Glossary

https://campus.barracuda.com/doc/99616715/

Term	Definition
Agent	An agent is a program that collects information or performs a task in the background at a particular schedule. Also known as a Collector.
Alarm	A potential threat or risk detected by the SIEM engine and that triggers a ticket in the SOC queue for further analysis.
Alert	A potential threat or risk details sent to the customer in the form of ticket.
Allow List	The Allow List is a list of threats that are not malicious, so do not create alerts. Users add threats that they consider not malicious to the Allow List. See Adding a Threat to the Allow List.
AnyRun	A service that lets cybersecurity specialists detect, analyze, and monitor cybersecurity threats. (https://app.any.run/)
Blue Team	An XDR team that continuously monitors (24/7) incoming threats in the SIEM environment and alerts the customer.
Cloud Monitoring	Secures customers’ cloud environments from unauthorized access to cloud mailboxes, admin changes in the environment, impossible logins, and brute force attacks.
Collector	See Agent.
Cyber Warranty	Financial protection against spear phishing, ransomware, and BEC for MSPs and clients. Using the Barracuda XDR solution suite streamlines the application and claim process, speeding the process time from months to days. For more information, see https://www.barracudamsp.com/content/dam/barracuda-msp/docs/resources/pdf/data-sheets/DS-Barracuda-Cyber-Warranty.pdf
Device	See Endpoint.
Endpoint	A unique responding hardware device.
Email Monitoring	Proactively monitors existing email security solution to enhance protection against spear phishing, business email compromise (BEC), and more.
Emerging Threats	Emerging threats and technologies that customers need to be prioritized and publish an advisory on it.
Endpoint Monitoring	Unifies and extends detection and response capability to endpoints, protecting them from common endpoint threats, including malware and ransomware.
Event	Raw data being analyzed by XDR.
eXtended Detection and Response (XDR)	**What is extended detection and response (XDR)? What does XDR mean in security?** Extended detection and response (XDR) deliver visibility into data across networks, clouds, endpoints, and applications while applying analytics and automation to detect, analyze, hunt, and remediate today's and tomorrow's threats. **How XDR works** XDR collects and correlates data across email, endpoints, servers, cloud workloads, and networks, enabling visibility and context into advanced threats. Threats can then be analyzed, prioritized, hunted, and remediated to prevent data loss and security breaches. **Why is XDR important?** With more visibility and context into threats, events that would have not been addressed before will surface to a higher level of awareness, allowing security teams to quickly focus and eliminate any further impact and reduce the severity and scope of the attack. **How to use XDR** XDR utilizes technologies that provide higher visibility and collect and correlate threat information, while employing analytics and automation to help detect attacks. **Find out more about XDR** https://blog.barracuda.com/2023/05/04/what-is-xdr https://blog.barracuda.com/2023/08/23/barracuda-xdr-insights-ai-patterns-protect https://blog.barracuda.com/2023/06/12/why-xdr-is-essential-for-msps **How Barracuda can help** https://barracudamsp.com/product-details/extended-detection-and-response-xdr/
Green Team	An XDR team that responds to customer queries about Barracuda endpoint solution and helps them to resolve their issues as soon as possible.
Indicator of Compromise (IOC)	Known malicious IP addresses, hashes, and domains/URLs that are ingested in threat feeds for Barracuda XDR alerting.
Indicator of Attack (IOA)	Known elements of attack patterns.
MISP (Malware Information Sharing Platform)	An open-source software solution for collecting, storing, distributing, and sharing cyber security indicators and threats about cyber security. See https://www.misp-project.org/documentation/.

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)	A guideline for classifying and describing cyberattacks and intrusions. See https://attack.mitre.org/
Network Monitoring	Monitoring that detects potential threat activity on customer's network such as command-and-control connections, denial-of-service attacks, data exfiltration, and reconnaissance.
Purple Team	An XDR team that looks after escalations from the Blue Team and helps them to mitigate threats. They also participate in automating certain threat detection rules.
Red Team	An XDR team that helps the Purple and Blue Teams with queries and concerns. They continuously evaluate detection rules and create new ones while also responding to major incidents taking place in the customer environments.
Rule	A definition that is used to analyze alarms and alerts to create threats.
Sensor/Customer Premise Appliance (CPA)	A collector that sits on customer environment in the form of **Physical box** or **Virtual image** to forward the logs from firewalls, servers etc.
Server Monitoring	Protects customers' critical servers from attacks such as password sprays, brute force attacks, and privilege escalation.
Security Operation Center (SOC)	The Barracuda XDR Security Operation Center (SOC) serves as the principle delivery arm for its Services. The Security Operations Center is located within a hardened facility that provides industry standard security protocols for both physical and logical security.
SOAR	Security Orchestration, Automation, and Response (SOAR) is a collection of automated technologies that analyzes, responds to, and mitigate threats.
Tactics (MITRE ATT&CK)	According to the MITRE ATT&CK protocol, what attackers are trying to achieve. See https://attack.mitre.org/tactics/enterprise/. Compare Techniques **.**
Techniques	According to the MITRE ATT&CK protocol, how attackers accomplish those steps or goals. See https://attack.mitre.org/techniques/enterprise/. Compare Tactics.
Threat	A potential risks found in Managed Endpoint Security.
Threat Advisory	Advice/Notifications on vulnerabilities, emerging threats and other cybersecurity risks developments to MSP or direct customers. See https://smartermsp.com/category/security/page/2/.
Threat Detection and Response (TDR)	The process of identifying threats and mitigating them before they impact customers.
Threat Hunting	The process of hunting for threats using logs. Typically Barracuda XDR performs research and reviewss IOAs and IOCs. Using this, Barracuda XDR creates queries and sometimes rules to detect threats.
Ticket	A case file that contains one or more Alarms and/or Alerts.
Use Case	
XDR Agent	A single, unified way to add monitoring for logs, metrics, and other types of data to hosts. See https://www.elastic.co/guide/en/fleet/current/fleet-overview.html. Also known as the Elastic Agent.