SOLUTION NOTE

INFOBLOX BLOXONE® UNIVERSAL DATA INSIGHTS CONNECTOR

OVERVIEW

Effective investigations and threat hunting require analyzing insights from multiple security tools.

Unfortunately, analysts today are wasting precious time logging into the various security tools, learning how to use each tool, or chasing the subject matter experts for each tool to gather the needed information. This inefficient, manual process slows investigations, and analysts are often forced to make decisions based on partial information. The Infoblox BloxOne® Universal Data Insights Connector simplifies this process by addressing a wide range of scenarios for the entire security team.

BACKGROUND AND CHALLENGES

Security is not only a necessity, but it must transform and adapt. Today, security teams are overwhelmed with vast on-premises and public/ hybrid cloud enterprise environments, and a plethora of defense-in-depth tools. It becomes an overwhelming process for the cybersecurity teams to independently, and typically manually, manage dozens of security tools and respond to hundreds or thousands of alerts daily. Plus, enterprise networks consist of many network and security devices that generate their own incidents but don't always share information. This lack of interoperability and integration creates silos between network and security teams–creating real concerns about missing cyber threats and taking too long to respond to high-risk security incidents.

INFOBLOX-IBM JOINT SOLUTION

Security effectiveness depends on threat intelligence above all else. The Infoblox BloxOne Universal Data Insights Connector works with IBM Cloud Pak® for Security to help improve security effectiveness and resiliency and to elevate SecOps efficiency. The solution allows organizations to accelerate incident response, remove silos, achieve near real-time visibility, and gain critical forensic insights and network data on incidents. BloxOne Threat Defense from Infoblox taps into DNS, DHCP and IP Address Management (DDI) data for valuable network context on incidents that can automatically be shared with other tools integrated with IBM Cloud Pak for Security to help security teams speed up incident response, remove silos, achieve near real-time visibility, and gain critical forensic insights and network data on incidents. DDI data and threat intelligence enrich events in a SIEM solution, such as IBM Qradar. 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

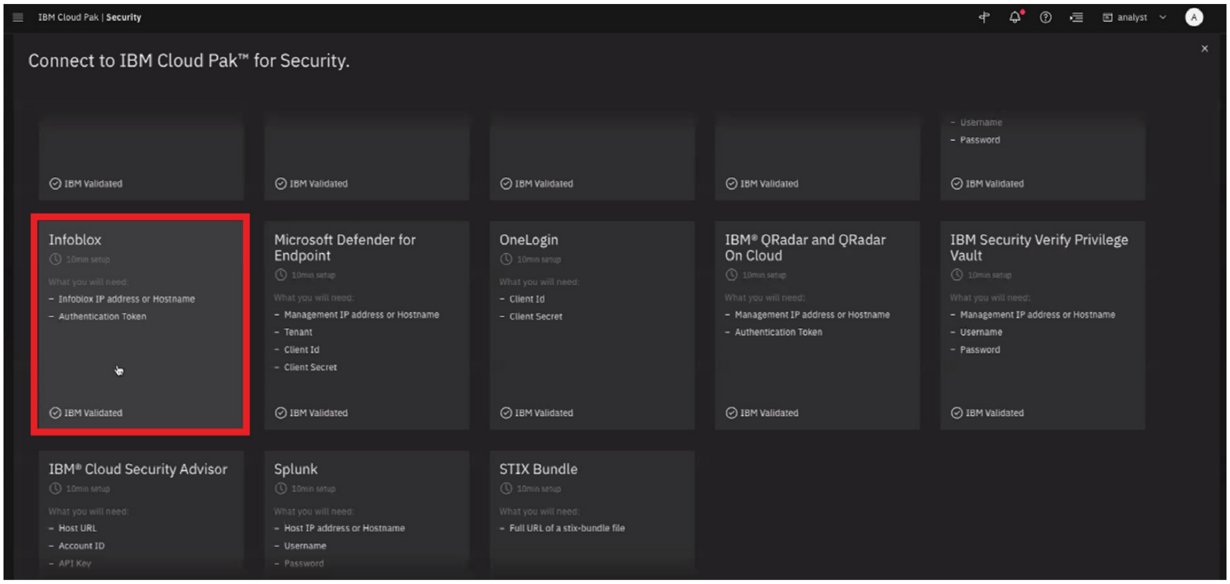
FROM IBM:

The IBM Security Technology Alliance Program is central to our open ecosystem for ISVs to integrate with IBM Security products. This enables our customers to respond to threats faster and reduce integration costs with hundreds of integrations from leading technology vendors. This community will help those vendors explore and implement product integrations, learn about developing custom integrations following best practices and have those integrations made available to customers via the IBM Security App Exchange.

accessing. It also indicates malicious activity, such as command and control (C&C) communications from compromised devices or client requests to access websites hosting malware.

