Hewlett Packard Enterprise

HPE Cyber Incident Readiness Review

An evaluation of your organization's ability to detect and respond to a cyber incident

Overview

Incident readiness capability review with SIEM

Security-related incidents are an undeniable reality for any organization with an IT infrastructure. Even organizations that have not invested in a cyber-security program will face security incidents requiring a response.

The HPE Cyber Incident Readiness Review quickly evaluates an organization's capability to perform steps along the incident response lifecycle.
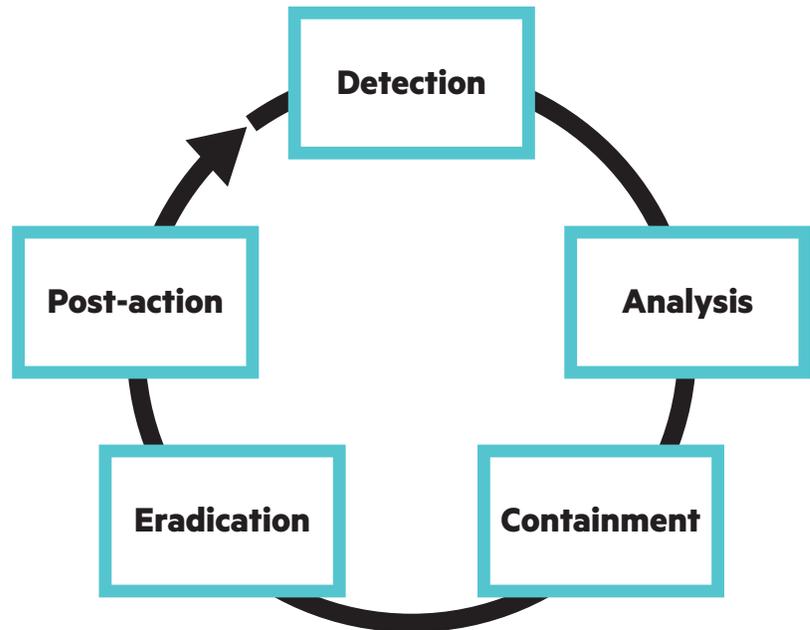
Attack lifecycle detection capability review

