Next presentation begins at 12pm...

Effective and Efficient Management of Vulnerabilities from Security Scanning

Richard Mayall
Partner & Technical Director
Acuity Risk Management

David Williams
Information Security Manager
Giesecke Devrient GB Ltd
Effective and Efficient Management of Vulnerabilities from Security Scanning

Richard Mayall
Partner & Technical Director
Acuity Risk Management

David Williams
Information Security Manager
Giesecke Devrient GB Ltd
Typical Cybersecurity Requirements

Enterprise Risk Management
- Cybersecurity, Business Continuity, HSSE, Quality, IT service, vendor management...

Cybersecurity Operations Management
- Rationalization from multiple cybersecurity technologies
- Risk-based prioritization of security operations activities

Cybersecurity Software
- Governance, Risk Management, Compliance (GRC)
- Security Operations, Analytics, Reporting (SOAR)

Cybersecurity Compliance
- ISO 27001, PCI, NIST ....
- Continuous compliance monitoring
- Remediation workflow

Cybersecurity Risk Management
- Enterprise risk reporting
- Asset-based threat & vulnerability mgmt
- Incident management
Overview

• Introductions

• Context – the importance of scanning and efficient remediation

• Nessus / STREAM Integration with Giesecke-Devrient GB:
  • **Phase 1** – Integration to read Nessus scanning data into **STREAM** as ‘Vulnerability Events’
  • **Phase 2** – Workflow / tracking of Events and Remediation Actions
  • **Phase 3** – Addressing operational practicalities and fine-tuning the integration
  • **Phase 4** – Integrated ‘risk prioritised’ reporting

• QUESTIONS
Your presenters...

- **Richard Mayall**  
  Acuity Partner and Technical Director  
  - 32 years experience in software engineering, information security and risk management  
  - Responsible at Acuity for 3rd party solution integrations for STREAM customers

- **David Williams**  
  GDGB Security Manager  
  - 14 years of experience in Information Technology including 8 years of progressive experience in Information Security domains  
  - Responsible at GDGB for Information Security & Risk Management
Frequent breaches are reported...

Probability of a breach: ‘...When rather than If...’

Compliance with Standards, e.g. PCI

Recognised key element of effective security operations (SOAR)

Respected solution options, such as Nessus, Qualys and others

Remediation efficiency is vital - exploits emerge within days or weeks of becoming public...
Challenges

- Frequent scans...
- Vast outputs...
- Criticality of issues varies...
- Need efficient routing to relevant IT staff
- Need to track remediation progress
- Overlap with Asset Management...
• Giesecke-Devrient and Vulnerability Scanning:
  • Various scheme requirements mandate frequent security testing. The schedule for penetration & vulnerability engagements can soon produce many findings which quickly become unmanageable....
  
  • Like a lot of companies we reverted to remediation via excel. Thus bringing issues of confidentiality & integrity and auditability. Who was doing what and when?
  
  • Most critical findings had to be addressed within 48 hrs or sooner depending on the nature of the asset being protected. How to link this effectively with the requirements of configuration management and change control...
  
  • Effectively ensuring all vulnerabilities were actually being addressed was a concern. What happened if something was missed or worse was marked as remediated but wasn’t...?!
Solution relationships

Technical Assurance Solutions

GRC / SOAR Solution

Asset CMDB

Technical Assurance Integration Utility

Qualys

Nessus

Pen Testing
Phase 1 - Integration to parse / read scanning data output

- Asset reconciliation with CMDB system...
- Select, parse and process scanning output file
- Goal: create trackable **Events** with prioritised **Remediation Actions**
- **Assign** and **notify** relevant staff automatically
- Enable managers to **track** and **report** on progress
- Filter detected vulnerabilities...
• Mapping of scanning solution settings to GRC solution settings
• Filtering of which scanning data to process
• Domain stripping, to simplify asset naming
• Need similar configuration settings for each scanning vendor
• We developed a template and field mapping for each product
• And fingerprints to identify nature of incoming data...

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>STREAM Event Impact Label</th>
<th>Process?</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Negligible</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>Low</td>
<td>2</td>
<td>No</td>
</tr>
<tr>
<td>Medium</td>
<td>3</td>
<td>Yes</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
<td>Yes</td>
</tr>
<tr>
<td>Critical</td>
<td>5</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Domain Extensions, e.g.

