you to suspicious events that affect the security state of your system.

9 **Combine business, security, risk and user context:** Combining business and user context lets you easily monitor assets and users that, when combined, may warrant a closer watch. For example, you might want to carefully monitor the highest value assets to which contractors have access. You can further prioritize risk by correlating suspicious events identified by Tripwire Log Center[13] with suspicious changes detected by Tripwire Enterprise[10] and vulnerabilities identified by Tripwire IP360[8]. For example, when integrated with a vulnerability management solution like Tripwire IP360, the log management solution will provide increased network and threat awareness within your environment. This combination of vulnerability and event information provides insights that enable you to identify risk and prioritize your security efforts.

10 **Collect and forward:** To forward only relevant and actionable data to your SOC and third-party tools such as SIEMs and threat intelligent solutions, pre-filter log data to identify anomalies and patterns known to be IoC. Advanced log management solutions should be able to filter and detect anomalies, suspicious behaviors and changes and patterns based on threat and IoC data.

11 **Automate:** Extend correlation rules to provide alerts and remediation. Identify the personnel and resources that need to be notified when specific situations are identified, and then extend the correlation to contact the personnel responsible to investigate and remediate the alerts. Also consider scripted responses for correlation rules that can automatically remove, mitigate or harden your endpoints.

THREAT DETECTION & RESPONSE

Advanced threats are designed to outwit traditional signature-based anti-virus (AV) solutions using polymorphic and self-updating, environment-aware malware[18]. This shouldn't be surprising. Old school detection was developed based on a very different threat landscape, one in which threats evolved much more slowly and were less sophisticated. Not too long ago, the security industry just needed to know something about an attack to write a signature or rule that would protect against it.

EDR is a new approach that evolved from the realization that the industry can't prevent attackers from getting in. Instead, we should assume they *will* get in, so focus on real-time detection of behavior that indicates a breach. Then, it's important to create effective incident responses designed to limit damage. EDR supplements traditional, signature-based technologies with anomaly detection and visibility across all enterprise endpoints, not just servers and workstations.

The principles of malware detection and response are:

A **Faster than a sniper's bullet:** Modern phishing attacks occur at nearly the speed of light, and the first hit is likely to be an innocent user clicking on a malicious attachment or URL in an email. The malware this action unleashes can cut through security defenses.

B

Attackers customize their attacks for your enterprise: These are targeted attacks. The attackers will use non-invasive techniques like social engineering to glean who your employees are and what their emails look like.

BOOT CAMP

Make sure you do the basics for every endpoint

1

Mind your SOPs: Earlier we discussed establishing your SOPs. In nearly every single breach there is a detectable change to the environment. These are the early indicators that an attack may be underway. Monitor applications that are running, and issue alerts on new software that's accessing critical data. If your SOPs limit software executables to a whitelist, then any anomaly must be investigated.

Unusual user access may also indicate a compromise. Update user credentials often and test users with random security awareness training. Finally, be sure that users are not reusing credentials outside the corporate environment to prevent someone else's breach from becoming yours.

2

Run anti-virus: While AV isn't stopping most malware these days, it still stops some of it. Symantec admits that AV only stops about 45% of attacks[19]—but at least it helps.

3

Run host-based firewalls/IPS: Remember when we talked about blocking unnecessary ports and services? Do this on every endpoint by limiting the applications authorized to run and the ports that may be opened. Advanced malware may still manage to find a port or process to hijack, but at least you'll be making it much more difficult for attackers.

ADVANCED TRAINING

Centralize management of malware detection

4 **Alternatives to anti-virus**: We already know that AV is not enough to thwart the most advanced attacks. Cybercriminals have also gained understanding of how AV works, and so they actively endeavor to get around these protections.

Your focus should be on the possible attack vectors and how to use the most effective protection technologies to stop the attack. For example, many recent attacks incorporate a compromised website as a way to make first contact with their victim. Web filtering would be the most effective way to prevent this type of infection by preventing accidental exposure.

Other possible alternatives include whitelisting, sandbox containment, exploit disruption, email and web filtering, network access control (NAC), host-based intrusion prevention (HIPS) and even changing user passwords. All of these tools have their place and should be considered as part of a multi-layered, defense-in-depth approach to protecting your most valuable endpoints.

5 **Send the logs to your SIEM for correlation:** At some point you will be looking for evidence of a breach or evidence that your latest breach has been contained. To do this, logs will need to go to a log management system such as Tripwire Log Center. As an added bonus, if you collect and analyze these logs in real time, you may be able to catch traces of activity before an attacker covers their tracks by deleting logs. Analytics derived from consolidating various logs in one place can lead you to hidden security gems and more accurate forensics.

6 **Make sure anti-virus is running:** Make certain your AV is running with up-to-date virus definitions using its enterprise management console. Alternatively, use a solution like Tripwire Enterprise's Security Dashboard.

