PRODUKTÜBERSICHT

Network Threat Analytics Suite

LogRhythm
The Security Intelligence Company

Unternehmen jeder Branche müssen sich heute mit der steigenden Anzahl an immer komplexeren Angriffen, die ihr Netzwerk bedrohen, auseinandersetzen. Jedoch der chronische Mangel an Sicherheitsexperten und fehlende Einblicke in die Netzwerkaktivitäten lassen Unternehmen, die Cyber-Bedrohungen abwehren möchten bevor sie in das Netzwerk eindringen und Schaden anrichten, straucheln. Ein ganzheitlicher Ansatz mit Security Intelligence sollte ein integraler Bestandteil einer Sicherheitsinfrastruktur sein. Eine leistungsstarke Lösung für die Netzwerkanalyse ist heute eine essentielle Komponente einer Sicherheitsstrategie, um Unternehmen zu befähigen, Cyber-Bedrohungen zu entdecken, einzuordnen, zu eliminieren und Transparenz zu schaffen.

Netzwerkanalysen

- ☑ Automatisierte Verhaltensanalysen und Statistien
- ☑ Netzwerkforensik und Deep Paket Inspection
- ☑ Erkennung und Vermeidungg von Sicherheitsverletzungen
- ☑ Umsetzungbewährter Sicherheitsverfahren

LogRhythms Network Threat Analytics Suite unterstützt Unternehmen dabei, alle Netzwerkaktivitäten, die in ihrer IT-Umgebung auftreten, zu verstehen. Hierfür bietet die Suite automatisierte, Out-of-the-Box-Funktionalitäten, die die Zeitspanne, Cyber-Bedrohungen zu erkennen und darauf zu reagieren, erheblich senken. Die LogRhythm Labs haben diese Lösung entwickelt, um fundierte Analysen zu liefern, die weit über die Leistungen von herkömmlichen NBAD-Auswertungen (NBAD: Network Behavior Anomaly Detection) oder Datenfluss-Analysen hinausgehen und Maschinendaten nutzen. Die LogRhythm-Analysen liefern Netzwerk- und Sicherheitsverantwortlichen den notwendigen Kontext, um Bedrohungen zu priorisieren und zielgerichtet zu agieren. Die Network Threat Analytics Suite nutzt die SmartFlow-Daten aus LogRhythms Network Monitor, der Deep Packet Inspection durchführt und dabei die Metadaten aus mehr als 2.500 Anwendungen automatisch identifiziert und extrahiert. Die Suite analysiert auch die Daten externer Quellen, beispielsweise von Routern, Switches, Remote-Access-Gateways, Firewalls, Next-Generation-Firewalls oder VPN-Konzentratoren sowie die Daten der Netzwerk-Sensoren anderer Anbieter.