HOW THE SOLUTION WORKS

IBM Cloud Pak for Security provides a unified interface that helps security teams uncover hidden threats and make more informed risk-based decisions. Through a RESTful Universal Data Insights (UDI) API, it integrates with the Infoblox BloxOne Universal Data Insights Connector to provide a federated search for threat indicators across single or multiple service instances. Security teams can drive automated or manual "Am I Affected" scans based on indicators of compromise embedded in threat reports provided by Infoblox Threat Intelligence Insights. Security teams can obtain better visibility and management of risks through the sharing of information.



Connect to IBM Cloud Pak™ for Security.

- Username
- Password

IBM Validated

Infoblox
10min setup
What you will need:
- Infoblox IP address or Hostname
- Authentication Token

IBM Validated

Microsoft Defender for Endpoint
10min setup
What you will need:
- Management IP address or Hostname
- Tenant
- Client Id
- Client Secret

IBM Validated

OneLogin
10min setup
What you will need:
- Client Id
- Client Secret

IBM Validated

IBM® QRadar and QRadar On Cloud
10min setup
What you will need:
- Management IP address or Hostname
- Authentication Token

IBM Validated

IBM Security Verify Privilege Vault
10min setup
What you will need:
- Management IP address or Hostname
- Username
- Password

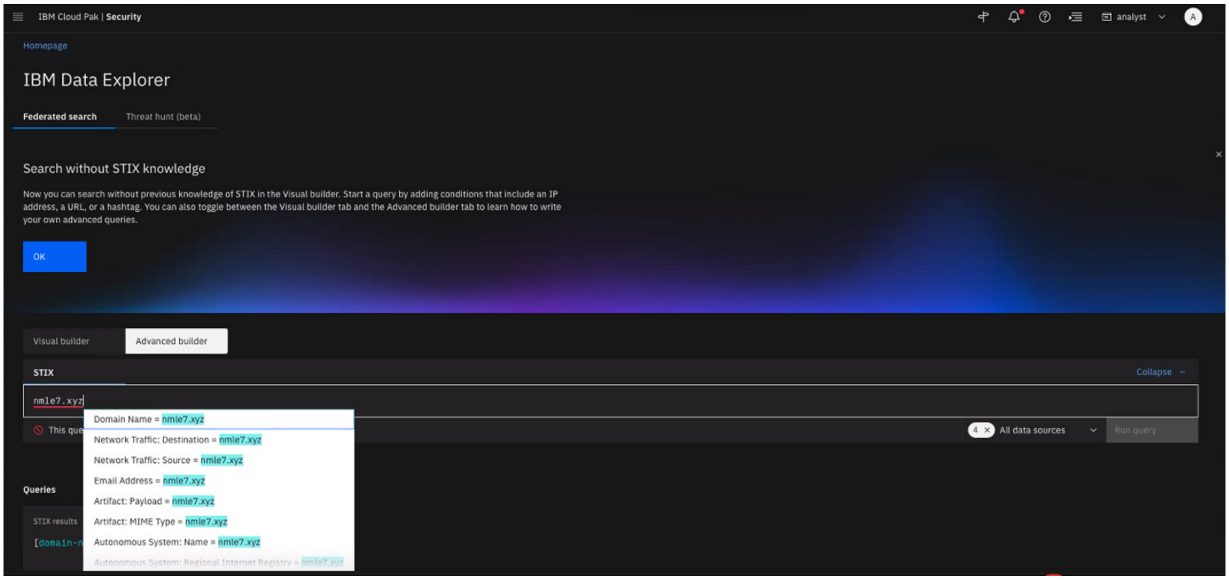
IBM Validated

IBM® Cloud Security Advisor
10min setup
What you will need:
- Host URL
- Account ID
- API Key

Splunk
10min setup
What you will need:
- Host IP address or Hostname
- Username
- Password

STIX Bundle
10min setup
What you will need:
- Full URL of a stix-bundle file

Figure 1: View of the IBM Cloud Pak for Security home page



IBM Data Explorer

Search without STIX knowledge

Now you can search without previous knowledge of STIX in the Visual builder. Start a query by adding conditions that include an IP address, a URL, or a hashtag. You can also toggle between the Visual builder tab and the Advanced builder tab to learn how to write your own advanced queries.

