ExtraHop

WHITE PAPER

How Network Detection and Response Makes the CIS Controls Easier

Reveal(x) Support for the CIS Top 20 Critical Security Controls

The CIS Critical Security Controls are meant to help your SOC rise above the noise. This document explains how ExtraHop Reveal(x) supports CIS Controls version 7, including several of the more important—and ambitious—coverage areas for asset cataloguing, administration privilege usage, and limitation of network ports, protocols, and services.

TABLE OF CONTENTS

How Reveal(x) Supports the CIS Top 20 Critical Security Controls 2
- Control 1: Inventory and Control of Hardware Assets 3
- Control 3: Continuous Vulnerability Management 3
- Control 4: Controlled Use of Administrative Privileges 4
- Control 6: Maintenance, Monitoring and Analysis of Audit Logs 4
- Control 8: Malware Defenses 5
- Control 9: Limitation and Control of Network Ports, Protocols, and Services 5
- Control 12: Boundary Defense 6
- Control 13: Data Protection 6
- Control 14: Controlled Access Based on the Need to Know 7
- Control 16: Account Monitoring and Control 7
- Control 19: Incident Response and Management 7

Conclusion 8
Appendix: CIS Controls Mapping 9

How Reveal(x) Supports the CIS Top 20 Critical Security Controls

When you have limited resources and a large attack surface to protect, you need to prioritize your efforts. Otherwise, you risk missing real threats in a noise of alerts. The Critical Security Controls from the Center for Internet Security (CIS) are a prioritized set of actions that organizations can take to rise above the noise and protect themselves and their data from known cyber attack vectors. Controls 1-6 are considered basic, meaning that they are essential first steps to improving your organization's security posture. Controls 7-16 are foundational actions, and Controls 17-20 are organizational actions. The CIS Controls are updated periodically, enabling organizations to revisit their coverage and adapt to changing threat behaviors.

This document shows how ExtraHop Reveal(x) supports CIS Controls version 7, including several of the more important—and ambitious—coverage areas for asset cataloguing, administration privilege usage, and limitation of network ports, protocols, and services.

Reveal(x) offers cloud-native network detection and response (NDR) capabilities for detecting and responding to network threats. In addition, the platform also provides excellent monitoring and auditing capabilities so that you can easily answer questions pertinent to multiple CIS Controls such as:

- Are there rogue or unmanaged devices on the network?
- Who is using administrator credentials, and what are they doing with those credentials?
- Has any device suspiciously elevated their access privileges recently?
- Are any devices using unencrypted FTP to transfer sensitive files?
- Are any devices using the SMBv1 protocol, which is vulnerable to malware exploits?
- Is traffic encrypted in particular subnets when it should be?

