EXTRAHOP

ExtraHop Threat Investigation Guide

Current Version: 1.0

The ExtraHop Threat Investigation Guide is designed to provide hands-on insights, best practices, and actionable strategies for optimizing network performance, enhancing security posture, and maximizing the value of your ExtraHop deployment. It is intended for practitioners who manage on-premises systems or leverage ExtraHop's RevealX™ 360 SaaS solution, equipping them with the knowledge needed to monitor, detect, and respond effectively in today's dynamic IT environments.

The document flows through a structured incident response lifecycle, mirroring the ExtraHop Investigation Cycle (as depicted in Appendix A). The key stages covered are:

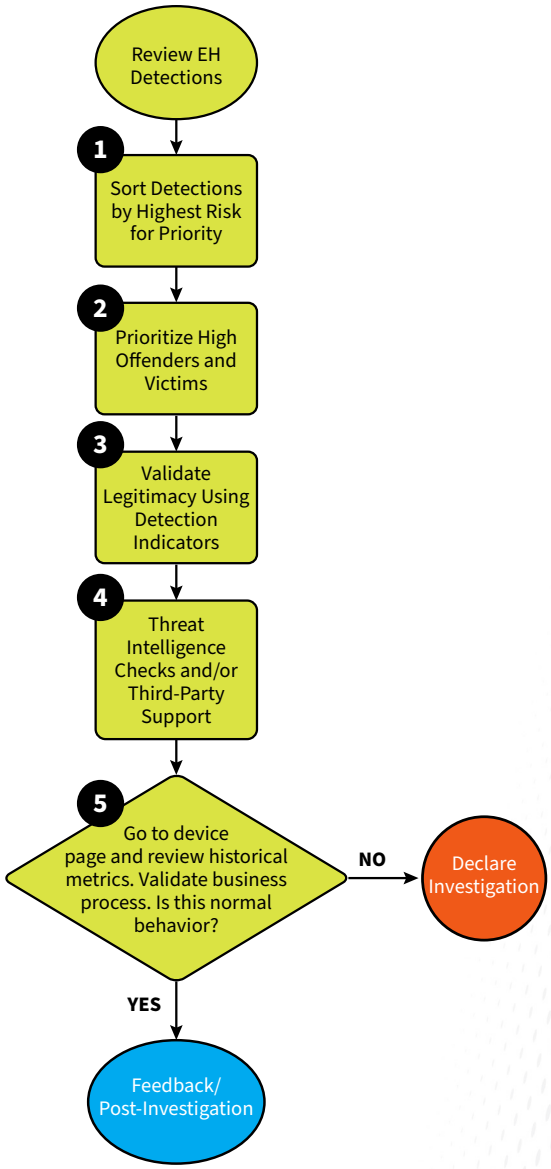
1. **Initial Review**
   Begin by reviewing ExtraHop detections, prioritizing based on risk, and validating legitimacy using detection indicators and threat intelligence.
2. **Declare Investigation**
   Determine if a detected activity warrants an investigation, relating it to existing cases or creating new investigations, and classifying its priority.
3. **Determine Investigation Scope**
   Open the victim device page to document peers and traffic, assess impact, and validate findings to define the investigation's breadth.
4. **Collect and Preserve Data**
   Generate reports, export records and packets, and preserve conversations and activity maps for historical reference.
5. **Perform Technical Analysis**
   Correlate data to distinguish normal from malicious activity, identify attack chains, and drill into suspicious traffic for IoC details.
6. **Contain and Remediate**
   This stage focuses on classifying the activity's intent, scoping and containing the compromise, and validating remediation.
7. **Feedback / Post-Investigation**
   Conclude the investigation, update rules, document findings, and conduct security awareness training to improve future responses.

This guide aims to be a comprehensive resource for navigating and responding to threats using ExtraHop, from initial detection to post-investigation review.

Table of Contents

1. Initial Review

Review ExtraHop detections by sorting for highest risk, prioritize key offenders and victims, validate legitimacy using detection indicators and threat intelligence, then check the device page to determine if the activity is normal business behavior, if not, declare an investigation.



1. Sort detections by highest risk for priority

By sorting with the highest risk score, you are prioritizing the detections that could have the most impact to your business.

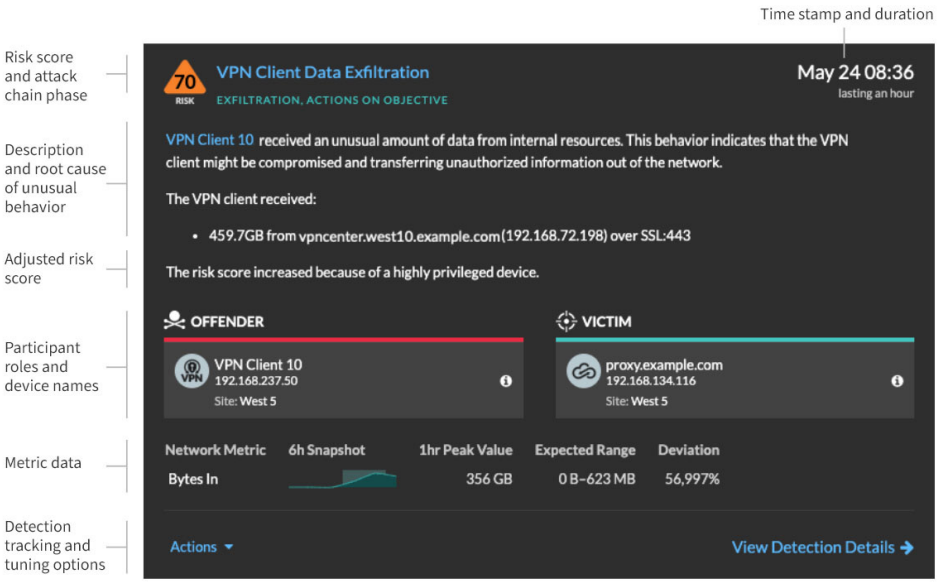
2. Prioritize high offenders and victims

Frequent/high offenders or victims are devices that have been seen in multiple detections and/or across multiple attack categories. These should be looked at first.