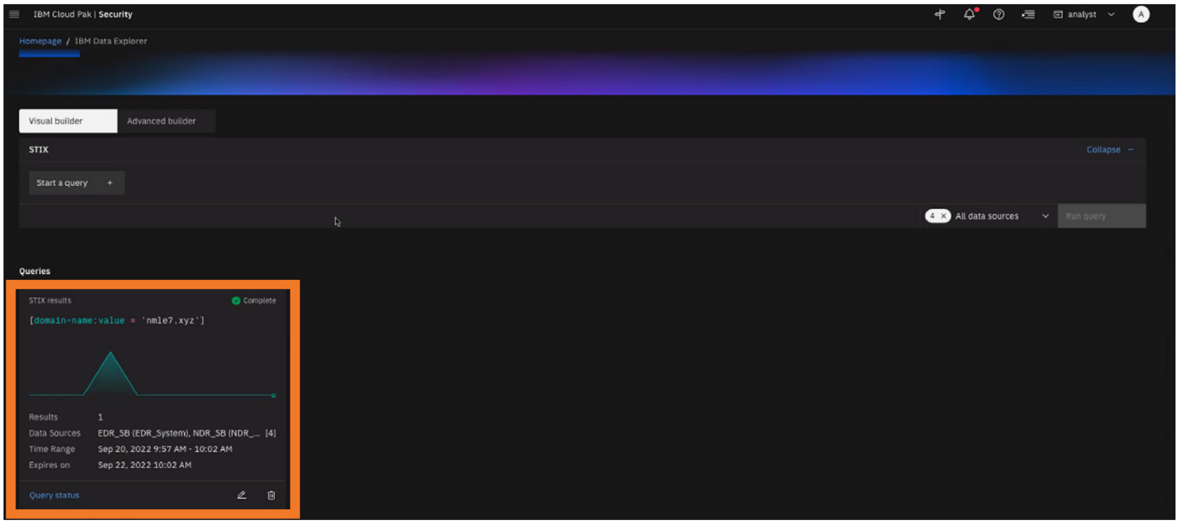
```
nmle7.xyz
```

Domain Name = nmle7.xyz
Network Traffic: Destination = nmle7.xyz
Network Traffic: Source = nmle7.xyz
Email Address = nmle7.xyz
Artifact: Payload = nmle7.xyz
Artifact: MIME Type = nmle7.xyz
Autonomous System: Name = nmle7.xyz
Autonomous System: Regional Internet Registry = nmle7.xyz

This que

[domain-n

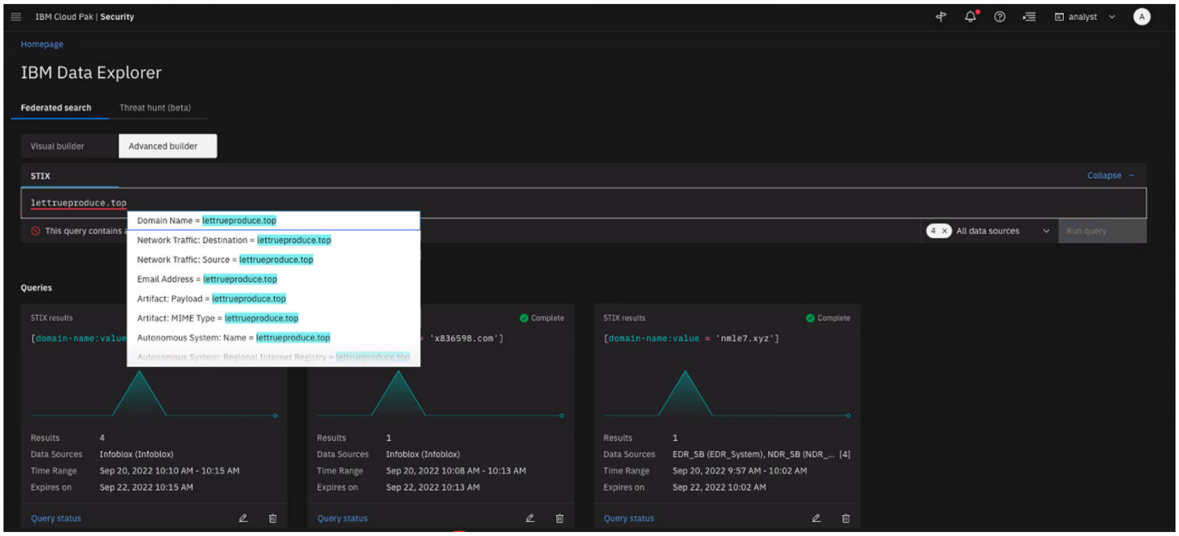
Figure 2: Query on a suspect DNS domain nmie7.xyz



```
[domain-name:value = 'nmle7.xyz']
```

