SOLUTION NOTE

Infoblox Data Connector

Easily Connect the Dots When Investigating Incidents

SUMMARY

Getting access to the right data for event correlation and incident response is not always easy, especially in dynamic environments. It involves manually gathering information from disparate sources, pushing it into a security information and event management (SIEM) platform and spending hours, if not days, sifting through mountains of data. This approach leads to long response times and skyrocketing SIEM costs.

A more efficient solution automatically correlates network context provided by DNS, DHCP and IP address management services (aka DDI) with security events to readily provide security teams with the scope of attacks and the criticality of compromised machines, while filtering out the noise from real threats.

Data Connector

Infoblox's cloud-managed Data Connector automatically collects DNS query and response data and security logs from various sources, filters the information and transfers it to security operations center (SOC) tools, such as a SIEM solution, for easy event correlation. The data is also used to enrich Infoblox reports, furnishing a seamless integrated view into network and security events across on-premises and cloud (hybrid) deployments.

Data Connector is available as part of BloxOne™ Threat Defense, the Infoblox solution suite that works with an organization's existing defenses to protect the network and automatically extend security to digital imperatives, including SD-WAN, IoT and the cloud. Because it is managed in the cloud, the Data Connector utility offers flexible scalability and ease of use for administrators.

Use Cases

Optimized Data Storage and Processing Costs for SIEM

SIEMs are excellent solutions for forensic analysis and correlating events but can be flooded with lots of data/alerts, which can skyrocket costs. DDI data and threat intelligence enrich events in a SIEM solution. DNS query and response information provides valuable insights into device activity including IoT, and it offers visibility into resources and services a client has been accessing. It also indicates malicious activity, such as command and control (C&C) communications from compromised devices or requests from clients to access websites hosting malware.

The Data Connector utility:

- Gathers information from Infoblox DDI, BloxOne DDI and BloxOne Threat Defense solutions
- Filters out legitimate activity
- Sends only suspicious DNS and security event activity along with information on compromised devices to a SIEM platform

SOC teams can now easily connect the dots when investigating incidents, perform analysis and take action. By filtering out unimportant information, Data Connector helps to optimize the amount of data storage and processing costs of a SIEM solution. Integrations are available either out of the box or via Syslog with CEF or LEEF message format.

Enriched and Integrated Reporting for Hybrid Architectures

Cloud-managed Data Connector helps enrich Infoblox reporting by automatically gathering data from DNS, DHCP and IPAM servers and pushing that data to on-premises Infoblox reporting as well as BloxOne Threat Defense cloud reports. This additional data provides deep visibility and context on network and security events, including:

- Device audit trail and fingerprinting
- Metadata including owner, app, security level, location
- Device/user profile and activity

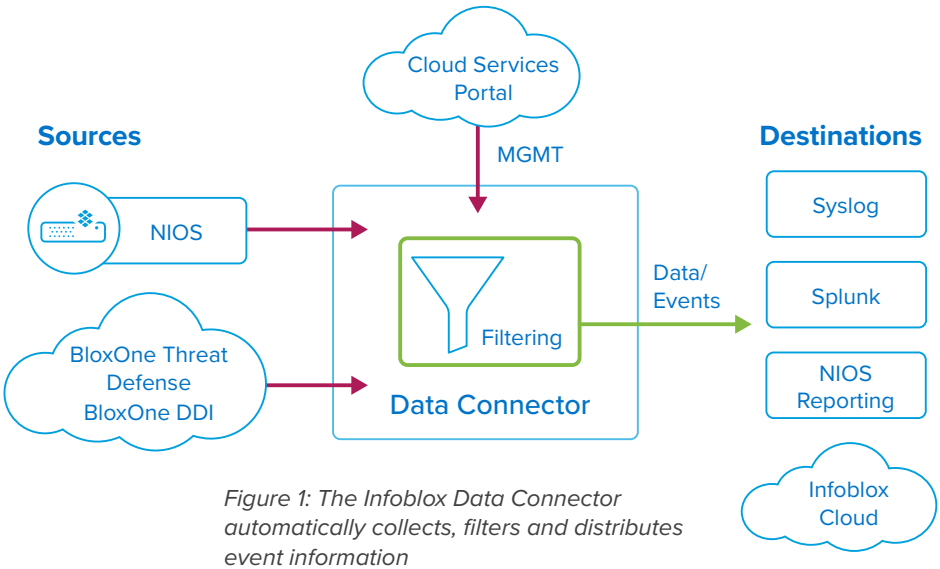

Figure 1: The Infoblox Data Connector automatically collects, filters and distributes event information

Conclusion

Security operations teams need timely access to contextual information to correlate events, understand the scope of a breach and respond to incidents. Cloud-managed Data Connector, as part of BloxOne Threat Defense, provides security teams with the data they need to better understand threats and investigate incidents.

For more information, go to https://www.infoblox.com/ThreatDefense

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com