Cyber Exposure: Essential Visibility into the Modern Attack Surface

Liz Leon
Security Engineer - Tenable
Interesting Exploit Facts

- **76%** of external attacks are carried out by exploiting software and web application vulnerabilities, according to Forrester.

- **42%** say it is difficult to prioritize which vulnerabilities are most important, according to Forrester.

- **99.9%** of exploited software vulnerabilities that had been compromised more than a year after the associated CVE was published, according to the Verizon 2015 Data Breach Investigations Report.
Economic Impact

Ransomware damage costs are predicted to reach $11.5 billion annually within the next year, according to Cybersecurity Ventures.

Source: 2018 Outlook report Goldman Sachs investment division
Large retail customer needed to find a way to improve security by remediating only the most critical vulnerabilities leveraged by Cyber criminals…

... Focused on CVEs that aligned to threat intelligence data. Reduced in-scope vulns to be remediated to 10% of the previous number …

... Eliminated 100% of incidents resulting from the exploitation of vulnerabilities
There is no such thing as being secure, everyone is just operating at an acceptable level of risk.
It’s Not All About Technology
Clicking Willy-nil...
The attack surface is expanding
Application containers are exploding in adoption...

Docker Adoption

DOCKER ADOPTION IS UP 40% IN ONE YEAR

Percent of Datadog Users


Month (segmentation based on end-of-month snapshot)

500,000+
Dockerized apps in Docker Hub

24 Billion+
Docker Container Downloads
...and are creating a major Cyber Exposure gap

Of organizations with containers in production¹

- 18%

Risk Assessment Index²
Organization’s ability to assess cybersecurity risks

- Containerization Platforms: Score: 52% Grade: F
- DevOps Environments: Score: 57% Grade: F

Average number of vulnerabilities in Docker Hub³

- Official Images: 15.9
- Community Images: 40.5

Sources:
1) Anchore, “Snapshot of the Container Ecosystem,” 2017
3) Tenable, “Sourcing Container Images from Docker Hosts,” 2017
Cyber Exposure Lifecycle: Integrations are key to success

- **Discover**
  - CMDB, Public Cloud Platform, Network Access Control, Network Monitoring

- **Assess**
  - Credential and Privileged Access Management, Mobile Device Management (MDM), IP Address Management

- **Measure**
  - Governance, Risk and Compliance (GRC)

- **Fix**
  - Service Desk / Ticketing / Workflow, Patch Management, Network Access Control

- **Analyze**
  - SIEM, Security Analytics, Endpoint Security
From vulnerability management to strategic guidance

- Live discovery of every asset
- Continuous exposure visibility
- Risk-based scoring & prioritization
- Communication of cybersecurity risk
- Strategic decision support
Four Key Questions

- Where are we exposed?
- Where should we prioritize based on risk?
- How are we reducing exposure over time?
- How do we compare to our peers?
Fundamentals

✓ Vulnerability Management working group
✓ Prioritize (threat data, attack path)
✓ Active scanning alone is no longer adequate for the modern attack surface
✓ A written, measurable patch policy
Fundamentals

✓ Measure and report on non-compliance
✓ Engage system/business owner
✓ Apply compensating controls
✓ Automate as much as possible
Tenable at a Glance

• Founded in 2002
• Exploded with the widespread adoption of Nessus and later, SecurityCenter
• Released Tenable.io in 2017 to introduce the first cyber exposure platform and evolve vulnerability management
• Relentless innovator:
  “Tenable has [massive] brand equity with Nessus, yet [is] one of the most forward-thinking companies in VM.” – Forrester, 2017