7 **The only good change is an approved change:** If you ticket and reconcile every change, then anything that isn't ticketed is an unauthorized change. Unauthorized changes are sometimes malicious and always a teachable moment for your admins. Using this approach, malware detection becomes a natural byproduct of good security configuration management practices

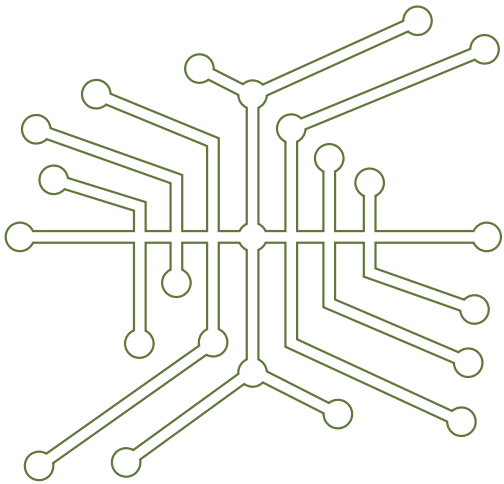
COMBAT READY

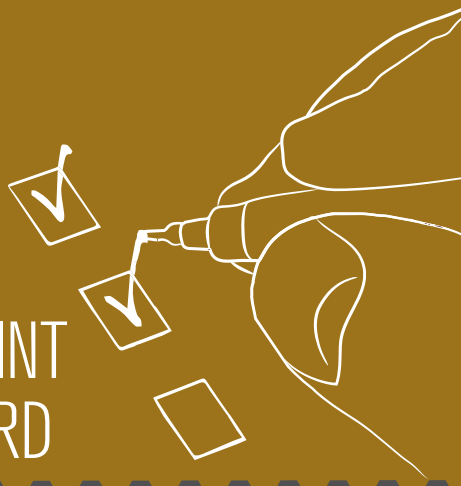
Integrate threat intelligence into your controls

8 **Integrate network threat intelligence with endpoint detection**: Use the integrations between Tripwire Enterprise and leaders in network threat intelligence like Check Point Software Technologies[20], Palo Alto Networks[21], Cisco[22], Lastline[23], Blue Coat[24], and FireEye[25]. These solutions bring network and endpoint security together to make detection and protection against advanced threats more accurate and timely using a three-step process. First, suspicious files on critical assets are identified. Next, the files are sent to a threat analysis service. Finally, security controls are updated based on identified threats.

9 **Integrate hash indicators of compromise with endpoint detection:** Utilize peer and community-sourced IoC hashes to gain intelligence on new and emerging threats. By leveraging STIX and TAXII standards or tailored commercial threat intelligence services, you will be able to look for threats that may be hiding in the blind spots of your defenses. These IOCs are automatically downloaded to Tripwire Enterprise, which then searches forensics data. If a threat is detected, you get an alert and are able to drive remediation.

10 **Integrate network indicators of compromise:** These vendors, as well as many others, provide threat intelligence about IPs, domains and names that are known to host malware, command and control servers and other attack infrastructure. Use this intelligence to modify firewall rules, IPS blocking and SIEM correlations. By correlating network intelligence with other security data in big data solutions like Splunk[26], you can rapidly determine when your enterprise is communicating with a known bad actor.





SUMMARY: ENDPOINT SECURITY SCORECARD

Knowing how mature your organization's EDR program is in comparison to the principles outlined in this field guide will quickly give you an idea of where additional refinements may be necessary.

We recommend you measure your organization against the guidance in this field guide to help improve your security risk posture. Complete the following scorecard and tally the results to help you understand what you need to do to improve the efficacy of each control as part of your EDR program.

Give your organization a 0–3 rating for each control...

0: "We're not doing anything."

1: "We only do the bare minimum, usually for compliance reasons."

2: "Yes, we do this, but it's not perfect."

3: "We have this down to a science and are constantly looking for ways to improve."

CONTROL	SCORE
Endpoint Discovery	
Software Discovery	
Vulnerability Management	
Security Configuration Management	
Log Management	
Threat Detection and Response	
TOTAL	

Your Score

0–6: Boot Camp

You face a range of challenges putting together a strong EDR program, but don't worry—we've got you covered. Here are some additional resources:

- Read the Endpoint Detection and Response For Dummies[27] e-book to learn about deploying and managing security for many kinds of endpoints
- Read the "Meeting the True Intent of File Integrity Monitoring"[28] white paper
- Read the Security Configuration Management For Dummies[29] e-book
- Sign-up for a Tripwire SecureScan[30] account for free vulnerability assessments

7–12: Advanced Training

Well done. Here are suggestions on how you can take your security programs to the next level.

