RUNBOOK

Global Security Operations Center

Introduction

This document outlines the Security Operations Center (SOC) runbook for responding to cyber threats for Barracuda XDR partners. The purpose of this document is to provide visibility and details into the people, processes, and procedures designed to protect partners and their customers against cybersecurity threats. If you have any questions pertaining to the information in this document, please contact your Regional Account Director.

To open a security incident, contact the SOC team using the information below:

Contact Information

Email: soc@barracuda.com

Phone: US: +1 855-838-4500

IRE: +353 57 865-7170

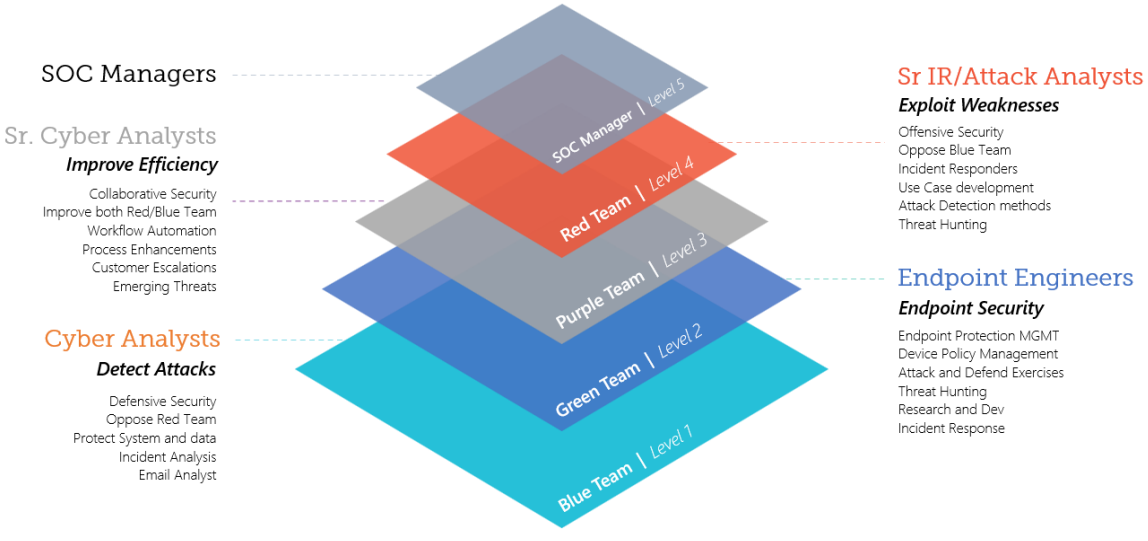
UK: +44 20 3695-8498

NLD: +31 77 799 8910

APAC: +61 2 7228 1891

Global coverage

Barracuda's global security experts are divided into teams to provide around-the-clock, real-time threat monitoring, analysis, and guidance. The location of XDR's security experts includes North America, Europe, and the Asia Pacific regions. The organization of the teams can be seen in the figures below:



SOC team roles & responsibilities

Blue Team	Detect ATT&CKS	• Defensive security • Oppose Red Team • Protect system and data	• Incident analysis • Malware analysis • Email analyst	Level 1 / Level 2
Green Team	Endpoint Security	• Scripts and policy mgmt. • Enable whitelisting policies • Test new malware variants	• Manage endpoint tenants • Manage support case • Manage product cases	Level 3
Purple Team	Improve Efficiency	• Collaborative security • Improve both Red and Blue Team • Emerging threats	• Customer escalation • Automation & enrichment • Process enhancements	Level 4
Red Team	Exploit Weaknesses	• Offensive security • Research, testing & dev. • Incident responders	• Use case development • Attack detection methods • Threat hunting	Level 5
White Team	Orchestrate	• Manage GSOC • Drive GSOC vision • Execute GSOC roadmap	• Customer feedback • Improve GSOC capabilities • Escalation point for L5	Level 6

Security monitoring

Incident detection

A combination of data feeds provides real-time information with which XDR detects suspicious or malicious activity in our customer's environments. Using a variety of tools, XDR aggregates this data and displays it to our security experts for analysis. Threat analysis is done in real time with SIEM rules and SOAR stories to alert XDR's security experts of suspicious activity as quickly as possible to ensure a prompt response. All XDR rules are mapped to the MITRE ATT&CK Framework to validate the coverage XDR has for each customer.