3. Validate legitimacy using detection indicators

Indicators to keep an eye on:

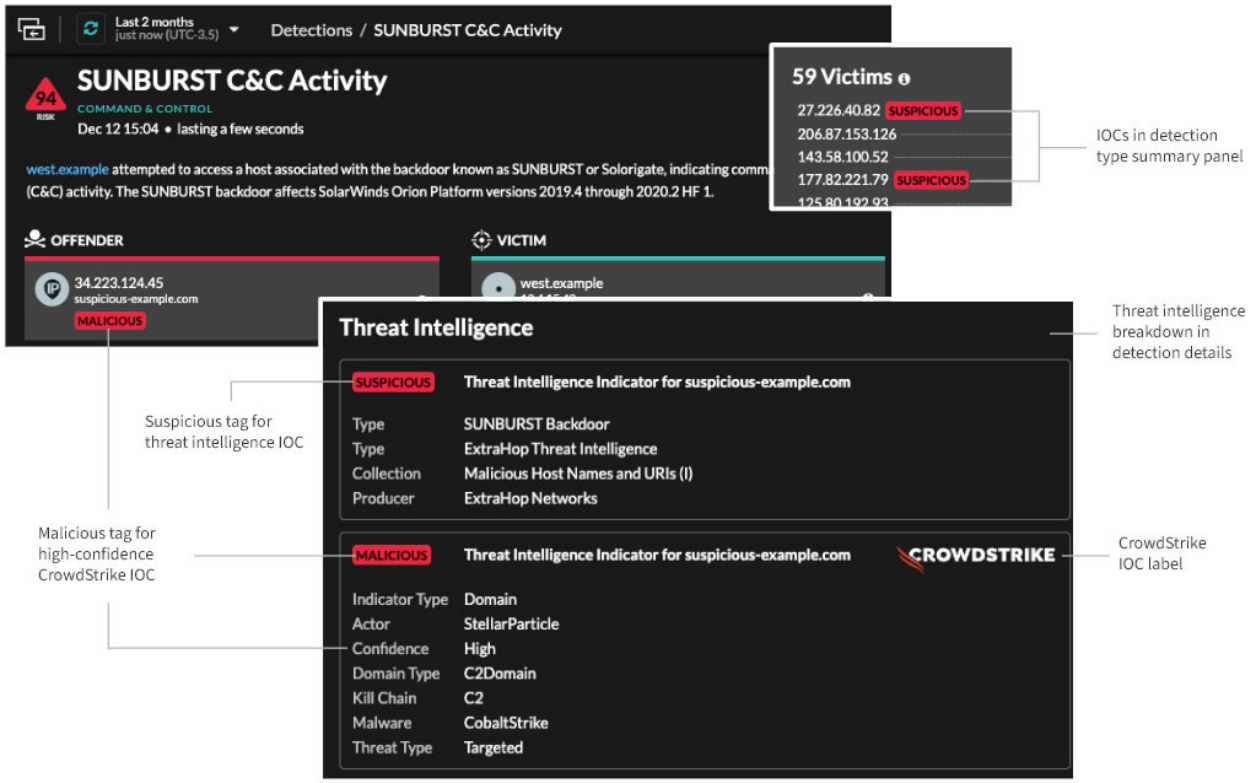
- Event Type, Risk Score, Offender/Victim (internal/external), Device IP, Protocol, Port, Duration, Start/End Time, Device Overview
- ML-Based: Deviation, Additional Metric, Snapshot Chart
- View Detection Details, Check Records/Packets, Related Detections with Timeline
- Visit Records page within the same time interval of the detection for further analysis



4. Threat Intelligence checks and/or third-party support

Leverage your existing Threat Intelligence or 3rd party (i.e., MSSP) to assist in reviewing certain IoCs. Did this come from a suspicious URL or IP? Has this been seen before in other environments? Correlating network traffic with known threat indicators to detect targeted attacks.

- Participants matching threat collections are tagged as Suspicious (or Malicious for high-confidence CrowdStrike IoCs) in detections, summaries, and records, with suspicious entries marked by a camera icon.



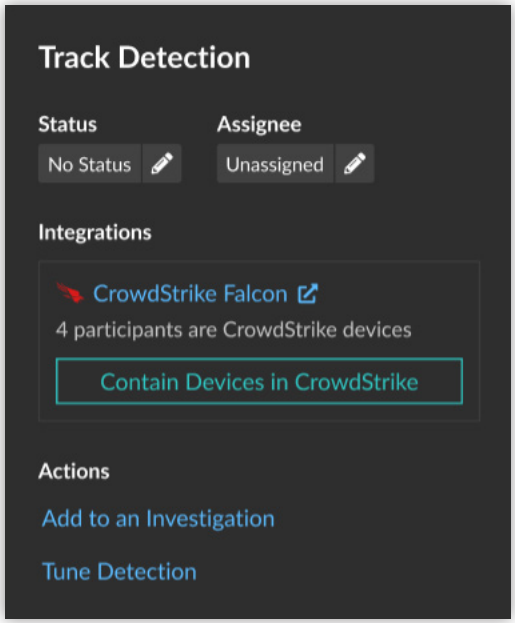
5. Go to the device page and review historical metrics

By navigating to the device details of the victim or offender, you can get an understanding of the context of the detection, such as, what else was happening at that time? Is this common in prior weeks as legitimate business transactions? Is there anything odd or abnormal about this transaction(s)?