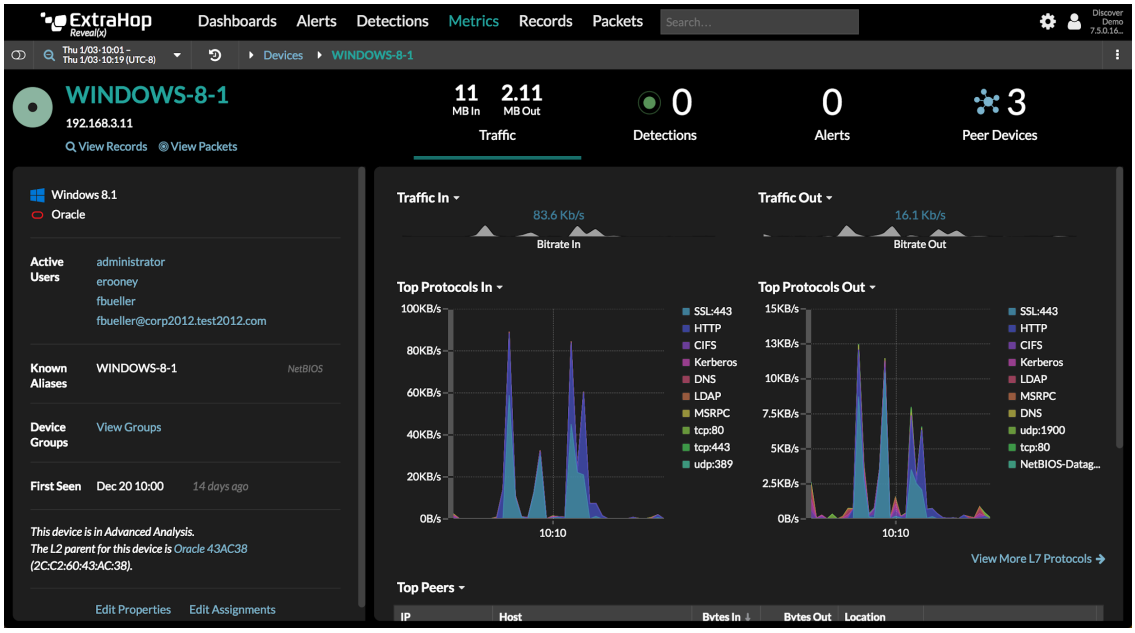
Examples of CIS Control Support

Control 1: Inventory and Control of Hardware Assets

You can't secure what you can't see. That truism is even more relevant in today's sprawling, dynamic environments where traditional methods of asset management cannot keep pace.

Many companies use active, scheduled scanners (Control 1.1), but lack the passive scanning required for Control 1.2 that is core to the Reveal(x) design. Passive monitoring has multiple benefits—it has no performance impact on users or networks, it cannot be detected by attackers, and it is always up-to-date since it is always monitoring network traffic.

Reveal(x) automatically discovers and classifies devices communicating on the network according to their activity. So if a device is functioning as a DNS server, Reveal(x) will categorize it as such automatically. The solution catalogues all activity for every device and extracts contextual details such as the manufacturer, operating system, and user credentials used on the system. This real-time information feeds Reveal(x) analysis of behavior and suspicious activity, and can also be streamed to a CMDB or SIEM for tracking new or rogue devices, or to firewall or network access control devices to enforce access policies.



Reveal(x) automatically discovers and classifies devices on the network by analyzing their communications. You can use this information to find rogue or unmanaged devices, track admin credential usage, or monitor the use of sensitive ports, protocols, and services.

Control 3: Continuous Vulnerability Management

IT Security is a battle determined by speed and knowledge. To succeed, attackers need to identify and take action on vulnerabilities before they are patched or protected with a compensating control. To know more, earlier, defenders need to scan the environment to identify vulnerable systems and protocols. One of the key issues in a continuous vulnerability management program is tracking which devices are scanned. This is because hackers can steal authorized admin account credentials by launching honeypot systems masquerading as a domain controller, SSH server, or web server.

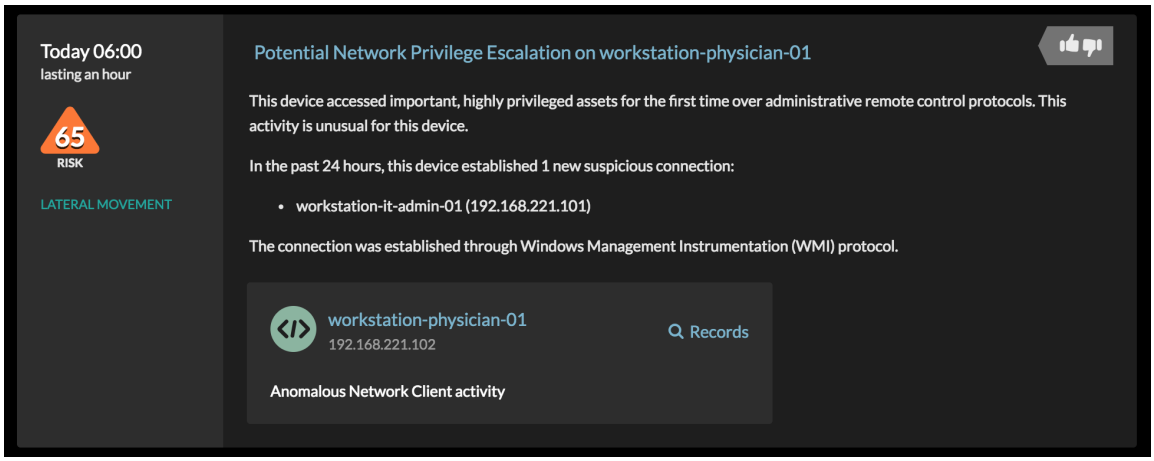
Reveal(x) tracks all scanning activity, including both authorized and unauthorized scans, and highlights devices that are new on the network, indicating a likely honeypot set up by a bad actor or red team. Reveal(x) includes the ability to hide detections from approved scanning devices to more effectively highlight unauthorized scanning activity.