- .production.uk
- .production.intern
- .production.be
Parse and import data

- Select and parse a scanning output file...
- Detect its type...
- Push the data into the GRC/SOAR solution...
Phase 2 - Workflow / tracking of Events and Remediation Actions

Parse data / Import data into STREAM
Phase 2 - Workflow / tracking of Events and Remediation Actions

Parse data / Import data into STREAM
Vulnerability Events

- Each detected vulnerability created as a distinct **Event**
- All data from the scanning solution carried through
- **Owner** assigned based on configured Asset Ownership
- Email alerts generated.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date of Event</th>
<th>Name</th>
<th>Owner</th>
<th>Event Category</th>
<th>Event Impact</th>
<th>Event Status</th>
<th>Event Type</th>
<th>Date Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>IATC012499-e-workp:8080</td>
<td>04/05/2016</td>
<td>Apache Axix2 Default Administrative Access</td>
<td>Richard Mayall</td>
<td>CGI</td>
<td>4</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC012499-e-workp:8443</td>
<td>04/05/2016</td>
<td>Apache Axix2 Default Administrative Access</td>
<td>Richard Mayall</td>
<td>CGI</td>
<td>4</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC036602-e-workp:2381</td>
<td>04/05/2016</td>
<td>OpenSSL Multiple Remote Security Vulnerabilities</td>
<td>S Jones</td>
<td>General remote service</td>
<td>1</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC0105459-e-workka</td>
<td>04/05/2016</td>
<td>EOL Obasele Software SNMP Version Detected</td>
<td>S Jones</td>
<td>Security Policy</td>
<td>5</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC0105459-e-workdn</td>
<td>04/05/2016</td>
<td>EOL Obasele Software SNMP Version Detected</td>
<td>S Jones</td>
<td>Security Policy</td>
<td>5</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC0105459-e-workip</td>
<td>04/05/2016</td>
<td>EOL Obasele Software SNMP Version Detected</td>
<td>S Jones</td>
<td>Security Policy</td>
<td>5</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC036602-e-workp:2381</td>
<td>04/05/2016</td>
<td>OpenSSL Multiple Remote Security Vulnerabilities</td>
<td>Richard Mayall</td>
<td>General remote service</td>
<td>4</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC045003-e-workp:2381</td>
<td>04/05/2016</td>
<td>Remote User List Disclosure Using NetBIS</td>
<td>Julien Pallard</td>
<td>Information gathering</td>
<td>2</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC036602-e-workp:2381</td>
<td>04/05/2016</td>
<td>OpenSSL Multiple Remote Security Vulnerabilities</td>
<td>Richard Mayall</td>
<td>General remote service</td>
<td>4</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC036602-e-workp:2381</td>
<td>04/05/2016</td>
<td>OpenSSL Multiple Remote Security Vulnerabilities</td>
<td>Julien Pallard</td>
<td>General remote service</td>
<td>1</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
<tr>
<td>IATC045003-e-workp:2381</td>
<td>04/05/2016</td>
<td>Remote User List Disclosure Using NetBIS</td>
<td>Richard Mayall</td>
<td>Information gathering</td>
<td>3</td>
<td>New Vulnerability</td>
<td>Qualys Vulnerability</td>
<td></td>
</tr>
</tbody>
</table>
Remediation Actions

- **Remediation Action** generated for each Vulnerability Event
- **Priority** carried through from scanning solution
- **Due date** determined based on priority
- **Owner** matched with Event, and email alerts generated.