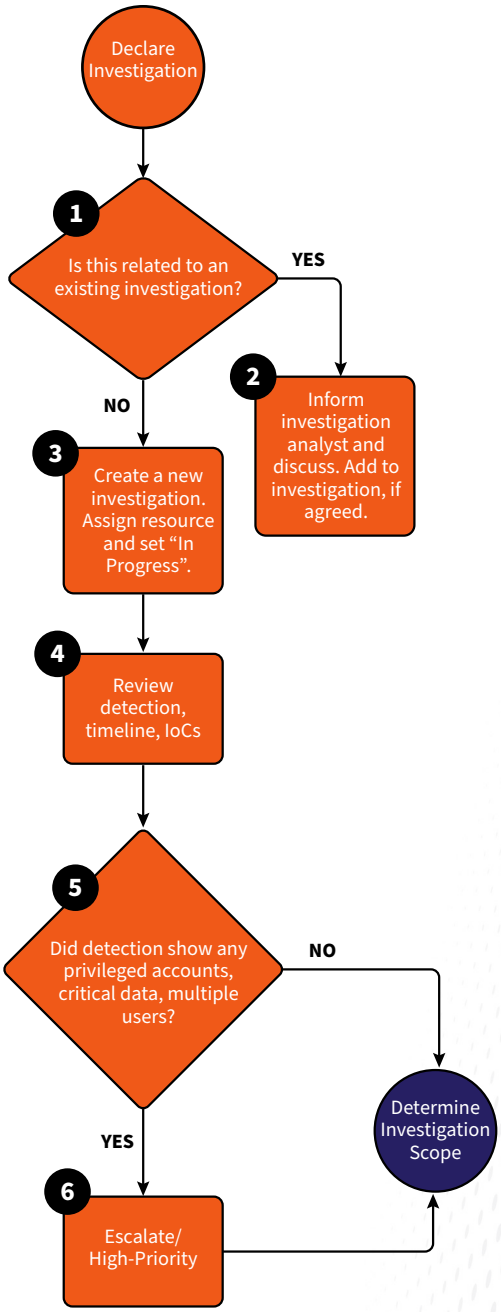
2. Declare Investigation

To declare an investigation, first determine if it relates to an existing case, consult with the investigation analyst to add it or create a new investigation, review the detection timeline and IoCs, check for privileged accounts or critical data exposure, then classify priority and determine the investigation scope.

Note: Machine learning-based detections allow you to investigate and respond to incidents faster.



Screenshot: Detection assign, update status, and add to investigation.



1. **Is this related to an existing investigation?**
   - Anomaly Detection: Investigate whether the detected behavior points to a low-priority issue or a potential security risk. You can start your investigation directly from the detection card.
   - Use Case - Find External Traffic
2. **If there is an existing related investigation, inform the Investigation Analyst and discuss.** Add to the investigation, if agreed.
3. **Create a New Investigation.** Assign Resource and Set "In Progress".
4. **Review, Assign, and View Details on Detection Card:** Understand the details of the participants and other parameters.
5. **Did detection show any privileged account usage, business-critical data, or multiple users?**

3. Determine Investigation Scope

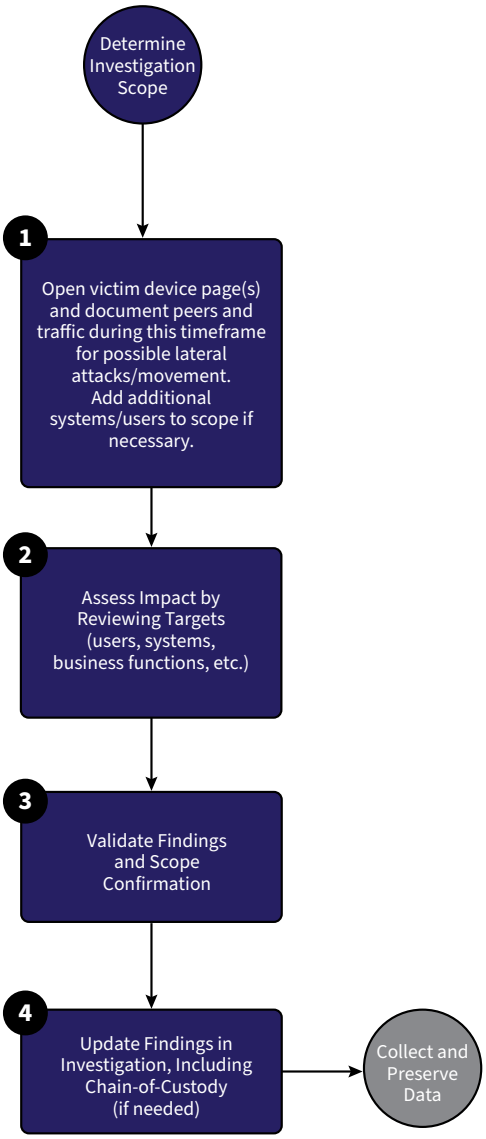
To determine the investigation scope, open the victim device page to document peers and traffic for lateral movement, assess the impact on targets, validate findings, and update the investigation with a chain-of-custody, if needed.