Control 4: Controlled Use of Administrative Privileges

Hackers and insider threats almost always need to escalate their privileges in order to carry out their objectives. For this reason, monitoring and controlling authentication and login functions is of utmost importance.

Attackers have a number of sophisticated techniques to steal credentials and elevate their privileges, making it difficult for Security teams to cover all their bases. Given enough time, a persistent attacker is likely to gain control over a device hosting a user or application with privileged access, putting the burden on Security teams to monitor how privileged accounts are used and detecting suspicious or non-compliant behavior.

Reveal(x) provides continuous, real-time visibility into suspicious and non-compliant use of privileged accounts throughout the environment, enabling Security teams to identify and resolve issues proactively. Reveal(x) also detects privilege escalation using machine learning. Multiple inference models continuously analyze all communications to determine which devices are important and which users are high-privileged, and then flag subtle but suspicious changes in user and device behaviors. In this way, a device that changes behavior to act like an admin will be noticed immediately, and flagged with high risk for instant attention.



Reveal(x) uses machine learning to detect suspicious privilege escalation activity.

Control 6: Maintenance, Monitoring and Analysis of Audit Logs

The average dwell time of attackers in an environment is 101 days, according to FireEye's M-Trends 2018 Report. One of the reasons that attackers can go undetected for so long is because of deficiencies in log record configuration, collection, and analysis—as well as the integrity of logs themselves. Savvy attackers know to cover their tracks by erasing or modifying logs, and by disabling logging after they have compromised a machine.

Security teams rely on their counterparts in IT to ensure that logging is enabled on all systems, and that those logs are aggregated into a central log analysis platform. However, the reality is that not all network activity is logged. DNS activity, which can shed light on attacker techniques, is a case in point—many IT organizations do not log all DNS activity because of the processing and storage resources required. IT teams are also often hesitant to enable logging on database servers for performance reasons.

Reveal(x) analyzes network traffic and extracts transaction records that are immediately indexed and available for ad hoc analysis. These transaction records include Layer 7 (application layer) details such as SMB/CIFS file names, SQL methods and statements, HTTP payload contents, and DNS queries—all automatically correlated for easy search and query. A unique benefit of this wire

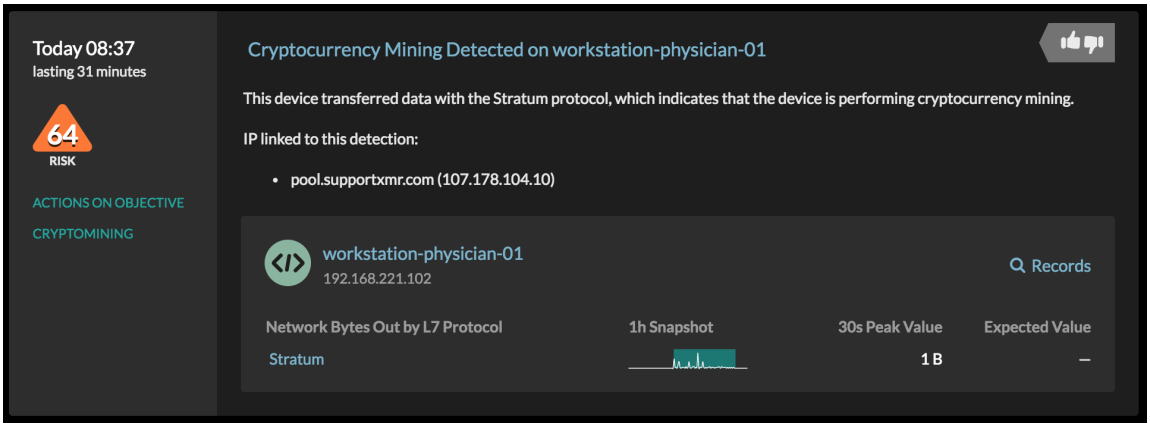
data is that it not susceptible to counter IR activities by an attacker as it cannot be altered or deleted. In fact, attackers will likely not know that this passive observation of their activities is taking place.