### Actions Screen

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date Raised/Updated</th>
<th>Name</th>
<th>Cost</th>
<th>Priority</th>
<th>Status</th>
<th>Date Closed</th>
<th>Action Owner</th>
<th>Date Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q105459-eworka</td>
<td>04/05/2016</td>
<td>Disable or remove SNMPv1/2c authentication. Use SNMP version 3 aut...</td>
<td>5</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>S.Jones</td>
<td>11/05/2016</td>
</tr>
<tr>
<td>Q105459-eworkdn</td>
<td>04/05/2016</td>
<td>Disable or remove SNMPv1/2c authentication. Use SNMP version 3 aut...</td>
<td>5</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>S.Jones</td>
<td>11/05/2016</td>
</tr>
<tr>
<td>Q105459-eworknp</td>
<td>04/05/2016</td>
<td>Disable or remove SNMPv1/2c authentication. Use SNMP version 3 aut...</td>
<td>5</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>S.Jones</td>
<td>11/05/2016</td>
</tr>
<tr>
<td>Q12499-eworknpn:8050</td>
<td>04/05/2016</td>
<td>Change the password for the &quot;admin&quot; account. This can be done by c...</td>
<td>4</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>Richard Mayall</td>
<td>25/05/2016</td>
</tr>
<tr>
<td>Q12499-eworktn:8443</td>
<td>04/05/2016</td>
<td>Change the password for the &quot;admin&quot; account. This can be done by c...</td>
<td>4</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>Richard Mayall</td>
<td>25/05/2016</td>
</tr>
<tr>
<td>Q38602-eworkpn:2381</td>
<td>04/05/2016</td>
<td>Customers are advised to install OpenSSL versions 0.9.8za, 1.0.0m, 1...</td>
<td>4</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>Richard Mayall</td>
<td>25/05/2016</td>
</tr>
<tr>
<td>Q38602-eworktn:2381</td>
<td>04/05/2016</td>
<td>Customers are advised to install OpenSSL versions 0.9.8za, 1.0.0m, 1...</td>
<td>4</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>Richard Mayall</td>
<td>25/05/2016</td>
</tr>
<tr>
<td>Q70003-eworkpn</td>
<td>04/05/2016</td>
<td>Null NetBIOS sessions can be disabled using the following methods: ...</td>
<td>4</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>Richard Mayall</td>
<td>25/05/2016</td>
</tr>
<tr>
<td>Q70003-eworktn</td>
<td>04/05/2016</td>
<td>Null NetBIOS sessions can be disabled using the following methods: ...</td>
<td>4</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>Richard Mayall</td>
<td>25/05/2016</td>
</tr>
<tr>
<td>Q45003-eworktn</td>
<td>04/05/2016</td>
<td>It is recommended that you disable null sessions. Before editing any ...</td>
<td>3</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>Richard Mayall</td>
<td>18/06/2016</td>
</tr>
<tr>
<td>Q45003-eworktn:1</td>
<td>04/05/2016</td>
<td>It is recommended that you disable null sessions. Before editing any ...</td>
<td>2</td>
<td>4</td>
<td>Not started</td>
<td></td>
<td>Julien Pallard</td>
<td>03/07/2016</td>
</tr>
<tr>
<td>Q38602-eworktp:2381</td>
<td>04/05/2016</td>
<td>Customers are advised to install OpenSSL versions 0.9.8za, 1.0.0m, 1...</td>
<td>1</td>
<td>1</td>
<td>Not started</td>
<td></td>
<td>S.Jones</td>
<td>02/08/2016</td>
</tr>
<tr>
<td>Q38602-eworktn:1:2381</td>
<td>04/05/2016</td>
<td>Customers are advised to install OpenSSL versions 0.9.8za, 1.0.0m, 1...</td>
<td>1</td>
<td>1</td>
<td>Not started</td>
<td></td>
<td>Julien Pallard</td>
<td>02/08/2016</td>
</tr>
</tbody>
</table>
Phase 3 – Operational review and fine-tuning

- Important to understand **how** Security Ops carry out remediation activities...
- Developed filterable tracking & reporting for **Open** Vulnerability Events / Actions
- ...with configurable ‘standard’ **Action Closure Options**
- Allows bulk update of tracking data in STREAM to align with estate-wide patching, for example...

**Action Closure Options**

- **Install missing security patch**
- **Upgrade Operation System to latest version**
- **Replace legacy system / process**
- **Restrict access to system / folder / files**
- **Reconfigure security settings to compliant level**
Audit trails are crucial

- Security ops staff needed an **efficient** way to update the Events and Actions in our GRC solution, to align with their activities
- The Technical Assurance Utility can quickly update and close out Vulnerability Events that have been dealt with
- ...and it populates the **Audit Trail**...
Phase 4 - Integrated risk reporting

- STREAM GRC system holds:
  - IT Asset details
  - Key Business Environment details
  - Linkages between Assets and Business Environments...
  - Threat lists, leading to Risk Registers for each Business Environment

- We introduced configurable logic to **identify** and **elevate** appropriate risks where the Business Environment depends on an Asset with ‘LIVE’ vulnerabilities...
Elevated risks due where ‘vulnerable’ assets are related to key processes...

<table>
<thead>
<tr>
<th>Reference</th>
<th>Threat Description</th>
<th>Asset</th>
<th>Residual Risk (£1,000)</th>
<th>Business Impact (£1,000s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Corrupt or loss of Application Data</td>
<td>Trading Process</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>A</td>
<td>Deliberate Application Mauze by Authorised User</td>
<td>Trading Process</td>
<td>68</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Deliberate Application Mauze by Outxader</td>
<td>Trading Process</td>
<td>289</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Eavesdropping or oher communications network interference</td>
<td>Trading Process</td>
<td>340</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Denial of Service Attack</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Malicious Software</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>External System Hacking</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Critical Service Failure</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Equipment Failure</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Platform Failure</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Network Failure</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Loss or Unavailability of Key Staff</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Loss or Theft of Mobile Devices</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Security incident resulting from use of system tools</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Loss or Unavailability of Premises</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Unauthorised Entry to Rooms and Facilities</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
<tr>
<td>A</td>
<td>Insecure 3rd party Relationship</td>
<td>Trading Process</td>
<td>290</td>
<td>500</td>
</tr>
</tbody>
</table>

Relevant risks elevated, while Event Vulnerabilities remain ‘LIVE’
• **Audit Trail** shows:
  • Initial risk assessment
  • Residual risk estimate taking into account mitigating controls
  • Elevated Residual Risk, due to Vulnerability Event being detected on a dependant asset
  • Rationale
  • Remediation ownership...