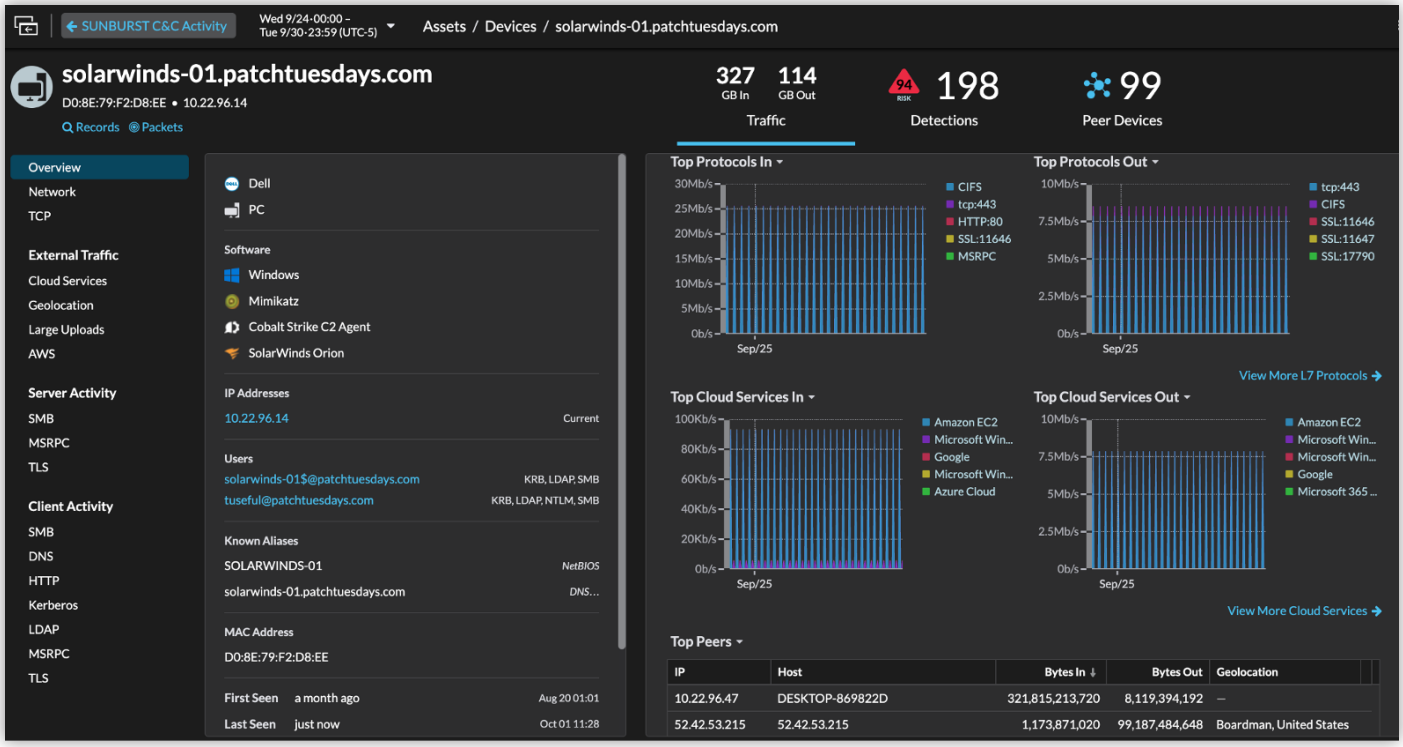
1. **Open the victim device page(s)** and document all peers and traffic during the relevant timeframe to identify potential lateral movement or attacks, expanding the investigation scope to include additional systems or users as necessary.

2. **Assess impact by reviewing affected targets,** including users, systems, and business functions. Assets, Peers, Records, Protocols, and/or PCAP.
   - CIFS, LDAP, DNS, DHCP, HTTP headers.
   - SIEM, SOAR, EDR: Cross-check with the integrated or supplemental tool data.
   - Ask the questions, "What business function does this system do?" "What user is being exploited or attempted?" "If there are other systems in the detection timeline, are they all related to the same function?"

3. **Validate all findings and confirm the investigation scope.**

4. **Update the investigation with documented findings**, including chain-of-custody procedures if required.

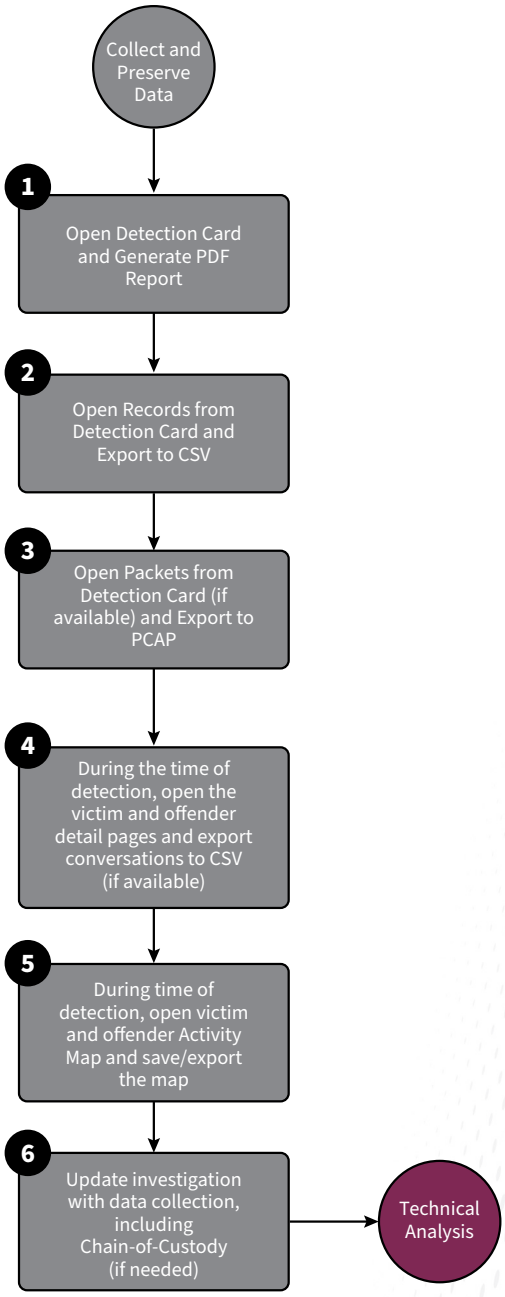




Screenshot: View of device page to review detailed analysis of traffic and behaviors.

4. Collect and Preserve Data

To collect and preserve data, generate a PDF report from the detection card, export records and available packets to CSV and PCAP files, export victim and offender conversations and activity maps from the detection timeframe, and update the investigation with chain-of-custody documentation. This is meant for historical reference and preservation.