All these transaction records from Reveal(x) can be streamed to existing SIEM platforms. Many Reveal(x) customers rely on these transaction records for detection and response, and value the enrichment of and correlation with their existing log data in their SIEM.

Control 8: Malware Defenses

Malicious software is a key piece of any attack from the Internet and enters through a wide variety of vectors, including end-user devices, email attachments, web pages, cloud services, removable media, and more. Endpoint security solutions are essential when protecting against malware, but are frequently compromised. Network detection and response provides a layered defense that can detect attacks that evade or disable endpoint protection.

Unlike network-based malware defenses that rely on signatures alone, Reveal(x) detects malware behavior on the network, from DNS queries to malicious domains and the initial payload delivery, to command and control communications and use of command shells to remotely control compromised systems. In addition to matching network activity with threat intelligence, Reveal(x) also applies machine learning to detect malware behaviors such as ransomware and cryptomining—even those strains that are designed to evade traditional rules- and signature-based detection. Transaction records for all these activities can be streamed to a SIEM for correlation with system logs and alerts, enabling rapid validation and investigation of malware incidents.



Reveal(x) detects malware activity on the network including ransomware and cryptomining.

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

The early days of networking emphasized interoperability, with little thought given to security. Hackers can take advantage of vulnerabilities--in services (poorly configured web servers, mail servers, file and print services, etc.); in newer, poorly implemented protocols such as are often used in IoT devices; and in older protocols such as SMBv1--to spread malware or gain control over remote systems. That is why many organizations control or limit what types of protocols and services can be used in the environment. But setting policy and ensuring that policy is adhered to are two very different things.

Many organizations conduct periodic port scans to detect unauthorized ports, but understanding what services are available in a highly dynamic environment can be challenging. In addition, some software installations will automatically enable services without informing the user or administrator.

Without relying on intrusive scanning, Reveal(x) passively analyzes all network communications so that Security teams can continuously monitor and detect non-compliant ports, protocols, and services in use. This is especially valuable for internal communications among critical assets such as a DMZ-located web server, internal database server, and Kerberos authentication

server, for example. With this visibility, Security teams can work to close vulnerabilities and harden the attack surface of the environment. Reveal(x) can also send information about violations to third-party tools such as firewalls to automatically block that activity.

Control 12: Boundary Defense

Nearly every facet of business operations today relies on the Internet in some fashion, but the Internet is a dangerous place. That's why you need to block access to known malicious IPs and domains, and monitor for suspicious traffic that could indicate attackers performing reconnaissance, remotely controlling compromised systems, or exfiltrating data. If your network is like a castle, then you need to watch on the walls and monitor the traffic coming in and out of the gates.