• **Risk Delta** concept for an Event:
  • A Vulnerability Event can elevate multiple risks in this way...
  • ...because a vulnerable asset might be related to several different threats, and underpin many business environments
  • It is therefore possible to sum the total Risk Delta for each ‘LIVE’ Vulnerability Event...
Risk Weighted priority...

- Scanning solution vendors use their own Impact ratings (e.g. ‘Medium’ or ‘3’)
- Some tools include CVSS (Common Vulnerability Scoring System) ratings
- The Risk Weighted Priority here is a ‘points system’ which sums the Total Risk Delta for the Event, taking into account all risks which are ‘elevated’ by the vulnerability...

<table>
<thead>
<tr>
<th>Event Reference</th>
<th>Event Impact</th>
<th>Risk Weighted Priority</th>
<th>Asset Name</th>
<th>Event Name</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q105459-eworka</td>
<td>5</td>
<td>9574</td>
<td>eworka</td>
<td>EOL/Obsolete Software SNMP Version</td>
<td>Simple Network Management Protocol (SNMP) is an &quot;Internet-standard protocol for managing devices on IP networks.&quot; The authentication of clients of earlier versions of SNMP may be performed only by a &quot;community&quot; of &quot;neighbors.&quot; In later versions, authentication is performed by the user. Apache Axis2 is a Web Services/SOAP/WSDL engine.</td>
</tr>
<tr>
<td>Q105459-eworkdn</td>
<td>5</td>
<td>9574</td>
<td>eworkdn</td>
<td>EOL/Obsolete Software SNMP Version</td>
<td>Simple Network Management Protocol (SNMP) is an &quot;Internet-standard protocol for managing devices on IP networks.&quot; The authentication of clients of earlier versions of SNMP may be performed only by a &quot;community&quot; of &quot;neighbors.&quot; In later versions, authentication is performed by the user.</td>
</tr>
<tr>
<td>Q12499-eworkpn:80</td>
<td>4</td>
<td>2311</td>
<td>eworkpn</td>
<td>Apache Axis2 Default Administrative</td>
<td>The instance of Axis2 on the target allows administrative access with default credentials. Apache Axis2 is a Web Services/SOAP/WSDL engine.</td>
</tr>
<tr>
<td>Q38602-eworkpn:23</td>
<td>4</td>
<td>2311</td>
<td>eworkpn</td>
<td>OpenSSL Multiple Remote Security</td>
<td>The instance of Axis2 on the target allows administrative access with default credentials. The OpenSSL Project is an Open Source toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a general purpose cryptography library.</td>
</tr>
<tr>
<td>Q70003-eworkpn</td>
<td>4</td>
<td>2311</td>
<td>eworkpn</td>
<td>Null Session/Password NetBIOS Access</td>
<td>Unauthorized users can connect to this NetBIOS service without a password. Unauthorized users may be able to exploit this vulnerability to obtain sensitive information.</td>
</tr>
</tbody>
</table>
Graphical reporting...
Being able to immediately inject the raw unaltered output from Nessus directly into STREAM created an ideal remediation platform. Each finding being categorised as an Event allocated to an individual with information to mitigate linked to an Action. At this point you are really being ‘spoon fed’ the ‘solution’.

The ability to quickly identify your critical findings and link to unique infrastructure; DMZ, Production, R&D etc. is certainly beneficial in managing the process.

Once allocated, the responsible individual is emailed with a list of allocated actions aiding and speeding up the allocation of work packages to be completed.

On completion of the remediation process the data base is backed up and the data purged from the system being available to recover at a later date for review or audit purposes.
Integration of vulnerability scanning with an asset based, risk based alerting system can be hugely beneficial, starting with rapid assignment of remediation actions to the right Ops staff.

- There are strong links between technical asset ownership, and remediation activities: Define clear technical asset ownership early on.
- Pre-define common Remediation Action types
- Important to align any such integration carefully with HOW remediation activities are carried out.
- Build into your approach the ability to deal with the most critical issues first.
- Prioritisation of vulnerabilities and remediation actions based on Risk Delta data provides a very important, business oriented view of the risk position where there are known ‘live’ vulnerabilities.
QUESTIONS?

Phase 1 – Parsing & reading Qualys / Nessus output data
Phase 2 – Workflow and remediation actions
Phase 3 – Operational review and fine-tuning
Phase 4 – Integration with Risk Management