Hewlett Packard
Enterprise

Get your security operations off the ground

Your security maturity level:

Developing

Featured resources:

Take HPE ArcSight Logger log management software out for a test drive—try for free now

Read more on how to launch your Security Operation Center

Related content:

Learn about HPE ArcSight Security Incident and Event Management

Explore how IT security teams use security analytics for intelligence—SANS Security Analytics Survey

Think you're too small to get hacked? Read Protecting Your Business from Today's Security Threats

Congratulations on your readiness to take your security center to the next level. Start by focusing on collection, searching, and reporting of your incident information. Then, you can build out your security program. Read on for the next steps.

Rely on the tools that can help

Although you may be collecting security logs, are you documenting incidents to draw lessons from them? Better documentation can help an organization move from an ad-hoc to more focused response.

- **Start with the foundational work of log management:** You don't just want to generate logs, you want to make them useful. Look for a tool that can unify collection, storage, log analysis and machine data from any device, vendor or source. Built-in rules and reports that can enable monitoring, alerting, and forensic investigation of security events are ideal.
- **Take a hard look at Security Incident and Event Management (SIEM) solutions:** Depending on your industry, compliance automation should support PCI, SOX, HIPAA, and IT governance. And, your tool should have a wide array of built-in reports that can later be customized as your organization evolves and matures.

Lay the foundation of your security center capabilities

To start building your security practice into a mature operation, you'll need to take some time to plan. All too often this planning focuses only on the people, process, and technology components of the project and ignores outlining what business problems the SOC will solve. Prior to building a security center, organizations must answer the following questions:

- Can you define what needs the center will meet for the organization?
- What are the specific tasks that will be assigned to the security center? (e.g., detecting attacks from the Internet, monitoring PCI compliance, detecting insider abuse on the financial systems, incident response and forensic analysis, vulnerability assessments, etc.)
- Who are the consumers of the information collected and analyzed by the security center?
- Who is the ultimate project sponsor for the security center?
- What types of security events will eventually be fed into the security center for monitoring?

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA5-8426ENN, November 2015, Rev. 1