EXECUTIVE BRIEF

DoD Zero Trust Architecture

Aligning ThreatQuotient

The ThreatQ data-driven threat intelligence platform is well aligned with the Department of Defense Zero Trust Architecture. This executive brief was written in partnership with Dave Shackleford, Senior Instructor at SANS Institute, and showcases the pivotal role ThreatQ plays in bolstering threat detection, investigation, and response while minimizing redundancy and noise.

Originating from the realm of threat intelligence, the ThreatQ Platform efficiently gathers extended detection and response (XDR) data from diverse sources, including SIEM, vulnerability management tools, critical services, applications, network devices, and endpoint security controls, all facilitated through seamless integrations and API support.

The DataLinq Engine is core to the ThreatQ Platform and focuses on five key requirements:

- Ingestion of a wide variety of data and information
- Normalization of all data including deduplication
- Correlation of data to inform security narratives
- Prioritization of threats for investigation and response
- Translation of data for investigation, automation and export to other tools and services for remediation

Data ingested by ThreatQ is stored in the Threat Library which encompasses a wide variety of threat details including adversaries, indicators of compromise (IoCs), attack patterns, malware, vulnerabilities, documented incidents, campaigns, and more. ThreatQ Smart Collections aggregate specific intelligence to fuel investigations and feed custom monitoring and reporting dashboards.

The ThreatQ Platform can also integrate with tools like EDR to trigger specific actions through APIs. For instance, if it detects a hash value IoC during an investigation, it can automatically block files with that hash on endpoints that can communicate with ThreatQ. ThreatQ is capable of exporting data and actions to EDR, NDR, SIEM, and other tools and includes a continuous feedback loop that is capable of sharing XDR security details back into DataLinq Engine for additional analysis and tuning.

ABOUT THREATQUOTIENT

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven threat intelligence platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data.

ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC.

ThreatQ Platform is a foundation for the DoD Zero Trust Architecture Cyber Threat Intelligence Program defined in 7.5.1 and 7.5.2:

7.5.1 Cyber Threat Intelligence Program Pt1

Associated Capability: Threat Intelligence Integration

Phase: Target Level ZT

Duration: 9.9 Months

Description: The DoD Enterprise works with the organizations to develop and Cyber Threat Intelligence (CTI) program policy, standard and process. Organizations utilize this documentation to develop organizational CTI teams with key mission/task stakeholders. CTI Teams integrate common feeds of data with the Security Information and Event Management (SIEM) for improved alerting and response. Integrations with Device and Network enforcement points (e.g. Firewalls, Endpoint Security Suites, etc.) are created to conduct basic monitoring of CTI driven data.

Outcomes: CTI team is in place with critical stakeholders; Public and Baseline CTI feeds are being utilized by SIEM for alerting; Basic integration points exist with Device and Network enforcement points (e.g., NGAV, NGFW, NG-IPS).

Predecessor(s): NA

Successor(s): In the context of the Cyber Threat Intelligence Program Pt2 and Threat Alerting Pt2, ThreatQ plays a crucial role by eliminating duplicates and prioritizing Cyber Threat Intelligence before sending it to the SIEM. This approach minimizes the noise caused by redundant data from multiple threat feeds, especially since ThreatQ can integrate over 30 commercial feeds, more than 100 open source feeds, and government feeds like DHS-AIS. Additionally, the ThreatQ scoring policy aids in further reducing noise and enhancing defense efficiency, allowing for the prioritization of threats like persistent attackers targeting US Government Agencies over those focused on ransomware attacks in the healthcare sector in Asia.