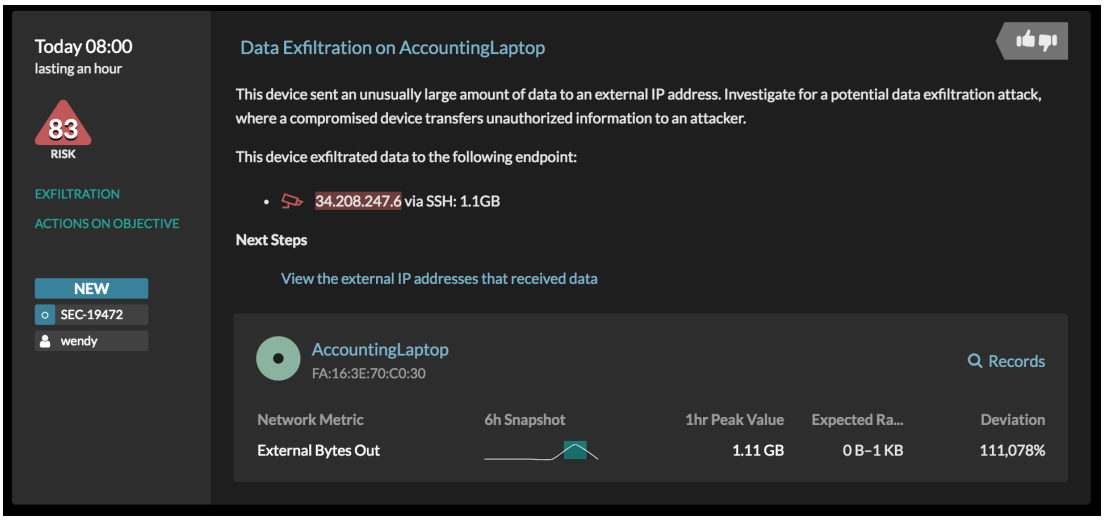
CIS recommends taking advantage of firewalls and threat intelligence to identify and block known-bad IPs and domains, collecting packets and NetFlow records, and deploying network-based IDS to defend network boundaries. These methods are valuable, but managing the disparate tools requires significant resources. In addition, the enterprise environment now spans on-premises and cloud deployments so that the network boundary or perimeter is now larger.

Reveal(x) directly supports important sub-controls for Boundary Defense, offering alternatives to deploying a traditional network-based IDS and capturing ingress and egress packets. Reveal(x) analyzes the contents of transaction payloads, applying both rules and behavioral analysis to detect known and unknown threats. Reveal(x) records all network communications, allowing Security teams to validate that their network policies are working, and also ingests threat intelligence feeds to detect communications with known-bad IPs and domains.

Control 13: Data Protection

Attackers are often after sensitive data for the purposes of espionage, theft, ransom, or destruction. To defend against these attacks, organizations need to identify their critical assets, and limit and monitor access to those systems. Other key defensive activities include encrypting data at rest and monitoring data leaving the network.

Reveal(x) can analyze all ingress and egress traffic on the network to alert on unauthorized use of encryption and use of unauthorized cloud services. In addition, Reveal(x) automatically builds and maintains dynamic profiles of an organization's most critical assets—including databases and file servers—by analyzing privileged access behaviors. This continuously updated view enables Security teams to identify where their sensitive information is and what data access patterns look like.



In addition to monitoring lateral (east-west) traffic within the datacenter, Reveal(x) also analyzes ingress-egress traffic to identify suspicious or malicious activity such as data exfiltration.

Control 14: Controlled Access Based on the Need to Know

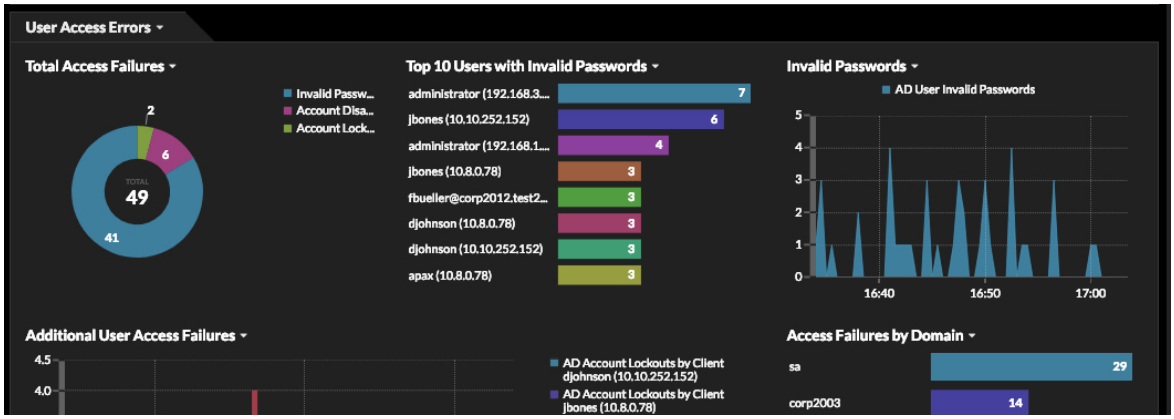
Every organization has a responsibility to control who can access that data to read, modify, or copy it. If their objective is data theft or espionage, then hackers must circumvent those controls without immediate detection. To prevent this from happening, organizations segment network access and encrypt data in flight and at rest. More frequently, however, data is inadvertently leaked through misconfiguration and user error. This is why Security teams need to know what type of data is available through publicly accessible AWS S3 buckets or application APIs.