1. **Open Detection Card and Generate PDF Report**

2. **Open Records from Detection Card and Export to CSV**

   - Records/Log Analysis: Correlating logs from various sources to identify attack vectors and compromised systems.
     - Records: Record type, grouping, fields, and time interval
     - DB failures: [Errors exists] + [DB Login Failure] + [RecordType-DB] Failed login attempts to databases and other database error messages
     - External SSH: [ExternalConnection=True] + [ServerPort≠22] + [RecordType-SSHOpen&SSHClose] SSH connections coming from outside your network that are using a non-standard port

3. **Open Packets from Detection Card (if available) and Export to PCAP**

   - Capture Network Traffic: Collect PCAP data, monitor real-time traffic, and identify anomalies while correlating findings.
   - Analyze PCAP: Dissecting network packets to uncover hidden threats and anomalies.
     - Analyze packets via ExtraHop packet analysis tool on the UI
     - Packets: Retrieve PCAP and/or session keys after filtering based on IP, MAC, Port, Berkeley Packet Filtering (BPF), and more

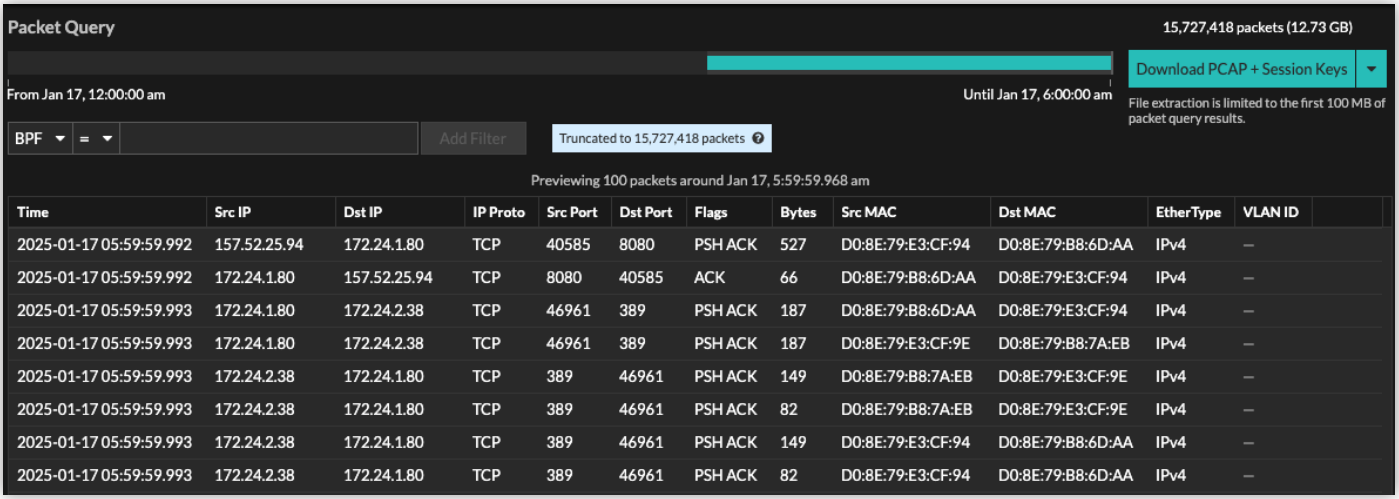
4. **During the time of detection, open the victim and offender detail pages and export conversations to CSV** (if available)

   - Go to Device Overview → Peer IPs → Conversations. Upper-right corner, click kabob to display “export to CSV”.

5. **During time of detection, open victim and offender Activity Map and save/export the map**

6. **Update Investigation with data collection, including Chain-of-Custody** (if needed)

   - Audit Log: Inspect ExtraHop system operations.