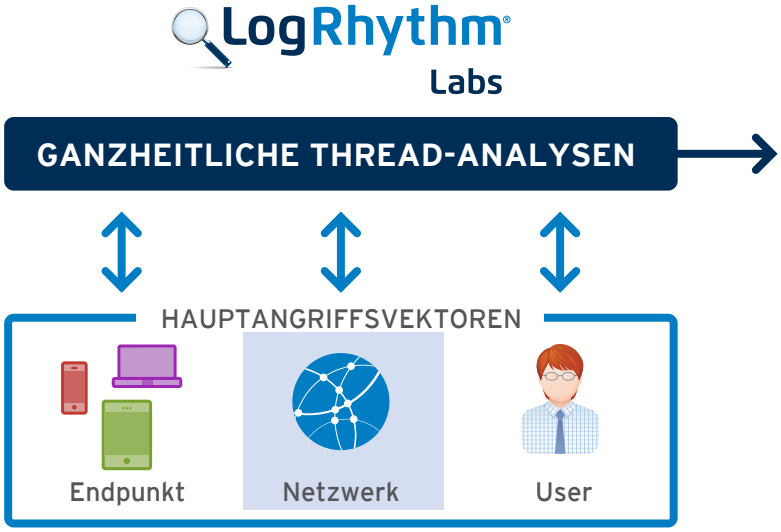
Die Funktionsweise

Die Network Threat Analytics Suite nutzt eine Vielzahl an innovativen Regeln für die Erkennung von Verhaltensmustern, die die AI Engine von LogRhythm bietet. Die AI Engine umfasst verschiedene Analysetechniken wie beispielsweise die Verhaltensanalyse, maschinelles Lernen und maschinelle Analysen (Erkennung von Gesetzmäßigkeiten) sowie Datenkorrelation über verschiedene Quellen hinweg. So erhalten Sicherheitsverantwortliche fundierte Einblicke und Informationen zu kompromittierten Geräten, verbreiteter Malware, Cyber-Kriminellen, politisch motivierten Angriffsversuchen, Datenverlusten und mehr. Unternehmen können das Modul für die Bedrohungsanalyse im Netzwerk so konfigurieren und einsetzen, dass sie eine Vielzahl an Anomalien in den Netzwerkaktivitäten sowie die Indikatoren für eine Kompromittierung unmittelbar sehen. Mit der Suite erhalten sie auch einen Leitfaden, der Instruktionen und Empfehlungen für die Installation und die Systemoptimierung umfasst, sodass sie praxisbewährte Verfahren effizient umsetzen und den gewünschten ROI schnell erzielen können.

Schadhafte Netzwerkaktivitäten
- Port-Scans und Sweeps
- Interne Ausspähung
- Denial-of-Service-Attacken
- Botnet-Aktivitäten
- und mehr...

Angriffe auf Webanwendungen
- SQL-Injection-Angriffe
- Cross-Site-Scripting
- übermäßige Zahl an HTTP-Fehlern
- Directory Traversal interner URLs (Manipulation der Pfadangaben)
- und mehr...

Versuchte Sicherheitsverletzung
- Verdächtige Datenübertragungen
- Besonders schadhafte Payload-Angriffe
- Anomale Muster im Datenverkehr
- Blacklist-Kommunikation
- und mehr...



Aufgrund des hohen Datenverkehrs in unseren Netzwerken, der zunehmenden Komplexität von zielgerichteten Attacken und der Zero-Day-Attacken bieten herkömmliche signaturbasierende Tools und präventive Schutzmaßnahmen für das Unternehmensnetzwerk nicht mehr ausreichend Schutz. LogRhythms Network Threat Analytics Suite und die Vielzahl der darin enthaltenen Technologien bietet einen umfassenden Ansatz für die Überwachung und Analyse des Netzwerkverhaltens in Echtzeit. Die Lösung ermöglicht es Unternehmen, sicherheitsrelevante Ereignisse unmittelbar zu erkennen, die Aktivitäten, die eine echte Bedrohung darstellen, zu priorisieren und automatisch Gegenmaßnahmen einzuleiten, um diese Angriffe zu eliminieren bevor sie größeren Schaden anrichten können.

Erkenndung vor dem Angriff: Damit Angreifer erfolgreich in ein Unternehmen eindringen und dieses attackieren können, müssen sie ihr mögliches Angriffsziel identifizieren und kennen. Aktivitäten wie Ping-Sweeps, Port-Scans und Port-Sweeps hinterlassen typischerweise auffällige Spuren. Deshalb versuchen Angreifer „so leise und unauffällig wie möglich" einzudringen, um einer Entdeckung zu entgehen. Die Regeln der LogRhythm Network Threat Analytics Suite können diese Aktivitäten erkennen und Sicherheitsverantwortliche benachrichtigen, wenn auf diese Aktivitäten weitere verdächtige Aktivitäten folgen. Hierzu zählen beispielsweise ein nachweislich erhöhter Datenverkehr im Netzwerk oder ein anderes komplexeres Angriffsverhalten. Unternehmen können so vorbeugende Maßnahmen einleiten und beispielsweise die IP-Adressen einer Blacklist beziehungsweise der Firewall-ACL zuordnen oder einen Schwachstellen-Scann starten, um festzustellen, ob die Angriffsziele durch diese spezifische Attacke gefährdet sind.

