Effort Doesn’t Equal Effectiveness
Measuring and Optimizing Your Security Stack

Evan Peña
FireEye Global Red Team Lead

Jeff Seely
Director of Security Effectiveness
Jeff Seely
Director of Security Effectiveness at Verodin

- Nearly 20 years in Information Security
- Hands on with Red Team, Blue Team, and SOC
- Founder of Relay Security – focused on penetration testing, security assessments for critical infrastructure industry
- Maximize the value of Verodin for prospects and customers
The FireEye Ecosystem

Verodin Security Instrumentation
Platform Synergies with Helix and FireEye’s Portfolio
A Powerful Combination

VERODIN

- Overview
- Value Proposition
- Demo

VERODIN

- Refining Existing Service Offerings
- Introducing New Service Offerings
- Case Study
BROKEN FORMULA

SECURITY INVESTMENTS + SECURITY EFFORT ≠ SECURITY EFFECTIVENESS
Cybersecurity today is based on **ASSUMPTIONS**
Cybersecurity today is based on **assumptions**

**WE ASSUME:**
Technologies work as vendors claim
Cybersecurity today is based on ASSUMPTIONS

WE ASSUME:
Technologies work as vendors claim

WE ASSUME:
Products are deployed and configured correctly
Cybersecurity today is based on **ASSUMPTIONS**

**WE ASSUME:**
Technologies work as vendors claim

**WE ASSUME:**
Products are deployed and configured correctly

**WE ASSUME:**
People are correctly handling events and processes are effective
Cybersecurity today is based on **ASSUMPTIONS**

**WE ASSUME:**
- Technologies work as vendors claim
- Products are deployed and configured correctly
- People are correctly handling events and processes are effective
- Changes to the environment are properly understood, communicated and implemented
Executives are more focused on security

- Critical Digital Assets Protected?
- Are we susceptible to the attack that just happened to company X?
- Could actor group (XYZ) compromise us?
- Can we be compromised by a malicious insider or accidental loss?
- Where can we reduce our budget?
Executives are more focused on security

Unable to answer key questions

- Critical Digital Assets Protected?
- Are we susceptible to the attack that just happened to company X?
- Could actor group (XYZ) compromise us?
- Can we be compromised by a malicious insider or accidental loss?
- Where can we reduce our budget?

Verodin provides quantifiable evidence of security effectiveness
VERODIN’S CORE BUSINESS VALUE
VERODIN’S CORE BUSINESS VALUE

Control Effectiveness / Configuration Assurance

• Are our controls working the way we expect them to?

• Are they properly configured?
VERODIN’S CORE BUSINESS VALUE

Control Effectiveness / Configuration Assurance

- Are our controls working the way we expect them to?
- Are they properly configured?

Optimization

- Are we able to increase the efficiency of the dollars already spent?
- Are we using the full value of our existing tools?
- Are we maximizing ROI?
VERODIN’S CORE BUSINESS VALUE

Control Effectiveness / Configuration Assurance

- Are our controls working the way we expect them to?
- Are they properly configured?

Optimization

- Are we able to increase the efficiency of the dollars already spent?
- Are we using the full value of our existing tools?
- Are we maximizing ROI?

Rationalization

- Where are our overlaps and true gaps?
- Can tools be removed from the stack?
- Can we simplify the environment?
VERODIN’S CORE BUSINESS VALUE

Control Effectiveness / Configuration Assurance
- Are our controls working the way we expect them to?
- Are they properly configured?

Optimization
- Are we able to increase the efficiency of the dollars already spent?
- Are we using the full value of our existing tools?
- Are we maximizing ROI?

Rationalization
- Where are our overlaps and true gaps?
- Can tools be removed from the stack?
- Can we simplify the environment?

Known Good Baseline
VERODIN’S CORE BUSINESS VALUE

Control Effectiveness / Configuration Assurance
• Are our controls working the way we expect them to?
• Are they properly configured?

Optimization
• Are we able to increase the efficiency of the dollars already spent?
• Are we using the full value of our existing tools?
• Are we maximizing ROI?

Rationalization
• Where are our overlaps and true gaps?
• Can tools be removed from the stack?
• Can we simplify the environment?