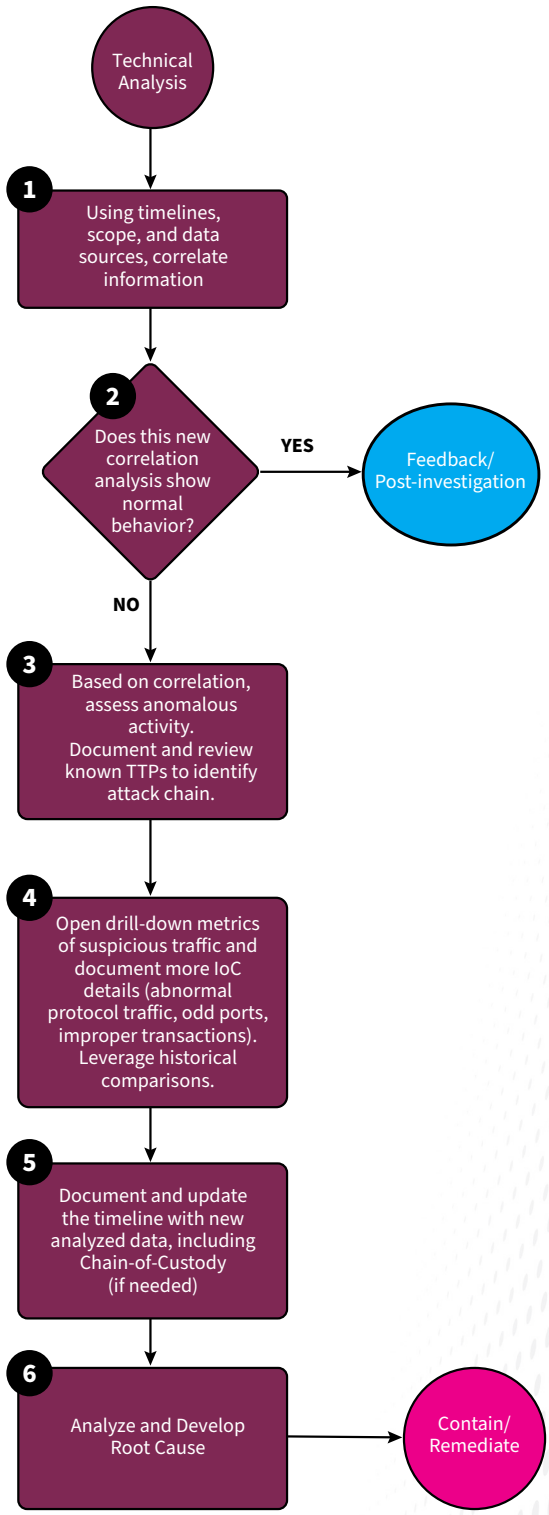


Time	Src IP	Dst IP	IP Proto	Src Port	Dst Port	Flags	Bytes	Src MAC	Dst MAC	EtherType	VLAN ID
2025-01-17 05:59:59.992	157.52.25.94	172.24.1.80	TCP	40585	8080	PSH ACK	527	D0:8E:79:E3:CF:94	D0:8E:79:B8:6D:AA	IPv4	–
2025-01-17 05:59:59.992	172.24.1.80	157.52.25.94	TCP	8080	40585	ACK	66	D0:8E:79:B8:6D:AA	D0:8E:79:E3:CF:94	IPv4	–
2025-01-17 05:59:59.993	172.24.1.80	172.24.2.38	TCP	46961	389	PSH ACK	187	D0:8E:79:B8:6D:AA	D0:8E:79:E3:CF:94	IPv4	–
2025-01-17 05:59:59.993	172.24.1.80	172.24.2.38	TCP	46961	389	PSH ACK	187	D0:8E:79:E3:CF:9E	D0:8E:79:B8:7A:EB	IPv4	–
2025-01-17 05:59:59.993	172.24.2.38	172.24.1.80	TCP	389	46961	PSH ACK	149	D0:8E:79:B8:7A:EB	D0:8E:79:E3:CF:9E	IPv4	–
2025-01-17 05:59:59.993	172.24.2.38	172.24.1.80	TCP	389	46961	PSH ACK	82	D0:8E:79:B8:7A:EB	D0:8E:79:E3:CF:9E	IPv4	–
2025-01-17 05:59:59.993	172.24.2.38	172.24.1.80	TCP	389	46961	PSH ACK	149	D0:8E:79:E3:CF:94	D0:8E:79:B8:6D:AA	IPv4	–
2025-01-17 05:59:59.993	172.24.2.38	172.24.1.80	TCP	389	46961	PSH ACK	82	D0:8E:79:E3:CF:94	D0:8E:79:B8:6D:AA	IPv4	–

Screenshot: PCAP Query to download for preservation.

5. Perform Technical Analysis

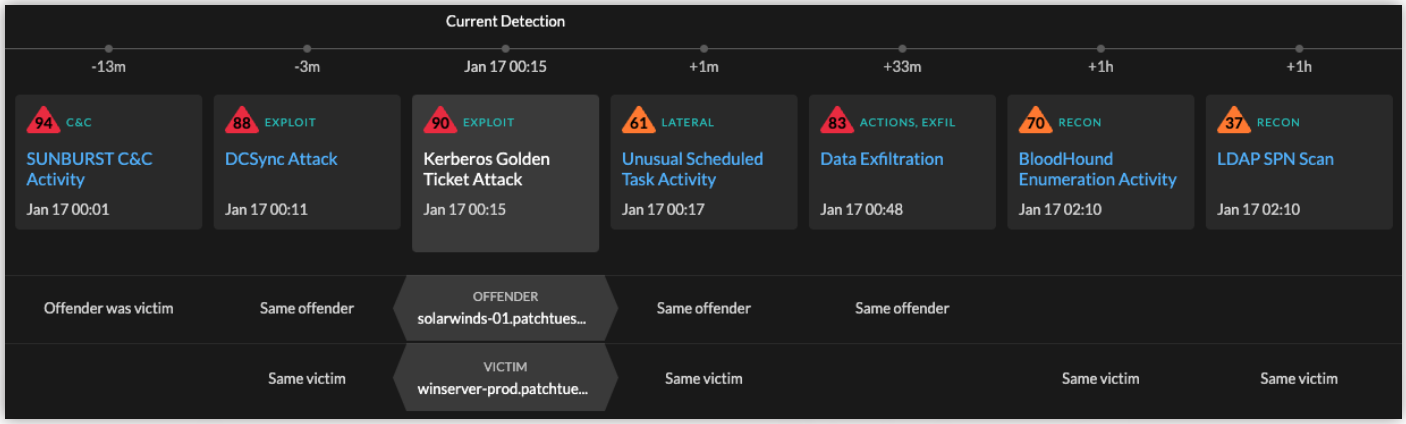
During technical analysis, correlate timeline and scope data to distinguish normal behavior from malicious activity, assess randomness and TTPs to identify the attack chain, drill into suspicious traffic metrics for IoC details using historical comparisons, then document findings and determine root cause.



1. **Using timelines, scope, and data sources, correlate information**
   - Document Timeline and Steps: Record, in chronological order, the actions taken to detect, contain, and remediate the incident. This helps to ensure accuracy and supports post-investigation analysis.
   - Containment: Isolating infected systems to prevent further damage.
     - Contain through ExtraHop
     - Contain on CrowdStrike or other tool
2. **Does this correlation analysis show normal behavior?**
3. **Based on correlation, assess anomalous activity. Document and review known TTPs to identify attack chains**
4. **Open drill-down metrics of suspicious traffic and document IoC details, including** abnormal protocol traffic, odd ports, and improper transactions while leveraging historical comparisons.
   - Drill Down by Metrics, Records, Protocols, Peers, Assets: Drill down from a dashboard or protocol page, on network capture and VLAN metrics, from a detection and from an alert.
   - Deep Dive into Metrics: Explore how metric data changed over time for a targeted system.
     - Use Case - Metrics to Investigate DNS Failures
5. **Document and update the timeline with new analyzed data, including Chain-of-Custody** (if needed)

