Continuous Cyber Attacks: Building the Next-Gen Infrastructure for the New Normal

Digital infrastructure plays a critical role in blunting cyber attacks.

How can an effective infrastructure be maintained?

1. Provide greater information visibility, context and meaning regarding security events.
2. Use technical analysts to understand the impact of security events in relation to business operations.
3. Drive deeper integration levels for security infrastructure with the rest of the business.
4. Leverage automation for faster response times and scalability.

How do leaders choose from the wide range of tools and technologies available?

1. Create the self-defending enterprise.
2. Focus attention on technology maturity.
3. Align threat intelligence with the business environment.
4. Implement deceptions to trap intruders.
5. Leverage automation.
6. Feed the analytics engine.

A next-generation security infrastructure should:

- Drive deeper integration levels for security infrastructure with the rest of the business.
- Leverage automation for faster response times and scalability.
- Offer flexible and open access to data and features.
- Provide greater information visibility, context and meaning regarding security events.
- Orchestrate existing capabilities to disrupt attacks.
- Break down silos to extract full potential from tools.
- Look to replace multiple older technologies with a single new one.
- Drive greater integration levels for security infrastructure with the rest of the business.
- Give technical analysts the ability to understand the impact of security events in relation to business operations.
- Offer flexible and open access to data and features.

To create an advanced security infrastructure:

1. Create the self-defending enterprise.
2. Focus attention on technology maturity.
3. Align threat intelligence with the business environment.
4. Implement deceptions to trap intruders.
5. Leverage automation.
6. Feed the analytics engine.

To promote security based on business context:

- Leverage automation.
- Focus attention on technology maturity.
- Align threat intelligence with the business environment.

To prepare defenses for what’s coming and hunt for what already might be in the environment:

- Leverage automation.
- Focus attention on technology maturity.
-Align threat intelligence with the business environment.

To enable higher fidelity detection of adversaries, learn from their attacks and limit damage:

- Leverage automation.
- Focus attention on technology maturity.
- Align threat intelligence with the business environment.

To focus security staff on more challenging issues:

- Leverage automation.
- Focus attention on technology maturity.
- Align threat intelligence with the business environment.

To focus security staff on more challenging issues:

- Leverage automation.
- Focus attention on technology maturity.
- Align threat intelligence with the business environment.

To identify subtle threats based on shifting behaviors in networks and devices:

- Leverage automation.
- Focus attention on technology maturity.
- Align threat intelligence with the business environment.

Rethink the organization’s focus on tools:

1. Orchestrate existing capabilities to divert attacks.
2. Break down silos to extract full potential from tools.
3. Look to replace multiple older technologies with a single new one.

Building a strong cyber defense infrastructure:

- Create cross-functional teams.
- Team to develop talent.
- Experiment: Pilot new security technologies and automation solutions, develop use cases and maintain momentum.
- Reuse security’s internal profile.
- Maintain operational excellence by adopting a comprehensive view of infrastructure security requirements.

High performance. Delivered.