- Understand why the tactics and strategies to respond to high-impact vulnerabilities differ from those used in other security events[31]
- Read "Restoring Trust After a Breach: Which Systems Can I Trust?"[32]
- Watch the video "How to Protect Against the Ransomware Epidemic"[33]

13–18: Combat Ready

Congratulations, you are a leader in your field, constantly looking for ways to improve security. Here are some resources for highly mature security organizations:

- Tips for taking your organization's vulnerability management program to the next level of maturity[34]
- Learn about Actionable Threat Intelligence: Automated IoC Matching with Tripwire[35]
- Get tips for taking your organization's vulnerability management program to the next level of maturity[36]
- Find metrics on how to assess the current state of your endpoint security program in the "SANS – A Maturity Model For Endpoint Security"[37] white paper

Learn More

Tripwire can show you how to build a holistic approach to endpoint security and strike the right balance between protection and detection. To get started, check out the EDR Resources page[38] featuring videos, guides and white papers designed to help you with your defensive strategy.

Definitions

Alert: A prioritized notification of critical security incidents

Asset: An asset is any company-owned information, system or hardware that is used in the course of business activities

Baseline: A "known-good" configuration of a device used for change comparison to identify suspicious changes

Business Context: Security metadata unique to each organization that aids in filtering and prioritizing security data

Change: A deviation from a known configuration that alters the state of a device

Configuration: How an endpoint is set up, including, but not limited to, registry settings, configuration files, database schemas and permissions, group and local policies, services and ports enabled

Contain: Minimize losses and repair systems

Detection: The identification of security incidents using endpoint monitoring

Endpoint: Any device that could be targeted in an attack, or any device that could be used to advance an attack

FIM: File Integrity Monitoring, a security solution that monitors key system files for changes

Hardening: Reduces the exploit risk of a device by optimizing configuration settings for security, including, but not limited to, disabling unnecessary services and accounts, removing unneeded applications, eliminating information exposures and remediating vulnerabilities

IIoT: Industrial Internet of Things

Investigate: The process of gathering and analyzing information related to security incidents, including ability to drill down into information about what changed and who changed it, as well as a launch-in-context ability to pivot between data sources

Information Technology (IT): Technology involving the development, maintenance and use of computer systems, software and networks for the processing and distribution of data

Operational Technology (OT): Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events

Policy: A specific set of preferred device configurations or states as defined by a governing or regulatory authority

Remediate: Mitigating steps taken to address a security issue or vulnerability

Threat Intelligence: Information from a third party that can be correlated with information you collect to detect threats

URLs of Links in this Document

1 csrc.nist.gov/publications/nistir/ir7693/NISTIR-7693.pdf

2 tripwire.com/state-of-security/featured/the-industrial-internet-of-things-fueling-a-new-industrial-revolution

3 tripwire.com/register/tripwire-asset-discovery-appliances-discovery-and-profiling-for-network-situational-awareness

4 nmap.org

5 www.tripwire.com/register/tripwire-ip360-with-lumeta-ipsonar-providing-unparalleled-visibility-for-vulnerability-management

6 kismetwireless.net

7 tools.ietf.org/html/rfc1918

8 tripwire.com/it-security-software/enterprise-vulnerability-management/tripwire-ip360

9 lifehacker.com/5962245

10 tripwire.com/it-security-software/scm/tripwire-enterprise

11 tripwire.com/register/tripwire-whitelist-profiler

12 tripwire.com/it-security-software/enterprise-vulnerability-management/purecloud-enterprise

13 tripwire.com/it-security-software/tripwire-log-center

14 cisco.com/c/en/us/products/security/ngips

15 tripwire.com/company/partners/technology-alliance-partner-tap-program

16 cio.com/article/2944673/security0/7-places-you-ll-be-surprised-to-learn-are-still-using-windows-xp.html

17 cisecurity.org/critical-controls

18 labs.lastline.com/analyzing-environment-aware-malware-a-look-at-zeus-trojan-variant-called-citadel-evading-traditional-sandboxes

19 dottech.org/157355/symantec-admits-anti-virus-software-is-no-longer-effective-at-stoping-virus-attacks

20 checkpoint.com

21 paloaltonetworks.com

22 cisco.com

23 lastline.com

24 bluecoat.com

25 fireeye.com

26 tripwire.com/register/tripwire-enterprise-and-splunk

27 tripwire.com/register/edr-for-dummies

28 tripwire.com/register/meeting-the-true-intent-of-file-integrity-monitoring

29 tripwire.com/scm

30 tripwire.com/securescan

31 tripwire.com/register/responding-to-high-impact-vulnerabilities-are-you-prepared

32 tripwire.com/register/restoring-trust-after-a-breach-which-systems-can-i-trust

33 tripwire.com/register/how-to-protect-against-the-ransomware-epidemic/

34 tripwire.com/register/the-five-stages-of-vulnerability-management-maturity

35 tripwire.com/register/actionable-threat-intelligence-automated-ioc-matching-with-tripwire

36 tripwire.com/register/the-five-stages-of-vulnerability-management-maturity

37 tripwire.com/register/sans-a-maturity-model-for-endpoint-security

38 tripwire.com/solutions/endpoint-detection-and-response