6. Analyze and develop root cause

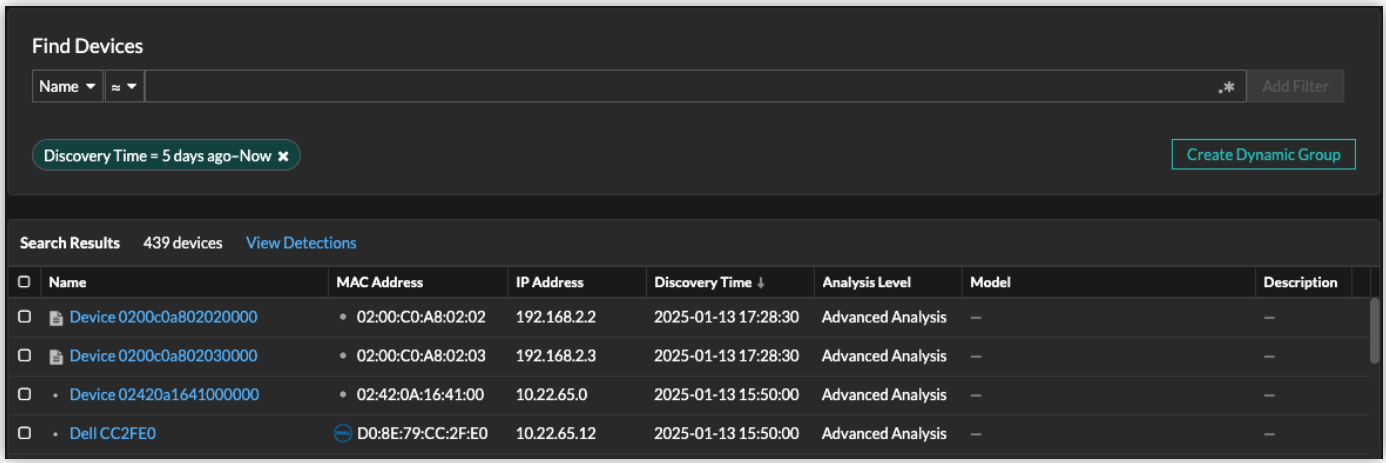
- Anomaly Detection: Investigate whether the detected behavior points to a low-priority issue or a potential security risk. You can start your investigation directly from the detection card.
  - Use Case - Find External Traffic
- Collect Further Data: i.e., Perimeter: Collect further evidence from the perimeter devices: firewalls, intrusion detection systems, and proxy logs that could give traces to external threats and entry points.



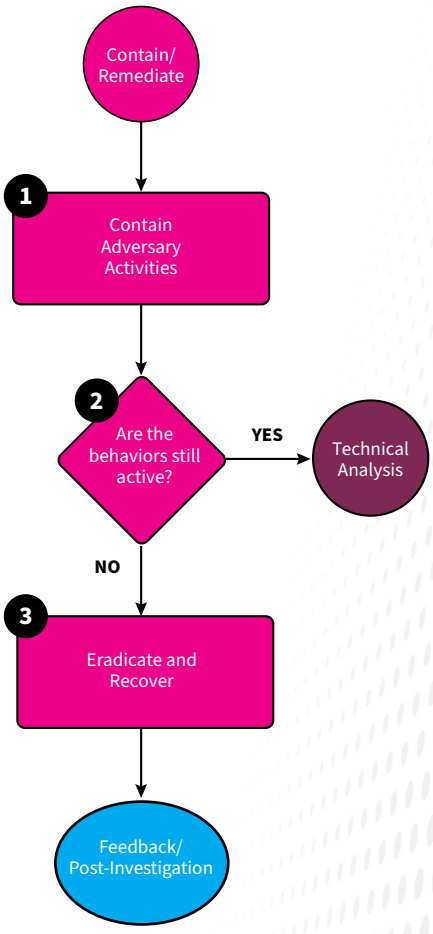
Screenshot: Detection Timeline

6. Contain and Remediate

The incident response lifecycle involves classifying the activity's intent, scoping and containing the compromise through ExtraHop integrations, and concluding with rigorous remediation validation and post-investigation reporting.



- Determine Nature of Activity: Is the detected activity Malicious, Benign, or Incidental?
- Update Investigation Scope: Based on the evaluation, refine the investigation by isolating the compromised hosts and tracing the attack path.
- Leverage ExtraHop: Use ExtraHop's live search and forensics to understand the full scope of interaction with the compromised asset.
- Integrate & Isolate: Use ExtraHop integrations (e.g., with your firewall or NAC) to quarantine malicious traffic or isolate compromised hosts.
- Block with IDS/IPS: Immediately push rules to firewalls and Intrusion Prevention Systems to block the identified attack patterns.
- Monitor for Lateral Movement: Enhance monitoring in ExtraHop for any follow-on activity or lateral movement from the contained asset.
- Validate Remediation: Use ExtraHop to continuously check for a recurrence of the malicious activity to ensure remediation was successful.
- Conduct Post-Investigation Review: Analyze the incident to identify lessons learned and improve security practices and ExtraHop detection rules.
- Review Security Operations Report: Sharing insights with the security community to help prevent future attacks. ExtraHop SOR provides a summary of the top detections and risks to your network for the time interval that you specify.
- Schedule Dashboard Reports: Obtain the preview of the selected dashboard for the time interval that you specify.



7. Feedback / Post-Investigation

During feedback and post-investigation review, close the investigation, create or update notification rules, document TTPs and IoCs, update network localities and tuning rules, create custom devices or detections if needed, and conduct security awareness training.

1. **Close Detection / Investigation**

2. **Create/Update Notification Rules**: Stay informed about key events on your ExtraHop system through email notifications and integrations with external services.

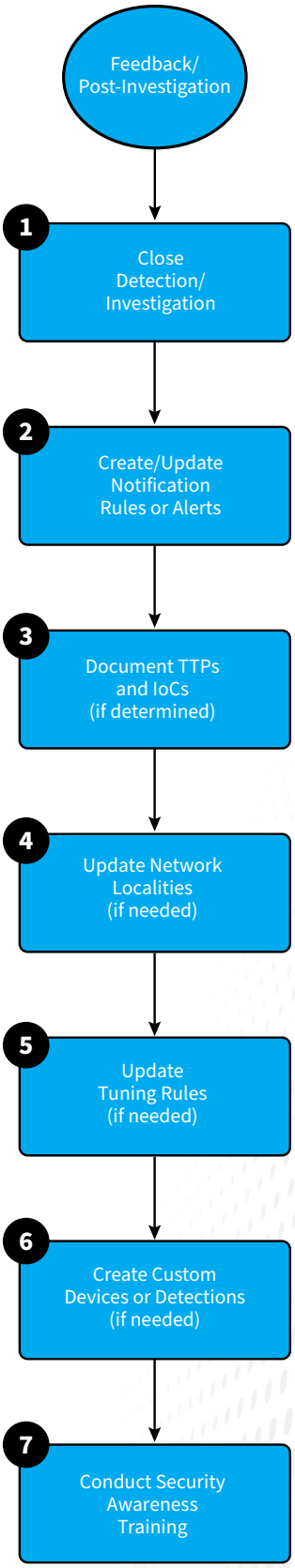
3. **Document TTPs and IoCs (if determined)**
   - Enhance Threat Intelligence
     - Enhancing Threat Intelligence: Stay up-to-date with the latest threat intelligence feeds and share select data with ExtraHop for review against a larger collection of CrowdStrike TI.
     - Update and refine incident response plans.