Angriffe auf Web-Anwendungen: Server mit direkter Internet-Verbindung und Web-Anwendungen stellen einen gefährdeten und öffentlich erreichbaren Eintrittspunkt dar, der von Cyber-Kriminellen sehr einfach ausgenutzt werden kann. Der Report „2014 Verizon DBIR" legt dar, dass 60 Prozent aller erfolgreichen Kompromittierungen auf die Ausnutzung von Schwachstellen in Web-Anwendungen basierten, wobei hier XSS- und SQL-Injection-Angriffe die gängigsten Angriffsmethoden waren und binnen Minuten erfolgten. Die LogRhythm Network Threat Analytics Suite kann die Sicherheitsverantwortlichen sofort über eine erkannte webbasierende Bedrohung informieren. Dies umfasst auch Versuche, die URL-Paramenter zu manipulieren oder JavaScript-Code in einer Website einzusetzen. SmartResponse kann diese Bedrohungsform automatisch neutralisieren und Maßnahmen einleiten, die die betroffenen Server in Quarantäne nehmen und die IP-Adressen der Angreifer der Firewall-ACL hinzufügen.

Die Kommunikation mit verdächtigen IP-Adressen: Die Netzwerk-Kommunikation mit verdächtigen IP-Adressen und IP-Bereichen ist ein hervorragender Indikator für Malware-Ausbrüche und erfolgreich durchgeführte Sicherheitsverstöße. Doch noch immer können viele Unternehmen verdächtigen Datenverkehr mit bekannten, aber unseriösen Quellen nicht automatisch erkennen. LogRhythms Network Threat Analytics Suite bietet zahlreiche Standard-Regeln, die verdächtige Netzwerkaktivitäten erkennen und diese Daten mit den aktuellen Informationen abgleichen, die das LogRhythm Threat Intelligence Ecosystem liefert. Diese Regeln bringen zudem zum Vorschein, welche Bedrohungen am gefährlichsten sind. Dies umfasst auch die Netzwerk-Kommunikation mit oder von Adressen, die auf der Blacklist stehen, oder Adressen, die geografisch nicht in der Whitelist aufgeführt sind.

Datenverkehr durch Botnetze und Command & Control: Die unmittelbare Erkennung von Botnets oder anderer Malware ist eine essentielle Komponente für die Netzwerksicherheit. Dennoch setzen viele Unternehmen keine Tools ein, um den schadhaften Datenverkehr, der mit dem Ausbruch dieser Angriffe einhergeht, zu erkennen. Bots nutzen oftmals die Standard-Ports für den Datenverkehr (HTTP/HTTPs, Telnet, FTP und SSH) oder eine andere erlaubte Datenübertragung, um Firewall-ACLs beziehungsweise herkömmliche Sicherheitssysteme zu umgehen oder ihre Aktivitäten zu verbergen, wenn sie mit Command & Control-Servern kommunizieren. LogRhythms Network Threat Analytics Suite bietet Standard-Regeln, die zahlreiche schadhafte Netzwerkaktivitäten im Zusammenhang mit Bots erkennen. Hierzu zählen beispielsweise anormaler, ausgehender Datenverkehr über IRC-Ports oder verdächtige Top-Level-Domains (TLDs). LogRhythms Network Monitor führt eine Deep-Packet-Inspection durch, um weitere Informationen zu liefern und verdächtigen Datenverkehr im Zusammenhang mit Botnet-Aktivitäten schnell zu erkennen.

Getarnte Datenübertragungen und Datenausschleusungen: Sobald Angreifer in die IT-Umgebung eingedrungen sind und versuchen, geschäftskritische Informationen wie personenbezogene Daten, Zahlungsinformationen oder Patientendaten aus dem Unternehmen zu schleusen, ist es von höchster Bedeutung, diese Sicherheitsverstöße sofort zu aufzudecken und den Schaden zu begrenzen. Die Regeln in LogRhythms Network Threat Analytics Suite sind darauf ausgerichtet, diese versuchten Datenausschleusungen festzustellen. Sie erkennen Datenübertragungen in ungewöhnlichen Größenordnungen sowie die Kommunikation mit verdächtigen IP-Adressen. Zudem entdeckt die Lösung Sessions, die ungewöhnlich lange dauern und denen möglicherweise der Versuch zugrunde liegt, Daten in kleineren Übertragungseinheiten zu entwenden. LogRhythms Network Monitor liefert zudem zusätzliche forensische Informationen, um die Angriffsziele durch die automatisierte und vollständige Erfassung der Datenpakete sofort aufzuspüren und jeden Versuch, Daten zu stehlen, aufzudecken.