ThreatQ offers more than 400 integrations through its marketplace, facilitating the connection of threat intelligence with device and network enforcement points. This transforms cyber threat intelligence into actionable insights that can be effectively deployed across various devices. For additional details about these integrations, you can visit: https://marketplace.threatq.com/

7.5.2 Cyber Threat Intelligence Program Pt2

Associated Capability: Threat Intelligence Integration

Phase: Target Level ZT

Duration: 19.5 Months

Description: DoD Organizations expand their Cyber Threat Intelligence (CTI) teams to include new stakeholders as appropriate. Authenticated, private and controlled CTI data feeds are integrated into Security Information and Event Management (SIEM) and enforcement points from the Device, User, Network and Data pillars.

Outcomes: Cyber Threat Intelligence team is in place with extended stakeholders as appropriate; Controlled and Private feed are being utilized by SIEM and other appropriate Analytics tools for alerting and monitoring; Integration is in place for extended enforcement points within the Device, User, Network and Data pillars (UEBA, UAM)

Predecessor(s): Cyber Threat Intelligence Program Pt1

Successor(s): NA

In addition to Cyber Threat Intelligence Feeds, ThreatQ can incorporate pertinent threat intelligence from various aspects, including Device, User, Network, and Data components. For instance, consider sandbox technology, which assesses file maliciousness. ThreatQ can receive data from the sandbox and then disseminate it to enforcement points across the network. Moreover, ThreatQ integrates seamlessly with User and Entity Behavior Analytics (UEBA) and User Activity Monitoring (UAM) tools, further enhancing its capabilities in this regard.

In addition to the DoD Zero Trust Architecture Cyber Threat Intelligence Program defined in 7.5.1 and 7.5.2, ThreatQ can also help with the following requirements:

ID # 6.5.1 Response Automation Analysis - ThreatQ has the ability to automate analysis within its platform and seamlessly collaborate with SOAR (Security Orchestration, Automation, and Response) products, streamlining the execution of playbooks and enhancing their efficiency. For instance, ThreatQ can enrich data before triggering a SOAR product to automate a response, optimizing the entire process.

ID # 6.5.2 Implement SOAR tools – ThreatQ TDR Orchestrator is a SOAR product designed to automate various scenarios involving external Cyber Threat Intelligence. ThreatQ TDR Orchestrator streamlines and automates repetitive and time-consuming tasks typically handled by threat intelligence personnel, resulting in fewer errors and a boost in team productivity.

ID #7.1.1 Threat Alerting Pt1 – ThreatQ facilitates the sharing of more than 30 commercial feeds, over 100 open source feeds, and government feeds (like DHS-AIS) with SIEM and infrastructure products such as XDR platforms. This integration with ThreatQ in the SIEM ecosystem effectively mitigates the issue of redundancy caused by multiple feeds reporting the same information. Without ThreatQ, direct integration between SIEM and Cyber Threat Intelligence (CTI) feeds could result in duplicate reports and redundant actions within the SIEM.

Employing ThreatQ in this context enables the presentation of a single record, complete with timestamps indicating multiple feed reports. This approach mitigates the noise and redundancy associated with direct feed inputs into SIEMs, ultimately enhancing SOC efficiency.

ID# 7.2.2 Threat Alerting Pt2 – ThreatQ offers the capability to share a wide range of feeds, including over 30 commercial, over 100 open source, and government feeds like DHS-AIS, with infrastructure products such as XDR platforms. This integration with infrastructure products effectively diminishes the noise generated by redundant information from multiple feeds. In contrast, direct integration with XDR products can be inefficient, as it may lead to overload if multiple CTI feeds continually report the same event, overwhelming the XDR tool.

Conclusion

The ThreatQ data-driven threat intelligence platform aligns seamlessly with the Department of Defense Zero Trust Architecture, playing a pivotal role in enhancing cybersecurity defenses while reducing redundancy and noise. From ingesting diverse data sources to automating analysis and integrating with various security tools, ThreatQ is a comprehensive solution for effective threat management.

To learn more about how ThreatQ can elevate your cybersecurity strategy, please contact us info@threatq.com.

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven threat intelligence platform helps teams prioritise, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.

Sales@ThreatQ.com • 703.574.9885 • www.threatquotient.com