The longer breaches go undetected and the further along the attack lifecycle the attacker is able to progress, the worse the potential loss and impact. HPE consultants will evaluate your detection measures for coverage against the attack lifecycle. This review aligns technology investments and architecture to the stages of the attack lifecycle, quickly identifying areas where gaps in coverage increase risk and allow adversarial activity to escape detection.
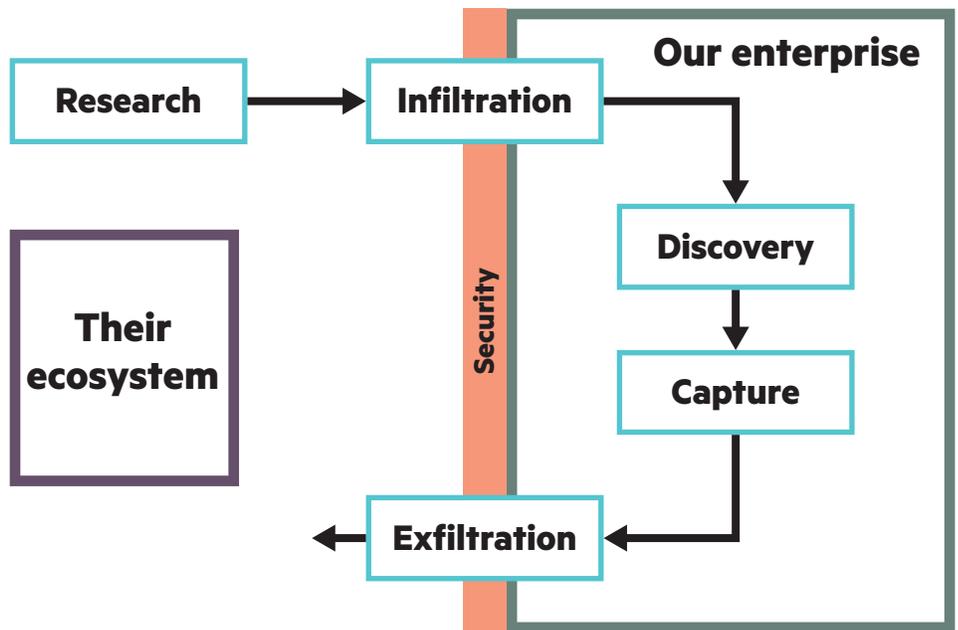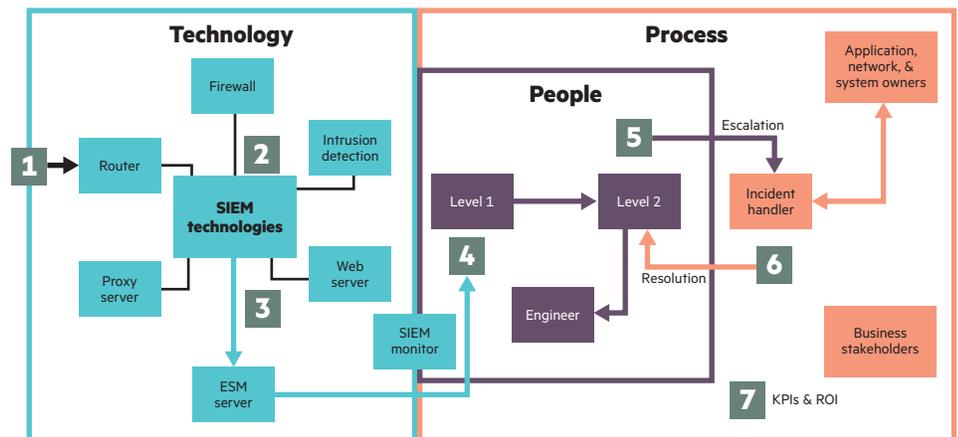
Analysis capability with SIEM review

As breaches are detected, the analytical process begins; successful analysis is largely dependent on the capability of the people and the structured workflow utilized by organizations. This stage of the review will look at key foundational components supporting individuals in the security program, the roles and responsibilities that are defined by the organization, and the capability and maturity of the people and process aspects of the operation.

Implementation

Evaluate operations

During the assessment, experienced HPE enterprise security consultants will:

Review the customer's existing cyber incident response capability, leveraging the HPE Security Operations Maturity Model (SOMM) through a combination of interviews, documentation review, discussions, and observations. The assessment will focus on these key functional areas:

- People: Review of organizational structure, roles and responsibilities, personnel experience and preparation, recruiting and retention, skill tracking, training, and career development

- Process: Review of analytical, operational, technological, and business processes that support the incident response capability

- Technology: Review technological aspects of incident response capability including the presence of SIEM technologies that support the incident response lifecycle.

Provide an incident readiness scorecard outlining the review results, key findings, and recommendations.

Planning and deployment

An HPE Services specialist will schedule the delivery of the Service at a time mutually agreed upon between HPE and the customer, which shall be during local HPE standard business hours, excluding HPE holidays, unless otherwise agreed by HPE. Any Services provided outside of HPE standard business hours will be subject to additional charges.

The HPE Services specialist will perform the following activities:

- Schedule and attend a kick-off meeting to review objectives, schedule, required audience, and deliverables

- Verify that prerequisites have been met

- Meet with your key stakeholders to assess the people, process, and technology components of your incident response capability

- Document findings and recommendations

- Schedule a close-out meeting to discuss key findings and recommendations

- An HPE Services specialist will be available to answer questions during the onsite or remote portions of the Service delivery

Service eligibility

Prerequisites
The customer must provide the following for delivery of this Service:

- Conference room with white board and projector

- Access to key stakeholders for interviews and group discussions:

  - **Incident response sponsor:** This is the CISO, CSO, Director of IT Security, IT Security leadership, IT Leadership, or champion of the incident response or security operations mission.

  - **Cyber incident response and/or Security operations manager:** This is the person who leads the day-to-day security operations/incident response capability.