It's one thing to create policy about data access and segmentation, but it's another thing to make sure that policy is actually working. Reveal(x) simplifies the task of monitoring data access policy compliance. You can easily see what devices and user accounts have read, modified, or otherwise touched file share folders and database tables. In AWS, you can track every bucket and file request to S3, including which users are making those requests and how much data is passed to each user. You can set alerts to know when devices on different VLANs are violating network segmentation policies. And you can continuously audit network communications to ensure that network encryption is turned on for sensitive data in transit.

Control 16: Account Monitoring and Control

Advanced attackers will target legitimate user accounts that they can use to conceal their activities. For this reason, Security teams need to keep track of accounts of contractors, employees, and even Red Team testers and disable those that are no longer needed. Additionally, Security teams must be able to detect suspicious activity by current employees with malicious intent, or former employees that still have access to administrative or other accounts.

Because Reveal(x) parses all LDAP, Kerberos, Diameter, and Radius transactions, Security teams can keep track of all authentication activity and associate user accounts with activity on various devices, helping to monitor the effectiveness of their Identity and Access Management and CASB solutions. The solution also enables Security teams to audit attempts to access deactivated accounts.



Reveal(x) automatically records all notable login activity by parsing LDAP, Kerberos, Diameter, and Radius transactions.

Control 19: Incident Response and Management

Having an incident response plan in place can dramatically lessen the impact of a security incident. One of the important aspects of incident response is well-understood runbooks. With guided investigations to help responders take the correct actions quickly, Reveal(x) can fit into existing incident response strategies and enhance analyst capabilities when investigating the scope of an incident, establishing a root cause, eradicating the threat, and performing network forensics. Reveal(x) can also improve the skills of junior analysts and equip newly recruited team members be more effective.

Conclusion

The CIS Top 20 Controls provide a framework for prioritizing projects and actions, and rising above the noise of random SOC activity. Adding a network-based view of activity in your environment can be one of the most efficient ways of quickly achieving visibility. Reveal(x) offers extremely scalable and deep analysis of network traffic, including details that enable organizations to support some of the most far-reaching and ambitious controls, including Inventory and Control of Hardware Assets, Controlled Use of Administrative Privileges, and Account Monitoring and Control.

For more information about Reveal(x) technology including deployment, download the Reveal(x) Technical Architecture Whitepaper.

Appendix: CIS Controls Mapping

ExtraHop Reveal(x) provides support for a broad selection of CIS Controls, but the level of support varies. The tables below include all the areas where Reveal(x) does provide support along with a brief explanation.

Significant support

Limited support

Compensating support

CIS Sub-Control	Title	Description	Reveal(x) Support
Inventory and Control of Hardware Assets			
1.2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	Reveal(x) automatically discovers newly connected devices through passive monitoring and can connect to asset inventory or active scanning systems through open APIs.
1.3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	Reveal(x) parses DHCP to automatically detect devices as they migrate, detect a new DHCP request and response, and initiate a workflow through an orchestration tool.
1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	Reveal(x) continuously and automatically discovers new network-connected assets and classifies their asset type based on behavior.
1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	Reveal(x) automatically provides the network address, hardware address, and machine name for new active network-connected devices.
1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	Reveal(x) can enable this workflow when discovering a newly connected device (requires vendor with open API and host firewall or NAC function).
1.7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	Reveal(x) can enable this workflow when discovering a newly connected device (requires vendor with open API and host firewall or NAC function).
Continuous Vulnerability Management			
3.1	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.	Reveal(x) can readily detect and identify specific vulnerable protocols or cipher suites in use.

