Effective, Automated Enterprise Incident Response

Link Security and IT Operational Processes and Tools for Maximum Efficiency

INTRODUCTION

Automation promises to reduce the impact of incidents and enable faster results, greater efficiency, and better application of scarce skills. It represents a critical success factor for maturing security operations. The challenge is operationalizing.

Security has the knowledge of what needs to be done, but other operational teams control the policies, processes, and technologies for getting it done. Successful automation requires collaboration, trust, and accountability across team members and starts with agreement on what is safe to automate. Over time, the definition of acceptable automation risk should evolve and expand.

Reveal(x) Crosses Silos

ExtraHop Reveal(x) facilitates operational cooperation through several enterprise-ready automation paths. These include perimeter, user, and asset-based actions via standard security and IT tools—essentially, "response-in-depth" that suits enterprise governance, risk, and operational practices. By leveraging existing policies, playbooks, and tools, automated responses initiated by Reveal(x) can sidestep process and budget hurdles that hinder many enterprises.

Support for Maturing SOCs

Security operation centers (SOCs) see incident response as part of their core charter of incident management. They strive to increase efficiency, speed, and accuracy of containment, mitigation, and remediation of threats and security risks. While this is a general and ongoing challenge, ExtraHop Reveal(x) specifically helps improve SOC performance:

- Reduce the impact and spread of attacks
- Increase the accuracy, speed, and measurability of response actions
- Quickly and safely adopt low-risk, high-reward actions
- Reduce reoccurrence or reinfection by initiating hygiene updates
- Expedite data sharing and collaboration between SOC and other operational teams (NOC, endpoint, Datacenter ops)

Invisible by Design

Reveal(x) provides real-time visibility including auto-discovery and classification of devices and users joining the network. As an out-of-band, passive system, Reveal(x) remains hidden to attackers who frequently disable monitoring systems. This early warning system permits containment activities less drastic than isolation, such as heightened monitoring, proactive scanning, or security posture assessment of a device or its applications (such as a browser) when it joins the network.

Using real-time stream processing, Reveal(x) detects malicious behaviors and activities as they occur. The network and correlated threat intelligence feed machine learning, rule-based, and custom detections that permit surgical response. Since actions are based on the "wire truth" of network data, security teams can precisely target the correct assets for automated intervention and clean up.

Integration with Everything

ExtraHop enables response via integrations with the myriad products that already provide policy-driven enforcement, as well as through open interfaces. Our supported integrations include security orchestration and automation (SOAR) products, ticketing systems, network access control, and firewalls. Extensive REST APIs facilitate custom integrations.

ACTION TARGET	ACTION
Perimeter	• Dropping and blocking connections to known bad domains and IP addresses
Endpoint	• Quarantining new, unmanaged, or rogue devices • Forcing on-demand scanning and policy check-in • Isolating suspicious devices until workflow or scan can execute
Orchestration (SOAR or SIEM)	• Launching playbooks based on detections or triggers • Distributing relevant detections, evidence, or packets to other tools to enrich analysis • Alerting operational partners of new and suspicious activities (i.e., building security, system or database admins, HR, or legal)
Ticketing	• Initiating tickets • Escalating priority

One simple use case for this best-of-breed approach is firewall-based isolation. Companies can leverage a direct 1:1 integration with Palo Alto Networks firewall to quarantine a host, or work through Splunk Phantom to use Palo Alto Networks (or another SOAR-integrated product such as an endpoint platform).

Customized Sensitivity

Automated responses can also be triggered by ExtraHop machine learning, rules, or custom triggers tied to thresholds, severity, timing, user, device type, or a match with an external threat intelligence database.

Organizational Leverage

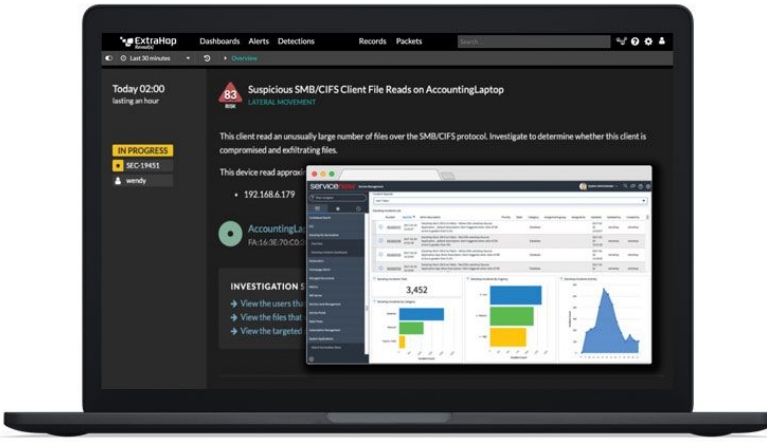
Because ExtraHop products are also used and approved by network, application, and cloud teams, operational responses can be readily understood and accepted. Especially when multiple humans remain in the loop, shared data, detections, context, and choices improve the efficiency of response.

Expert Services

If you don't have the time, ExtraHop and its partners can help you implement your integration and automate response using standard and open data formats, APIs, and interfaces. With more than ten years working with enterprises, we are pros at practical, operational, and industry best practices.

Summary

Putting it all together, the integrated Reveal(x) approach accelerates enterprise programs, reduces errors and duplicated effort that come with one-off and siloed decision-making, and minimizes disruption and risk from tool false positives. Get started today in taking the Enterprise security and operational preparedness to the next level of security.



Learn more about our current partners, integrations, and APIs available at
www.extrahop.com/integrations

ExtraHop demo online at
www.extrahop.com/demo

ABOUT EXTRAHOP NETWORKS

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions and applies advanced machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring delivery of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.