  - **Senior security operations personnel:** These are the people who lead the security operations (for example, shift leads, Level-2/3 analysts, and so forth).

  - **Incident response personnel:** These are the people who drive the cyber security incident response processes.

  - **Security engineering:** These are the people responsible for the management of the SIEM, security devices, or other security technology.

  - **Ancillary security functions:** This term refers to any other security personnel that might have a vested interest in the cyber incident operations (for example, compliance, risk, and so forth).

- For any onsite services delivery, all requisite logistical accommodations to the HPE Services specialist, including but not limited to adequate physical work location, access to the customer's network, Internet access, telephone access, and access to the customer's offices where work will be performed

Limitations

This Service will be delivered as a single, continuous event. Environments requiring multiple engagements or phases over longer periods of time are not included in this Service, but can be accommodated at additional cost through a statement of work (SOW). Activities such as, but not limited to, the following are excluded from this Service:

• Installation and configuration of HPE software or appliances

• Racking of appliances or servers

• Development of FlexConnectors

• Delivery of standard Education offerings

• Performance testing or modeling services that, in the opinion of HPE, are required due to unauthorized attempts by non-HPE personnel to install, repair, maintain, or modify hardware, firmware, or software

• Services required due to causes external to the HPE-maintained hardware or software

• Any services not clearly specified in this document or services beyond the license limitations of the included products

Customer responsibility

Contact an HPE Services specialist within 90 days of the date of purchase to schedule the delivery of the Service.

Coordinate Service deployment on third-party-maintained hardware/software (if applicable) with HPE.

Assign a designated person from the customer's staff who, on behalf of the customer, will grant all approvals, provide information, attend meetings, and otherwise be available to assist HPE in facilitating the delivery of this Service.

Ensure that all Service prerequisites as identified in the Service Eligibility section are met.

Ensure the availability of all hardware, firmware, and software required by the HPE Services specialist to deliver this Service.

Retain and provide to HPE upon request all original software licenses, license agreements, license keys, and subscription service registration information, as applicable for this Service.
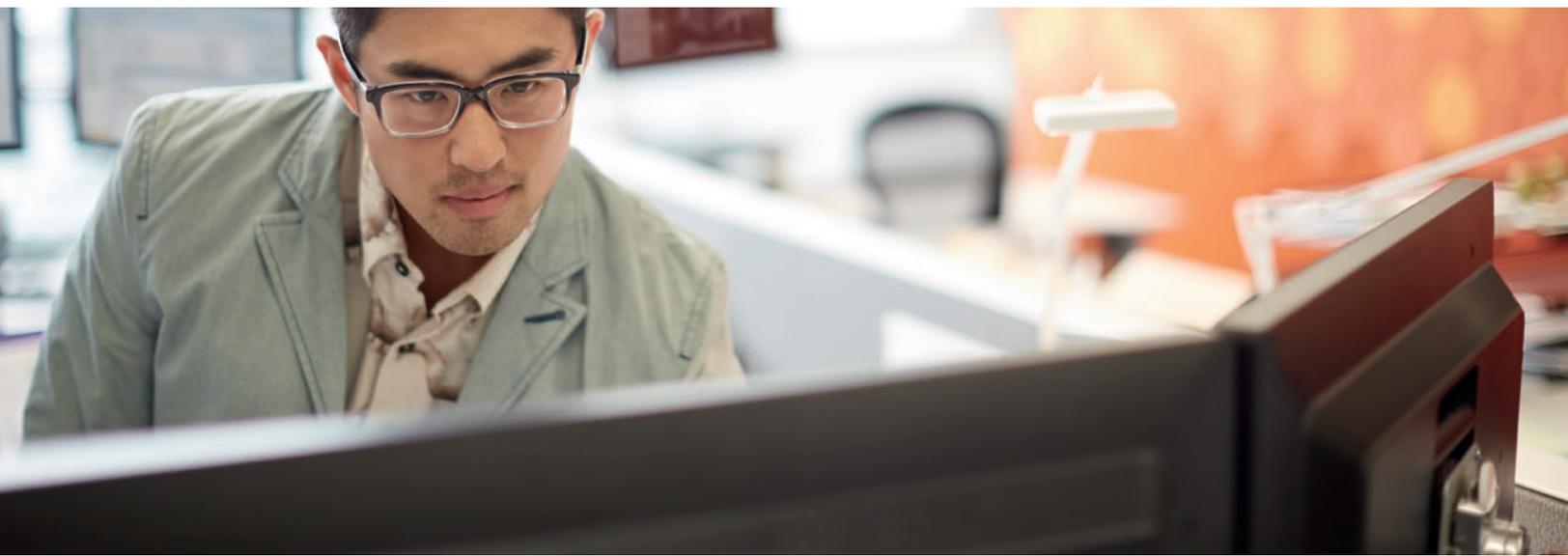
The customer shall provide reasonable access and working space at the site as HPE may reasonably request. The customer will provide HPE and HPE subcontractor staff standard telephone and dial-up or comparable data access to HPE's Network at industry-standard speeds. HPE shall observe the customer work rules and security and safety policies while performing HPE Services at the side of which HPE is informed of in writing in advance and that are not inconsistent with HPE's own business practices.