Incident analysis

Initial analysis of an incident will typically begin with a Level 1 security analyst. The analyst responds to an alarm in the XDR platform and if necessary, the customer is contacted regarding the incident (either through a support ticket integration, email, or phone call). The information is displayed in the Barracuda XDR dashboard regarding the triggered alarm or alert, security threat advisories, and more.

Extensive analysis of potential intrusions is performed by Level 2 security experts and above within the SOC's incident escalation procedure. This capability will usually involve analysis leveraging various data artifacts to determine the who, what, when, where, and why of an incident to help facilitate containment, eradication, and recovery from the incident. The security expert will document the details of this analysis, usually with a recommendation for further action, and include it with each alarm or alert.

Security incident categories

All XDR rules are mapped to the MITRE ATT&CK framework. This categorizes the incident into specific tactics and techniques and includes a corresponding playbook. The playbook ensures XDR provides the customer with the appropriate investigative actions to gather all pertinent information and mitigation recommendations. If needed, an additional incident response service will be conducted to contain the potential breach/incident.

Alert escalation

Alert priority categories

Security alarms and alerts are organized into three priorities based on the level of risk associated with an incident.

High Risk: Incidents at this level are actionable high-risk events that have the potential to cause severe damage to customer environments. High-risk events require customers to take immediate defensive actions. Endpoint threat not contained, privilege escalation, hacking tool detected, and similar incidents are assigned to this priority level. Please note all high-risk events will be followed up by a phone call from XDR.

Medium Risk: Incidents at this level also require action be taken, but typically would not lead to substantial impact as a standalone event. Incidents such as suspicious login events, brute-force attempt or password spraying, threat intelligence matches, and many more are examples of rules assigned to this priority level.

Low Risk: Incidents in this category involve activity within a customer environment that is valuable for awareness but may not require action to be taken. User account created, data transfer detected, password change, and similar events are assigned this priority level.

Escalation

In accordance with the policies outlined in the individual Service Descriptions, Barracuda XDR escalates security incidents to the previously established authorized customer contacts as outlined below.

Note: During a high-risk security alert escalation, Barracuda XDR will attempt to reach the designated customer contacts until a contact is reached or all escalation contacts have been exhausted. Those items that require immediate action are prioritized for escalation to the corresponding customer. Lower-level items are escalated to customers in accordance with the recommended time to resolve the issue.

Escalation methods

The table below illustrates the escalation methods for each security alert classification.

Alert Classification	Primary Method	Secondary Method
High Risk	Phone call	Email or ticket integration
Medium Risk	Email or ticket integration	N/A
Low Risk	Email or ticket integration	N/A
False Positive	Barracuda XDR Customer Security Dashboard	N/A

Escalation path

Barracuda XDR uses a defined escalation path to contact customers during a security incident. This escalation path includes the order in which to call authorized security contacts, and the phone numbers Barracuda XDR may use. A security incident escalation that requires immediate action triggers the call-tree process documented in the corresponding customer profile. Starting with the primary security contact, Barracuda XDR dials through all provided phone numbers prior to moving to the secondary contact. The process repeats for each authorized contact in the escalation path until a customer contact is reached, or all contacts have been exhausted.

Incident response guidance

The time to respond to an incident can depend on the scope of the issue at hand. In most scenarios, a Level 1 security expert will initially process the data provided and decide on what steps to take next; this may include escalating the issue to a higher Level within the team or simply devising a client notification. In either situation, the Level 1 security expert will field an initial alarm or notification from the customer, and then submit the issue to the Level 3 security experts for review. Once an incident is confirmed, our security experts will immediately open a zoom bridge to initiate the incident response guidance.

Service level agreement

The goal is to provide our customers best in class response times on security alerts and general requests managed by Barracuda XDR. The XDR SLA establishes response time objectives based on risk level for security alarms resulting from the Barracuda XDR platform. The SLA becomes effective when the enablement process has been completed, and support and management of the services have been successfully transitioned to “active”.