3.2	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.	Reveal(x) can automatically detect systems where the required agents need to be applied to ensure complete coverage. In addition, Reveal(x) highlights new devices being scanned, which may be honeypot systems set up by hackers or red teams to steal credentials as the scanner authenticates in the system.
3.3	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.	Reveal(x) can alert and report on account and machine activity to ensure policy adherence.

Controlled Use of Administrative Privileges			
4.1	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Reveal(x) detects privileged user escalation and has the ability to alert on group changes.
4.3	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	Reveal(x) provides audit and reporting capabilities for administrative account usage.
4.6	Use of Dedicated Machines For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.	Reveal(x) can flag unexpected N-S traffic, such as from an external user to the machine dedicated to administrative tasks. In addition, Reveal(x) can detect abnormal connections to administrative systems from other internal network segments (E-W traffic).
4.8	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	Reveal(x) detects privileged credential escalation attacks through machine learning-driven behavioral analysis.
4.9	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	Reveal(x) detects anomalous administrative account behavior and can provide dashboards to provide real-time visibility to admin account activity.

Maintenance, Monitoring and Analysis of Audit Logs			
6.1	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	Reveal(x) can audit for NTP sources for each device on the network and can alert if it is ever less than three.
6.2	Activate audit logging	Ensure that local logging has been enabled on all systems and networking devices.	The transaction record capabilities of Reveal(x) augment system log data in SIEMs, filling in gaps and serving as an objective data source off the wire.
6.3	Enable Detailed Logging	Enable system logging to include detailed information such as a event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	Reveal(x) transaction records contain detailed information including Layer 7 application details such as SQL statement, methods, and errors.

6.5	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.	Reveal(x) provides real-time audit capabilities to discover devices that are not emitting syslog or from which the Security team is unable to collect logs.
6.6	Deploy SIEM or Log Analytic tool	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.	The transaction record capabilities of Reveal(x) augment system log data in SIEMs, filling in gaps and serving as an objective data source off the wire.
6.7	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	Reveal(x) applies machine learning to surface anomalous activity and behaviors as they happen. In addition, Reveal(x) enables Security teams to set up rules-based alerts to catch specific suspicious activity.
6.8	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.	Reveal(x) can be used to not only detect behavioral anomalies, but to also proactively search the entire environment to discover sources of false positives (e.g. expired certificates) as well as hunt for threats.

Malware Defenses			
8.1	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	Reveal(x) adds an additional layer of defense with a cloud-based behavioral detection engine that is updated automatically by the ExtraHop threat research team. This approach adds detection of malware behavior in internal (East-West) traffic.
8.6	Centralize Anti-malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	Any behavioral anomaly detections discovered by Reveal(x) can be analyzed in detail (including forensic packet capture of the malware) or sent to a SIEM for alerting and correlation with other data sources.
8.7	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	Reveal(x) records all DNS traffic on the network and cross-references against known malicious domains listed in STIX threat intelligence feeds.
8.8	Enable Command-line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.	Reveal(x) detects all command shell activity and can either write logs to a SIEM or generate reports.

Limitation and Control of Network Ports, Protocols, and Services			
9.1	Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.	Reveal(x) enables detection of active ports, services, and protocols and can hand off details via REST APIs to your asset inventory.
9.2	Ensure Only Approved Ports, Protocols and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	Reveal(x) detects unapproved active ports, services, and protocols and can enforce an action via REST APIs to other third-party tools.
9.4	Apply Host-based Firewalls or Port Filtering	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Reveal(x) monitors port usage and then alerts and reports on violations.

9.5	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.	Reveal(x) is not an application firewall, but monitors all network traffic and can detect unauthorized traffic, record this activity, and enforce an action via REST API to a third-party tool to block.