Results 1
Data Sources EDR_SB (EDR_System), NDR_SB (NDR_... [4]
Time Range Sep 20, 2022 9:57 AM - 10:02 AM
Expires on Sep 22, 2022 10:02 AM

Figure 3: Query results on suspected DNS domain nmie7.xyz, including number of hits and time range



```
lettrueproduce.top
```

This query contains

Domain Name = lettrueproduce.top
Network Traffic: Destination = lettrueproduce.top
Network Traffic: Source = lettrueproduce.top
Email Address = lettrueproduce.top
Artifact: Payload = lettrueproduce.top
Artifact: MIME Type = lettrueproduce.top
Autonomous System: Name = lettrueproduce.top
Autonomous System: Regional Internet Registry = lettrueproduce.top

```
[domain-name:value
```

Results 4
Data Sources Infoblox (Infoblox)
Time Range Sep 20, 2022 10:10 AM - 10:15 AM
Expires on Sep 22, 2022 10:15 AM

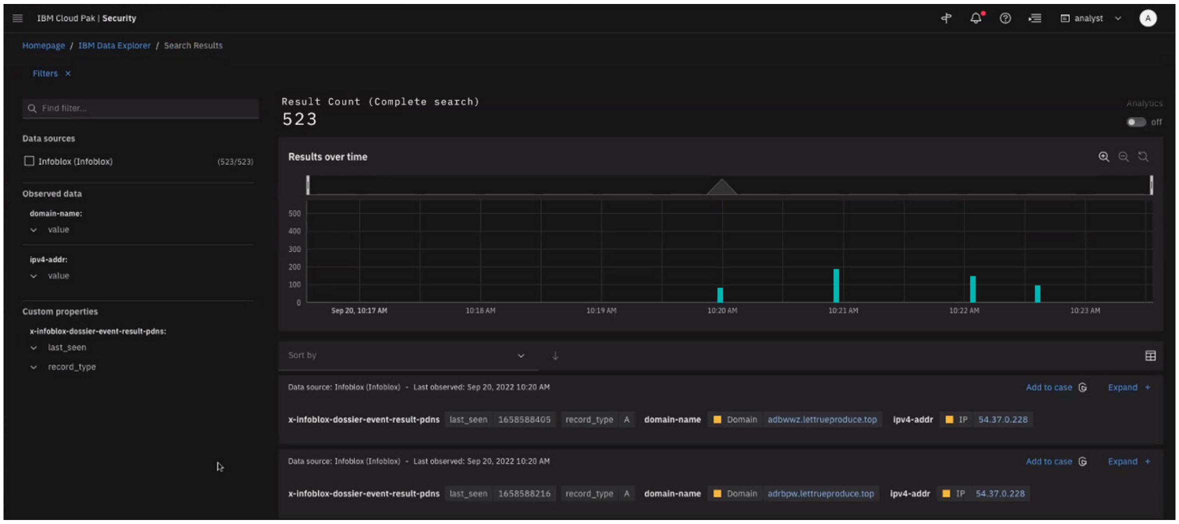
```
'x836598.com']
```

Results 1
Data Sources Infoblox (Infoblox)
Time Range Sep 20, 2022 10:08 AM - 10:13 AM
Expires on Sep 22, 2022 10:13 AM

```
[domain-name:value = 'nmle7.xyz']
```

Results 1
Data Sources EDR_SB (EDR_System), NDR_SB (NDR_... [4]
Time Range Sep 20, 2022 9:57 AM - 10:02 AM
Expires on Sep 22, 2022 10:02 AM

