Wazuh Indexer

Wazuh dizinleyicisi, son derece ölçeklenebilir, tam metin arama ve analiz motorudur. Bu Wazuh merkezi bileşeni, Wazuh sunucusu tarafından oluşturulan uyarıları dizinler ve depolar ve neredeyse gerçek zamanlı veri arama ve analiz yetenekleri sağlar. Wazuh dizinleyicisi, ölçeklenebilirlik ve yüksek kullanılabilirlik sağlayan tek düğümlü veya çok düğümlü bir küme olarak yapılandırılabilir.

Wazuh dizinleyicisi verileri JSON belgeleri olarak depolar. Her belge, bir dizi anahtar, alan adı veya özelliği, dizeler, sayılar, boole değerleri, tarihler, değer dizileri, coğrafi konumlar veya diğer veri türleri olabilen karşılık gelen değerleriyle ilişkilendirir.

Bir dizin, birbirleriyle ilişkili belgelerin bir koleksiyonudur. Wazuh dizinleyicisinde depolanan belgeler, parçalar olarak bilinen farklı kapsayıcılara dağıtılır. Belgeleri birden fazla parçaya ve bu parçaları birden fazla düğüme dağıtarak, Wazuh dizinleyici yedekliliği sağlayabilir. Bu, sisteminizi donanım arızalarına karşı korur ve düğümler bir kümeye eklendikçe sorgu kapasitesini artırır.

Wazuh farklı olay türlerini depolamak için dört farklı endeks kullanır:

Dizin	Tanım
wazuh - **uyarılar**	Wazuh sunucusu tarafından oluşturulan uyarıları depolar . Bunlar, bir olay yeterince yüksek önceliğe sahip bir kuralı tetiklediğinde her seferinde oluşturulur (bu eşik yapılandırılabilir).
wazuh - **arşivler**	Wazuh sunucusu tarafından alınan tüm olayları (arşiv verileri) , bir kuralı tetikleyip tetiklemediğine bakılmaksızın depolar.
wazuh - **izleme**	Wazuh aracı durumuyla ilgili verileri zaman içinde depolar. Web arayüzü tarafından bireysel aracıların ne zaman olduğunu veya olduğunu göstermek için kullanılır `Active`, `Disconnected`, veya . `Never connected`
wazuh - **istatistikler**	Wazuh sunucu performansıyla ilgili verileri depolar . Web arayüzü tarafından performans istatistiklerini temsil etmek için kullanılır.

Wazuh dizinleyici

Image not found or type unknown

Örnek Sorgu

Wazuh dizinleyici kümesiyle etkileşime girebilirsiniz, bu da çok fazla esneklik sunar. Aramalar yapabilir, belgeler ekleyebilir veya silebilir, dizinleri değiştirebilir ve daha fazlasını yapabilirsiniz.

İşte SSH tekniğini kullanarak son yanal hareket uyarısını döndüren Wazuh indeksleyicisine bir sorgu örneği:

```
GET /wazuh-alerts-4.x-*/_search
{
  "query": {
    "bool": {
      "must": [
        {"term": { "rule.mitre.tactic": "Lateral Movement" } },
        {"term": { "rule.mitre.technique": "SSH" } }
      ]
    }
  },
  "sort": [
    { "timestamp": { "order": "desc" } }
  ],
  "size": 1
}
```

Aşağıda, dizinlenmiş uyarı belgesinin bir parçası olan sorgu sonucunun bir özeti yer almaktadır:

Output


```
{
  "timestamp" : "2022-04-24T17:24:56.110+0000",
  "agent" : {
    "ip" : "10.0.1.52",
    "name" : "Amazon",
    "id" : "001"
  },
  "data" : {
    "srcip" : "68.183.216.91",
    "srcport" : "53820"
  },
  "rule" : {
    "description" : "sshd: insecure connection attempt (scan).",
    "id" : "5706",
    "level" : 6,
    "pci_dss" : ["11.4"],
    "mitre" : {
      "technique" : [
        "SSH"
      ],
      "id" : ["T1021.004"],
      "tactic" : [
        "Lateral Movement"
      ]
    }
  },
  "full_log" : "Apr 24 17:24:55 ip-10-0-1-52 sshd[32179]: Did not receive identification string from 68.183.216.91 p
  "location" : "/var/log/secure",
  "predecoder" : {
    "hostname" : "ip-10-0-1-52",
    "program_name" : "sshd",
```

```
    "timestamp" : "Apr 24 17:24:55"
  },
  "decoder" : {
    "parent" : "sshd",
    "name" : "sshd"
  },
  "GeoLocation" : {
    "city_name" : "Frankfurt am Main",
    "country_name" : "Germany",
    "region_name" : "Hesse"
  }
}
```


Wazuh dizinleyicisi, neredeyse gerçek zamanlı bir arama platformu olduğu için güvenlik analitiği ve altyapı izleme gibi zamana duyarlı kullanım durumları için oldukça uygundur. Bir belgenin dizine eklenmesinden aranabilir hale gelmesine kadar geçen gecikme süresi çok kısadır, genellikle bir saniyedir.

Wazuh indeksleyicisinin hızı, ölçeklenebilirliği ve dayanıklılığının yanı sıra, veri toplama, uyarı, anormallik tespiti ve indeks yaşam döngüsü yönetimi gibi verileri depolamayı ve aramayı daha da verimli hale getiren çeşitli yerleşik özellikleri vardır.

Revision #9
Created 6 December 2023 17:31:57 by LastGuard
Updated 11 December 2024 16:04:54 by Ayşegül Sarıkaya