4. **Update Network Localities**: Classify traffic from IP addresses or CIDR blocks as internal or external. Name each locality, such as "DMZ" or "Guest Network," and use it to filter devices and records.
   - Update Analysis Priorities: Prioritize your assets based on the importance of devices, such as Active Directories, servers, endpoints, or applications, and their roles in the organization

5. **Update Tuning Rules (if needed).** Refining detection rules to improve accuracy and reduce false positives.
   - Update Tuning Parameters: Improve metrics and suppress low-value detections from ever being generated.

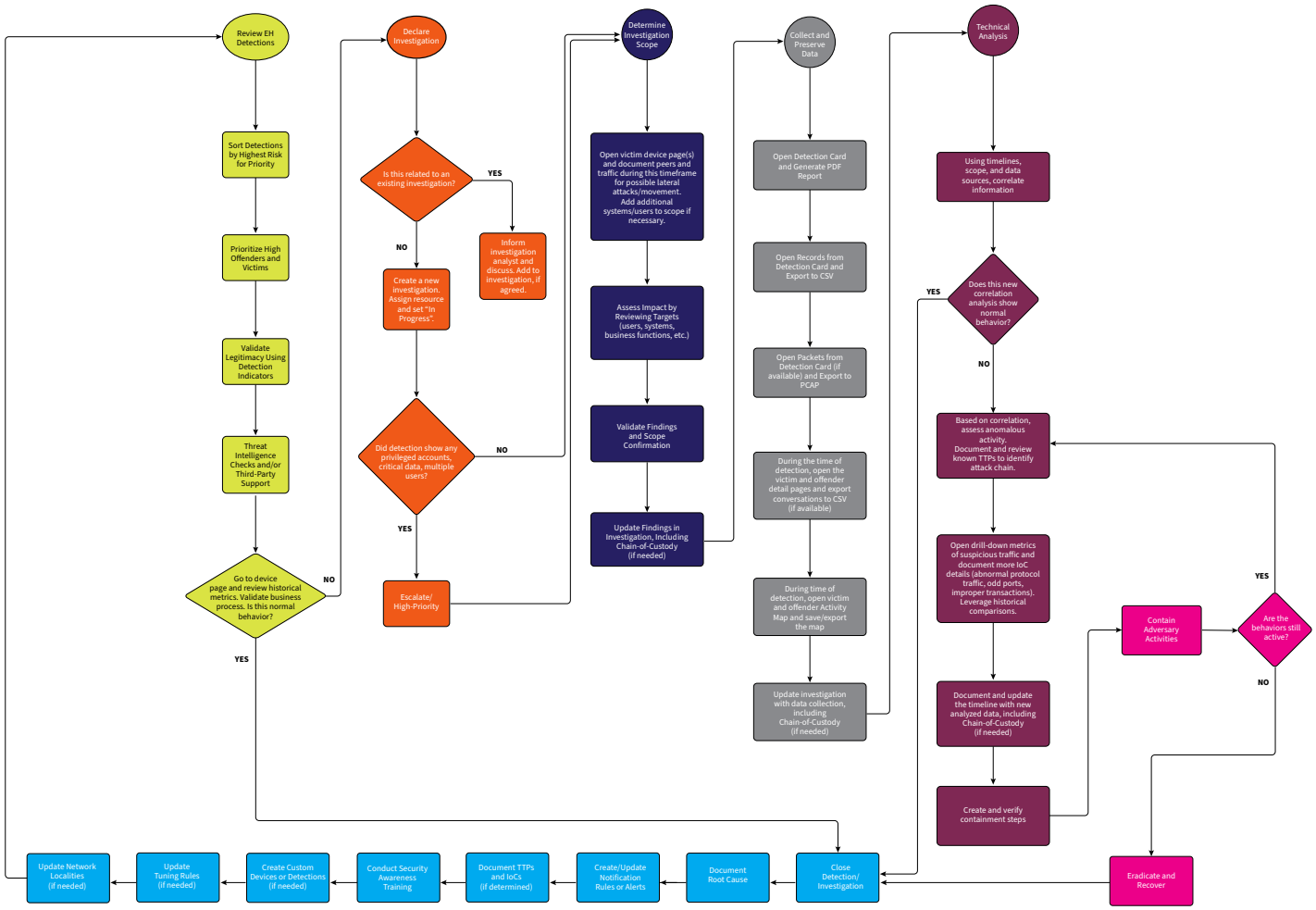
6. **Create Custom Devices or Detections**: Monitor network segmentation with custom detections to help improve security by only allowing certain clients to access servers that contain sensitive data.
   - Create Device Tags: Differentiate devices on the ExtraHop system that share a common attribute or characteristic.

7. **Conduct Security Awareness Training**
   - Educating employees about security best practices to minimize human error. ExtraHop offers various learning materials that cover security best practices.



Appendix A: ExtraHop Investigation Cycle

Appendix B: ExtraHop Investigation Workflow



ExtraHop Threat Investigation Key

- Initial Review
- Declare Investigation
- Investigation Scope
- Data Collection and Preservation
- Technical Analysis
- Contain / Remediate / Recover
- Feedback / Post-Investigation

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP®

info@extrahop.com
extrahop.com