Figure 4: Query on suspected phishing and malware DNS domain lettrueproduce.top



☐ Infoblox (Infoblox) (523/523)

Result Count (Complete search)
523

Data source: Infoblox (Infoblox) - Last observed: Sep 20, 2022 10:20 AM

x-infoblox-dossier-event-result-pdns last_seen 1658588405 record_type A domain-name Domain adbwwz.lettrueproduce.top ipv4-addr IP 54.37.0.228

Data source: Infoblox (Infoblox) - Last observed: Sep 20, 2022 10:20 AM

x-infoblox-dossier-event-result-pdns last_seen 1658588216 record_type A domain-name Domain adrbpw.lettrueproduce.top ipv4-addr IP 54.37.0.228

Figure 5: Results detailing 523 phishing and malware attributes over a time span of several minutes

KEY COMPONENTS

BloxOne Threat Defense

BloxOne Threat Defense operates at the DNS level to see threats that other solutions do not and stops attacks earlier in the threat lifecycle. BloxOne Threat Defense DNS, DHCP, and IPAM (DDI) integration with IBM Cloud Pak for Security offers threat feeds to help improve security while freeing operations and threat intelligence teams to focus on more urgent tasks. Through pervasive automation and ecosystem integration, it drives efficiencies in SecOps, uplifts the effectiveness of the existing security stack, secures digital and work-from-anywhere efforts and lowers the total cost of cybersecurity. The unique hybrid security of BloxOne Threat Defense uses the power of the cloud to detect a broad range of threats while tightly integrating with your on-premises ecosystem. It also provides resiliency and redundancy not available in cloud-only solutions.

Read more about BloxOne® Threat Defense.

BloxOne Threat Defense for Threat Intelligence Data Exchange (TIDE)

Infoblox uses highly accurate machine-readable threat intelligence data that can be shared across the security stack. TIDE (Threat Intelligence Data Exchange) is an optional feature of BloxOne Threat Defense to automate the aggregation, curation, and distribution of threat intelligence across a broad range of infrastructures.

Read more about TIDE.

BloxOne Threat Defense for Dossier™

BloxOne Threat Defense offers a powerful threat indicator research tool, Dossier™, provides analysts, threat researchers, security staff and SOC team members easy access to automatically collected and correlated threat intelligence from dozens of open source, proprietary or premium commercial resources, based on your preferences, and presents it in a single view. This approach allows analysts to quickly pivot between intelligence sources to complete investigations faster and drive a rapid and more effective response.

Read more about Infoblox Dossier™.

KEY BENEFITS

The Infoblox BloxOne Universal Data Insights Connector helps drive efficiencies in SecOps, uplifts existing security stack effectiveness, and lowers the total cost for cybersecurity. It improves visibility and control of even highly evasive threat activity across the threat lifecycle while slashing threat investigation and response times through more effective incident response and fast access to valuable context.

- Collect and manage real-time curated threat intelligence from internal and external sources in a single, open and flexible platform.
- Improve security posture and situational awareness of an organization by sharing the curated threat intelligence data with the security infrastructure.
- Dossier™ supplies quick access to the most recent news from the Infoblox Cyber Intelligence Unit (CIU) on emerging threats. Threat researchers can download and share Infoblox Cyber Intel news reports as PDFs.
- Gain insights into a rich history, detailed timeline and available analysis for the indicator being researched, explore deep insight into related indicators, domains, URLs, and IPs.
- Improve security effectiveness, resiliency and elevate SecOps efficiency by gaining insight into DNS Events, Network Traffic, User Account details, IPv4 Address and MAC Addresses.
- Accelerate threat investigation and responses by automatically correlating event, network, and threat intelligence from dozens of sources to speed investigations by as much as two-thirds.

IBM SECURITY APP EXCHANGE

The IBM Security App Exchange is an ecosystem that helps you extend the capabilities of IBM Security solutions with a host of ready-to-install Business Partner apps and add-ons.

The collaborative platform allows you—whether a customer, developer or IBM Business Partner —to share and install applications, security app extensions and enhancements to IBM Security solutions.

With the IBM Security App Exchange, your enterprise can:

- Increase efficiency and performance of your security solutions with ready-to-install apps
- Find solutions in near real-time
- Improve security app integration and data sharing
- Share best practices and learn from others

Please visit the Infoblox BloxOne Universal Data Insights Connector page at the IBM Security App Exchange to learn more.

infoblox

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20230918v1