Service Levels

- 24 hours per day, 365 days per year
- 99.5% service availability of Barracuda XDR services
- Maintenance windows - notification by email of maintenance windows that result in complete outage or service availability (rolling upgrades or changes that do not affect overall system uptime are excluded)

Alarm Classification and Escalation Handling

When a rule triggers within the XDR platform, an alarm is created, assigned a specific level of risk, and escalated to Barracuda XDR security experts and/or customer per an established escalation policy.

Classification	Description	Escalation Policy	Escalation Method	SOC Response Time	Customer Actions
HIGH RISK	Security incidents at this level are actionable, high-risk events that have the potential to cause severe damage to customer environments. Examples: • Endpoint threat not contained • Privilege escalation • Hacking tool detected • Login from high-risk country	XDR will escalate to the designated primary escalation contact via phone call while issuing the security alert to the customer alert distribution group via email or ticket integration. Escalations will include information on the type of threat and recommendations on mitigation activities. If the primary contact is unreachable, XDR will attempt to contact the additional customer escalation contacts in priority order until a contact is reached, or all contacts are exhausted. In the instance of a true-positive security alert with impact to a customer, XDR will provide guidance throughout the duration of the incident. Please refer to the XDR Incident Response Plan for more detail.	Phone call AND Email or ticket integration AND Barracuda XDR Dashboard	20 minutes	Acknowledge receipt of the security alert immediately and confirm it is actively being reviewed. If no response, Barracuda XDR will attempt to reach the designated customer contacts until a contact is reached or all escalation contacts have been exhausted.
MEDIUM RISK	Security incidents at this level also require action be taken, but typically would not lead to substantial impact as a standalone event. Examples: • Suspicious login events • Brute-force attempt or password spray • Threat intelligence matches	XDR will escalate to the customer distribution group via email or ticket integration. Escalations will include information on the type of threat and recommendations on mitigation activities.	Email or ticket integration AND Barracuda XDR Dashboard	1 Hour	Acknowledge receipt of the security alert within 24 hours of when it was issued by XDR. If no response is received within 24 hours, a follow up to the alert will be sent via email.

LOW RISK	Security alarms at this level involve activity within a customer environment that is valuable for awareness but may not require action to be taken. Examples: • User account created • Data transfer detected • Password change	XDR will escalate to the customer distribution group via email or ticket integration. Escalations will include information on the type of threat and recommendations on mitigation activities.	Email or ticket integration AND Barracuda XDR Dashboard	8 Hours	Acknowledge receipt of the security alert within 24 hours of when it was issued by XDR. If no response is received within 24 hours, a follow up to the alert will be sent via email.

Customer Request Classification and Handling

All requests, either via email or phone call, coming from customers to Barracuda XDR security experts are subjected to the below SLA guidelines.

Barracuda XDR will respond to the below mentioned email requests with an initial acknowledgement to the customer within the below mentioned timeframe.

Request Type	First Response Time	Completion Time
General Inquiries	1 Hour	48-72 hours
Endpoint Security Administration/Tuning	1 Hour	24 Hours
Email Security Administration/Tuning	1 Hour	24 Hours
Cloud Security Tuning	1 Hour	24 Hours
Network Security Tuning	1 Hour	24 Hours
Server Security Tuning	1 Hour	24 hours
Threat Analysis/Investigation	1 Hour	48-72 Hours
Rule Creation Request	1 Hour	2.5 weeks

Conclusion

Barracuda XDR strives to provide best in class services to our customers by adhering with the processes and timeframes for communication with our customers as outlined in this document. This will optimize defense against the ever-changing cybersecurity threat landscape. If you have any questions, please do not hesitate to contact your account executive or the SOC directly at soc@barracuda.com.

Disclaimer

Client understands that, although Barracuda XDR's Services may discuss or relate to legal and/or compliance issues, Barracuda XDR does not provide legal advice or services, none of Barracuda XDR's Services shall be deemed, construed as, or constitute legal advice and that Client is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries, advisories, alerts, or reports provided by Barracuda Managed XDR in connection with any Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Client's legal or regulatory compliance.