Boundary Defense			
12.1	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.	Reveal(x) can identify network boundaries and alert if changes are made.
12.2	Scan for Unauthorized Connections across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	Reveal(x) passively and continuously detects unauthorized connections across policy-defined network boundaries.
12.3	Deny Communications with Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.	Reveal(x) can ingest existing threat intelligence feeds from a customer and identify connections to known malicious or unused Internet IP addresses and then send a REST API call to initiate an action by a NAC or firewall.
12.4	Deny Communication over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	Reveal(x) monitors all network traffic from all devices and sends a REST API call to a third-party tool to deny communication activity over unauthorized ports.
12.5	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.	Reveal(x) can record packets as well as the metrics and transaction records for traffic passing through network boundaries.
12.6	Deploy Network-based IDS Sensor	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	Reveal(x) performs full payload analysis on all network traffic to detect behavioral anomalies without relying on signatures to detect threats.
12.8	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.	Reveal(x) does not collect NetFlow or logs but it can monitor the actual network traffic itself and write logs to a SIEM.
12.10	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.	Reveal(x) can detect and alert on SSL/TLS traffic not going through the proxy.
12.11	Require All Remote Login to Use Multi-factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	Reveal(x) can audit and report on who is logging in, to what, when, and from where.

Data Protection			
13.1	Maintain an Inventory Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.	Reveal(x) auto discovers and classifies all devices on a network and heuristically determines which of those assets are critical and then monitors all network traffic to provide visibility into how sensitive information is being accessed.

13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.	Reveal(x) audits data and system usage and can be used to determine what systems should be removed.
13.3	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	While Reveal(x) cannot block the actual transfer, it has various integration partnerships that could block unauthorized data transfer upon detection. Reveal(x) can also detect anomalous activity that may precede a potential data exfiltration scenario.
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.	Reveal(x) provides the ability to audit cloud application usage, a "CASB-lite" (audit only) functionality.
13.5	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	Reveal(x) monitors all traffic, including traffic leaving the network and can audit ciphers to detect unauthorized encrypted traffic. If desired, Reveal(x) can initiate blocking actions at the firewall through its REST API.

Controlled Access Based on the Need to Know			
14.1	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	Reveal(x) auto-discovers and classifies critical assets as well as application dependencies to simplify segmenting a network.
14.2	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	Reveal(x) monitors all network communications and enables a real-time auditing capability to ensure compliance. Behavioral anomaly detection would also detect anomalous access patterns between certain assets.
14.3	Disable Workstation to Workstation Communication	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or microsegmentation.	Reveal(x) does not actively disable workstations but can detect and report on device activity. Application dependency mapping is also another area where Reveal(x) provides visibility, enabling Security teams to understand baseline activity.
14.4	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	Reveal(x) can audit network communications to provide an understanding of what information is being transmitted and what encryption ciphers are used.
14.5	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider and update the organization's sensitive information inventory.	Reveal(x) can monitor and audit what information is transmitted across an environment and provide an understanding of where this information is stored.
14.6	Protect Information through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	Reveal(x) monitors all assets in an environment and can show who is accessing those systems, alert on unauthorized access and determine if that behavior is normal or anomalous.
14.7	Enforce Access Control to Data through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.	Reveal(x) can audit access control systems and how data is being used.

14.9	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	Reveal(x) can provide visibility into communications for critical assets like databases and network storage and file shares to augment SIEM platforms.

Account Monitoring and Control			
16.1	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.	Reveal(x) can provide visibility into authentication systems using these protocols: LDAP, Kerberos, AAA, RADIUS
16.12	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.	Reveal(x) tracks attempts to access deactivated accounts as well as detects anomalous login behavior, such as potential brute-force attempts.
16.13	Alert on Account Login Behavior Deviation	Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.	Reveal(x) detects and alerts on abnormal login behavior through peer group analysis, and also ties users to the various devices they have logged into.

Incident Response and Management			
19.1	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.	The Reveal(x) incident response workflow streamlines investigations and can be incorporated into an existing incident response strategy.
19.7	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.	The Reveal(x) platform can enhance existing incident response strategies and enhance incident responders' capabilities.

ABOUT EXTRAHOP

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions in real time and applies advanced machine learning to help you investigate threats, ensure the delivery of critical applications, and protect your investment in the cloud.

ExtraHop Networks, Inc.
520 Pike Street, Suite 1600
Seattle, WA 98101 USA

http://www.extrahop.com/
info@extrahop.com
T 877-333-9872
F 206-274-6393