# Security Solutions

## IBM® X-Force® Incident Response and Intelligence Services (IBM X-Force IRIS)

IBM® X-Force® Incident Response and Intelligence Services (IBM X-Force IRIS) provides security intelligence, incident response and strategic remediation that can help organizations achieve better control over security incidents and breaches. The IBM X-Force IRIS team can help deliver a comprehensive, programmatic approach designed to help prepare for, prevent, detect and respond to security incidents more efficiently and effectively

**Highlights**

Utilize a team of highly skilled experts with decades of leading-e dge incident management and security intelligence experience
Identify, detect and contain potential threats before they spread and cause more damage
Streamline incident response by planning and coordinating with business stakeholders before an incident occurs
More effectively protect your intellectual property, client data, reputation and market share
Minimize the time and costs associated with successful incident recovery

## Manage Security Services -MSIEM

IBM Security QRadar SIEM can serve as an anchor solution within an organization's security operations center.

IBM® QRadar® SIEM can serve as the anchor solution within your organization's security operations center to collect, normalize and correlate network data using years' worth of contextual insights. It also integrates with hundreds of IBM and non-IBM products and provides complete, unified visibility to security events in on-premises, hybrid, and cloud environments. An advanced Sense Analytics Engine is at the heart of this solution, designed to capture real-time log event and network flow data, and apply advanced analytics to reveal the footprints of would-be attackers.

QRadar SIEM is a highly scalable, enterprise solution that consolidates log source event data from thousands of devices distributed across a network, storing every activity in its database, and then performing immediate correlation and application of analytics to distinguish real threats from false positives. It also captures Layer 4 network flow data and, more uniquely, Layer 7 application payloads, using deep packet inspection technology. An intuitive user interface shared across all QRadar family components helps IT personnel quickly identify and remediate network attacks based on priority, ranking hundreds of alerts and patterns of anomalous activity into a drastically reduced number of offenses warranting further investigation.

QRadar SIEM deploys quickly and easily, providing contextual and actionable surveillance across the entire IT infrastructure, helping organizations detect and remediate threats often missed by other security solutions. These threats can include appropriate use of applications; insider fraud and theft; and advanced, "low and slow" threats easily lost in the "noise" of millions of events.

**State of Georgia Options**

| **Environment Assumption:** | •**Contract Term:** 36 Months | **Small** | **Medium** |
|---|---|---|---|
| *Note: IBM will have to review your specific environment to provide firm pricing.* | •**Transition Period:** 2 Months | - (1) All in One QRadar appliance deployed on prem (hw, sw, licensing not included) | - (1) Console QRadar appliance deployed on prem (hw, sw, licensing not included) |
| | •**Ongoing Operations Duration:** 34 Months | - 1000 EPS | - (1) Event Process/Collector QRadar appliance deployed on prem (hw, sw, licensing not included) |
| | •**Service Level:** Threat Monitoring and Device Management (Full Service) | - (5) log types | - 5000 EPS |
| | •**Total SIEM Appliances:** 1 | - (15) log sources | - (10) log types |
| | •**Total Gateways:** 1 | - (1) hour P1 SLA | - (30) log sources |
| | •**Events per Second (up to):** 5,000 | - Management/Monitoring | - (1) hour P1 SLA |
| | •**Priority 1 Security Incident Notification:** 1 Hour | - Global SOC delivery | - Management/Monitoring |
| | •**Change Requests per Month:** Unlimited | - No travel | - Global SOC delivery |
| | •**Deliverables:** | | - No travel |
| | •Project Plan | | |
| | •SIEM Macro and Micro Design | | |
| | •Communications Plan | | |
| | •Runbook | | |
| | •Monthly Report Set | | |
| | •**Support Tier:** Tier 1 is included, (Tier 2 and Tier 3 services are not included as part of this proposal) | | |

## X-Force IRIS Vision Retainer Service Tiered Pricing

| Level | Description | SLA | Price |
|---|---|---|---|
| **Ad Hoc** | •Time and materials terms and conditions | •Triage: Best Effort<br>•Onsite:  Best Effort | **$425/hour** |
| **Tier 1** | •Onsite Kickoff Workshop<br>•Quarterly Review Updates<br>•60 annual subscription hours<br>•Additional discounted hourly staff-rate | •Triage:  4 hours<br>•Onsite:  Best Effort | **$35,000** |
| **Tier 2** | •Onsite Kickoff Workshop<br>•Incident Response Program Assessment<br>•5 IR Playbook Customization<br>•1 Tabletop Exercise<br>•Quarterly Status Review and Report<br>•80 annual subscription hours for IR or proactive services<br>•Additional discounted hourly staff-rate<br>•IBM X-Force Threat Analysis Service – 2 seats | •Triage:  1 hour<br>•Onsite:  24-48 hours | **$50,000** |
| **Tier 3** | •Onsite Kickoff Workshop<br>•Incident Response Program Assessment<br>•10 IR Playbook Customization<br>•2 Tabletop Exercises<br>•Quarterly Status Review and Report<br>•150 annual subscription hours for IR or proactive services<br>•Additional discounted hourly staff-rate<br>•IBM X-Force Threat Analysis Service – 4 seats | •Triage:  1 hour<br>•Onsite:  24-48 hours | **$100,000** |

## Manage Security Services -MSIEM Pricing

| Level | Description | | Price |
|---|---|---|---|
| **Small Environment Pricing** | •One Time Charge (OTC) | *2 months* | **$150,000.00 (Transition)** |
| | •Monthly Recurring Charge (MRC) | *34 months* | **$9,600 (Steady State)** |
| | •Estimated Pricing Small Environment<br>Termination Charges May Apply | | **•$150,000 (OTC) + $326,400 ($9,600 X 34 Months) = $476,400.** |
| | | | |
| **Medium Environment Pricing** | •One Time Charge (OTC) | *2 months* | **$150,000.00 (Transition)** |
| | •Monthly Recurring Charge (MRC) | *34 months* | **$24,300 (Steady State)** |
| | •Estimated Pricing Medium Environment<br>Termination Charges May Apply | | **•$150,000 (OTC) + $826,200 ($24,300 X 34 Months) = $976,200.** |

*You may cancel the Services at any time during the initial or any renewal Contract Period by providing 60 days prior written notice. Upon cancellation, you agree to pay IBM all Services charges through the effective date of cancellation, and an early cancellation charge in accordance with the following:*

*1. · if canceled during year one, the early cancellation charge shall be 100% of the Services charges for the remaining Contract Period;*

*2. · if canceled during year two or beyond, the early cancellation charge shall be 50% of the Services charges for the remaining Contract Period;*