ATARC ZT Phase II Integrated Lab Read Ahead

Introduction

The DoD Zero Trust Strategy outlines 152 activities across 45 capabilities and 7 pillars, each representing a critical area of protection. Gigamon and Darktrace provide complementary solutions that enhance Zero Trust implementation by addressing core principles like network visibility, threat detection, and automated response across target and mature levels. In this ATARC ZT Phase II Integrated Lab presentation, attendees will see how the joint Gigamon-Darktrace solution addresses numerous ZT activities in 13 scenarios (Refer to Appendix A for descriptions of all scenarios and Appendix B for optional DDIL scenarios).

Gigamon's Role in Zero Trust

Gigamon excels in providing deep network traffic visibility across hybrid environments, including on-premises and cloud. Key features include:

- **Traffic Optimization:** Efficiently aggregates and processes network traffic for analysis.
- **Granular Monitoring:** Offers detailed insights into east-west and north-south traffic flows.
- **Integration with Security Tools:** Feeds enriched metadata into other security platforms for improved detection.

By ensuring complete visibility, Gigamon helps enforce policies and provides critical data for threat identification.

Darktrace's Role in Zero Trust

Darktrace's AI-powered Network Detection and Response (NDR) enhances Zero Trust with:

- **Anomaly Detection:** Identifies deviations from normal behavior to flag potential threats.
- **Autonomous Response:** Leverages AI to respond to threats in real-time without manual intervention.
- **Adaptive Learning:** Continuously learns network behaviors, improving detection accuracy over time while reducing human effort in identifying anomalous behavior.

Darktrace strengthens Zero Trust by detecting hidden threats (zero-day, insider, supply chain, nation-state) and mitigating risks in dynamic, complex environments in real-time.

How Gigamon and Darktrace Work Together

The integration of Gigamon and Darktrace enables enhanced Zero Trust implementation:

1. **Data Enrichment:** Gigamon provides high-quality, optimized traffic data aggregation, enhancing Darktrace's AI detection capabilities across the entire digital estate.
2. **Comprehensive Visibility:** Gigamon's traffic insights cover blind spots not traditionally seen in network traffic, while Darktrace's ML/AI approach analyzes behaviors across the entire network.

3. **Faster Response:** Darktrace uses RAW network traffic along with telemetry sourced by Gigamon to automate threat detection and response.

For example, in a hybrid cloud environment, Gigamon aggregates network traffic from all endpoints, further enhancing Darktrace's capabilities in detection and response—ensuring policy enforcement and minimal disruption.

Conclusion

Gigamon and Darktrace form a powerful duo for implementing Zero Trust. Their collaboration ensures comprehensive visibility, accurate threat detection, and timely responses. Organizations adopting this approach benefit from enhanced security posture, better resource utilization, and adherence to Zero Trust principles.

Appendix A: Scenarios

Scenario 1: An agency employee is working remotely, using personally owned devices, must regularly access a public cloud based, agency application. The employee routinely accesses the system as a standard user but occasionally switches to administrator mode to perform systems maintenance. The user's physical location changes frequently with personal travel. At times, that travel takes the user to countries designated as a high threat due to state-sponsored cyber activity. Beyond standard user and administrator activity, there is a specific instance when the user is using administrator privileges to troubleshoot an issue and accesses another system. Further into the troubleshooting process, the user attempts to access a third system but does not have administrator privileges.

Scenario 2: An agency employee and/or contractor, working on from an agency satellite office and using government furnished equipment, is accessing Internet sites. The sites vary between sites supporting job related research and his/her personal bank. Limited personal use is acceptable per agency policy.

Scenario 3: A contracted employee provides ongoing improvements to an agency system as part of a development team and provides administrator and routine maintenance to the operational system. Development is performed from the contracted employee's corporate offices using devices provides by his/her company. Development is performed on a separate network, isolated from the production network. Both operate within a data center located at the agency's facilities. When appropriate, the contracted employee moves systems from the development environment into production.

Scenario 4: Use the conditions described in Scenario 3 but both the development and production systems are cloud-based.

Scenario 5: A public user accesses an agency's citizen facing system that houses sensitive/PII information. The user must be verified (i.e. Identity proofing) and have an account on the system for access. The user will be entering data into the system but also occasionally checking the status of their request in the system (e.g. TSA PreCheck)

A. system is located on-premises in the agencies' data centers.
B. System is located in cloud environment.

Scenario 6: An agency system interfaces with another agency's system (e.g. accessing fingerprint information as part of a background investigation process). Both systems are public cloud-based. Describe both normal, ongoing operations and an incident when the agency is informed the other agency's system is experiencing an active exploit.

Scenario 7: Use Scenario 6 but both systems are located on-premises in the agencies' data centers.

Scenario 8: Use Scenario 6 but the primary system is located on-premises in the agencies' data centers and the secondary, accessed system is in a public cloud.

Scenario 9: Use Scenario 6 but the primary system is housed in a public cloud and the secondary, accessed system is located on-premises in the agency's data center.

Scenario 10: Use Scenarios 6 through 8 above but address from the perspective the primary agency system is being accessed to gain fingerprint data (PII or High Categorized) by another agency's system.

Scenario 11: The remote users (e.g. telework, off-site) of an agency's cloud-based HVA system are having connectivity issues that are inconsistently kicking them off their session. Outline any tools you provide for administrators' troubleshooting.

Scenario 12: The ICAM administrator has reported a user's credentials were compromised. Describe any tools/methods you provide to validate unauthorized access to systems under the ZTA umbrella has not occurred, either on-premises or cloud-based.

Scenario 13: An agency has decided to perform penetration exercises against their HVA systems operating under the ZTA umbrella, both on-premises and cloud-based. Describe the tools/methods you provide or support to accommodate these penetration exercises.

Appendix B: Optional Use Cases (DDIL)

Optional Use Case 2: Satellite office with highly reliable, robust connectivity
The following assumptions should be applied to this use case:

- Satellite office location may be CONUS or OCONUS.
- Staff size ranges from a dozen to several hundred.
- Robust, reliable connectivity is available from multiple sources.
- Users operate using government furnished equipment on a network with a clearly definable perimeter.
- Users access data and applications located both on-premises, HQ-based on-premise, and in the cloud.

Optional Use Case 3: Bandwidth challenged satellite office and little to no local IT support staff
The following assumptions should be applied to this use case:

- Satellite office location may be CONUS or OCONUS.
- Staff size ranges from 10 to several dozen.
- Connectivity options are limited and sometimes/often prove unreliable.
- Users operate using government furnished equipment on a network with a clearly definable perimeter.
- Users access data and applications located both on-premises, HQ-based on-premise, and in the cloud.