Splunk Services for Breach Response Readiness

Splunk Services for Breach Response Readiness can help you quickly gather, analyze, investigate, respond and report on cyber incidents to better control the impact to your business. Splunk experts guide you through best practice processes to make sure the right data is available to the platform in order to quickly make decisions when time is of the essence.

Offering Highlights

- Assistance with deploying tactical incident response indicators and pre-built Splunk content
- Helps you establish on-going monitoring and alerting capabilities for future threats
- Provides you with a best practice response model and development for future responses
- Speeds your time to response using Splunk tools in support of a specific security event
- Leverages the expertise of security professionals who have built and managed security teams and services around the globe

Customers using the service receive escalated resourcing and expert guidance on how to leverage Splunk products. The service offers multiple options to accomplish a consultative and resource support model for you.

For many organizations, the start of an incident is just the beginning of the overall remediation plan required to protect against similar attacks in the future. Many incident response processes cover the immediate need to recover systems, and services that the organization uses. However, after the immediate response has been delivered, follow-up activities ensure that an organization does not suffer from a repeat attack. This process takes longer and it's for this reason that Splunk has developed a service offering that looks at the complete recovery process, from incident through problem management[1].

The Breach Response Readiness Service offers a suite of professional services[2] capabilities to deliver a highly coordinated, tactical and condensed response assistance capability enabling:

- Rapid identification of data sources and data onboarding
- Prebuilt breach searches and dashboards to facilitate tracking and reporting
- Automated workbooks and playbooks to enable monitoring, detection and response
- Historical and investigative data acceleration
- Escalated product administrative support

This service is focused on accelerating the access to the data you need either by accelerating summarization or historical context. **On-Demand** services are then used to provide iterative expert administrative or content support over the length of the subscription periods. **Assigned Expert** Services supports consultative and strategic planning, monitoring and analysis. There are two different subscription levels that align to the amount of time an Assigned Expert will work with the customer.

- **Splunk Services for Breach Response Readiness** (12 months) subscription utilizes Splunk T&M, OnDemand and Assigned expert for immediate value and long-term assistance.
  - Designed for existing customers with Splunk Enterprise Security and Phantom
  - Standard - 25 days per year of subscription
  - Premium - 50 days per year of subscription
- **Add-on: Implement Splunk Enterprise Security** supports accelerating fundamental searches, correlations and threat intelligence ingestion to provide coverage during a changing breach response.
- **Add-on: Implement Splunk Phantom** supports rapid adoption of a security automation plan and provides automation for recursive threat intelligence activities during a changing breach response.

1. The ITIL framework defines incident as the reactive process to resolve issues and problems. Problem management is longer term activities required to resolve the root cause of the incident.
2. The Professional Services portfolio includes a catalogue of OnDemand Services, Assigned Expert Services and traditional Professional Service engagements.

Outcomes

By leveraging this service, customers can achieve the following benefits and outcomes:

- Blueprints for endpoint and network monitoring of the identified critical assets via Splunk Enterprise
- Custom built detections for the discovered IOC's[3]
  - Rapid data onboarding in support of required detections with either Splunk Enterprise or Splunk Enterprise Security
- Leveraging externally provided curated threat intelligence feeds for the particular IOC's in regards to this particular threat
- Splunk Phantom SOAR workbooks and playbooks to guide you thru your response activities
  - Recursive threat intelligence activity
  - Event notification upon recursive detection
  - Breach Response Plan Workbook
- Ongoing support from Splunk services (via Assigned Expert or OnDemand) for your response team
  - Alert generation
  - Dashboard creation
  - Additional custom searches
  - Workbook and playbook creation
  - Case management automation
- Best-practices aligned After Action report for process improvement
- Opportunities for our customer's team to understand how to improve their leverage the Splunk portfolio of solutions and services to protect the organization

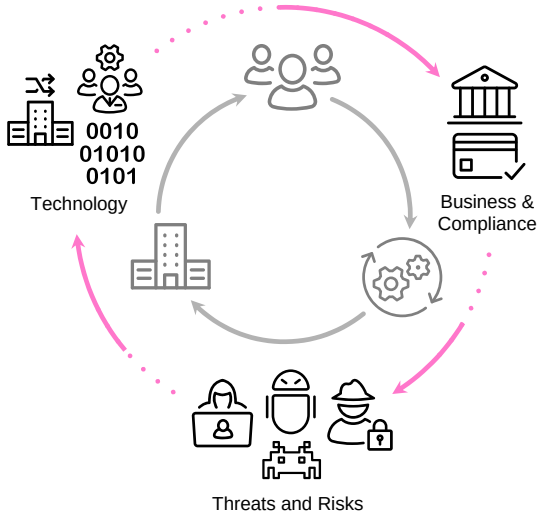
Power Through Your Tactical Response

Splunk is passionate about your data and our mission of bringing **data to everything**, including your toughest security challenges. In incident response, you need as much of the right data as you can handle and you need it available when it is required to track and respond. We want our customers to know Splunk is invested in your success and recovery. We are standing by to support your needs wherever we can. Splunk makes the world's leading SIEM and SOAR solutions, used by some of the best incident response teams in the business. By combining this best-of-breed technology with Splunk's security expertise, we are ready to support your team and rapidly respond to security incidents.

3. Indicators of Compromise (commonly considered IOCs) are indicators that are provided by the customer, their hired IR partner, or publicly IOCs approved by the customer.

During a security incident, we recommend you bring in the security incident response team to lead your remediation. Splunk Professional Services is available to support your needs with: rapid-data onboarding, rapid dashboard creation, expert search, and automation development so that you can bring data to every facet of your investigation and provide the necessary staff augmentation via our Incident Response Readiness Service.

We bring the people, processes and technology to support your breach response activities and can provide a lasting value across your organization.



Splunk Professional Services

Our services are backed by Splunk-accredited consultants, architects and delivery managers. They leverage Splunk best practices and experience from thousands of Splunk deployments. Reach out to your Splunk sales representative to let us help you via **email**.

Find out more about **Splunk Enterprise Security**, **Phantom** or read **our blogs** on the coverage of latest breaches.