Duration

Delivery of this Service will not exceed a total of 20 service hours. This Service will be delivered by one HPE Services specialist and includes one onsite visit for up to two days in duration.

Terms

This offering consists of a consulting and training effort and is governed by the HPE Customer Terms. All capitalized terms used in this Data sheet, but not otherwise defined, will have the meaning assigned to them in the Terms. For purposes of this Data sheet, "Services" mean consulting, integration, professional services, or technical services performed by HPE under this Data sheet. Services excludes hardware maintenance and repair, software

maintenance, education services, or other standard support services provided by HPE; software as a service; managed print services; and outsourcing services.

Acceptance of deliverables occurs upon delivery.

Hiring of employees. You agree not to solicit, or make offers of employment to, or enter into consultant relationships with, any HPE employee involved, directly or indirectly, in the performance of services hereunder for one year after the date such employee ceases to perform services under the terms of this Data sheet. You shall not be prevented from hiring any such employee who responds to a general hiring program conducted in the ordinary course of business and not specifically directed to such HPE employees.

Authorization to install software. During the provision of services, HPE may be required to install copies of third-party or HPE-branded software and be required to accept license terms accompanying such software ("Shrink-Wrap Terms") on your behalf. Shrink-Wrap Terms may be in electronic format, embedded in the software, or contained within the software documentation. You hereby acknowledge that it is your responsibility to review Shrink-Wrap Terms at the time of installation, and hereby authorizes HPE to accept all Shrink-Wrap Terms on its behalf.

Intellectual property. HPE may provide HPE tools, templates, and other pre-existing intellectual property of HPE during the course of providing services ("HPE Pre-existing IP"). HPE Pre-existing IP does not include, nor is considered a part of, either the deliverables or HPE software products. HPE retains all intellectual property ownership rights in such HPE Pre-existing IP. All HPE Pre-existing IP is HPE confidential information. HPE Pre-existing IP may be governed by additional license terms that are embedded in the HPE Pre-existing IP.

Payment and validity

This offering will be pre-billed. You agree to pay invoiced amounts within thirty days of the invoice date. If applicable, you must schedule delivery of the offering to be completed within a period of one year from the date of purchase. Notwithstanding the previous sentence, HPE's obligations to deliver the offering under this Data sheet are considered fulfilled and your rights of receipt of the offering under this Data sheet will expire one year from the date of purchase.

Pricing for the offering may vary by country.

Cancellation

To avoid a Cancellation Fee as defined herein, you shall notify HPE in writing of cancellation or rescheduling at least ten business days prior to the offering start date. Cancellations or rescheduling with less than ten business days notification will incur 100 percent of the offering fee ("Cancellation Fee"). If you cancel ten or more business days in advance of scheduled delivery, you may reschedule only if delivery will be complete within one year from the purchase date.

Change in scope

Changes in scope are not allowed. You can request additional or different services, if available and at an additional cost, through a SOW or change order.

SKU: H8H66A1

Learn more at
hpe.com/software/sioc

Hewlett Packard Enterprise