Known Good Baseline

Continuous Validation
Environmental Drift Detection
VERODIN’S CORE BUSINESS VALUE

Control Effectiveness / Configuration Assurance

- Are our controls working the way we expect them to?
- Are they properly configured?

Optimization

- Are we able to increase the efficiency of the dollars already spent?
- Are we using the full value of our existing tools?
- Are we maximizing ROI?

Continuous Validation

Rationalization

- Where are our overlaps and true gaps?
- Can tools be removed from the stack?
- Can we simplify the environment?

Known Good Baseline

Environmental Drift Detection

Demonstrate improvement over time
ARCHITECTURE
ARCHITECTURE

INTEGRATIONS

DIRECTOR

SIEM  NGFW  IDS/IPS  DLP  EDR  AV

NETWORK  ENDPOINT  EMAIL  CLOUD

ACTORS
VERODIN’S CORE BUSINESS VALUE

Control Effectiveness / Configuration Assurance

- Are our controls working the way we expect them to?
- Are they properly configured?

Optimization

- Are we able to increase the efficiency of the dollars already spent?
- Are we using the full value of our existing tools?
- Are we maximizing ROI?

Rationalization

- Where are our overlaps and true gaps?
- Can tools be removed from the stack?
- Can we simplify the environment?

Known Good Baseline

Environmental Drift Detection

Demonstrate improvement over time

Continuous Validation
Evan Peña

- Lead for Verodin integration into Mandiant services
- Been with Mandiant 7+ years
- 2 years in ALX office, 2+ years in LA office, Now in Texas

- Developed tools such as:
  - ADEnumerator
  - EyeWitness Active Scan
  - WMImplant Contributor
  - Veil 3 Contributor
Expanding Mandiant’s Professional Services

Where we are today

Red Team for Security Operations
aka Red Team

Incident Response
aka Blue Team
Expanding Mandiant’s Professional Services

What’s New

Red Team for Security Operations aka Red Team

Incident Response aka Blue Team

Purple Team
**Purple Team: New Name, Similar Game**

- Replaces the current Red Team for Security Operations ("RTSO").
- Automates scenario-based attacker scenarios with Verodin.
- Maps to the MITRE ATT&CK framework.
- New scoring metrics and scorecard
- New report templates, plan template, and playbooks.
Attack Lifecycle Mapped against MITRE

<table>
<thead>
<tr>
<th>Prevent</th>
<th>Detect</th>
<th>Respond</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Initial Reconnaissance
- Initial Access

Initial Compromise
- Initial Access, Execution, Defense Evasion

Establish Foothold
- Execution, Persistence, Defense Evasion

Escalate Privilege
- Privilege Escalation, Credential Access

Internal Reconnaissance
- Discovery, Collection, Defense Evasion

Move Laterally
- Persistence, Command and Control, Defense Evasion

Maintain Presence
- Credential Access, Lateral Movement, Defense Evasion

Complete Mission
- Exfiltration, Impact
Continuous Purple Team
Spring Training for Security Ops

Average engagement: 3 months

Mandiant re-runs failed scenarios weekly for 2-3 months.

Timing
Continuous Practice
Baseline & Re-assess
Continuous Improvement

- Start with baseline Purple Team,
- Conclude with re-appraisal Purple Team

Customers continue training to improve detection & response to failed scenarios.
Strategic Services

Technical validation - automated

- Response Readiness Assessments
- Security Program Assessments
- Justify and influence observations with technical evidence
- Long term testing of a client’s security transformation
Technical Implementation Options
# Infrastructure Implementation Options

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th>Preferred</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Mandiant actions</td>
<td>45</td>
<td>60</td>
<td>85</td>
</tr>
<tr>
<td><strong>Cloud Infrastructure:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Director &amp; Network Actor</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td><strong>On-Premise Infrastructure:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Actor</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Endpoint Actor</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>SIEM Integration</td>
<td>Optional</td>
<td>Optional</td>
<td>Preferred</td>
</tr>
<tr>
<td>Endpoint Detection Integration</td>
<td>Optional</td>
<td>Optional</td>
<td>Preferred</td>
</tr>
</tbody>
</table>

![Diagram showing network connections between NA_internet, Internet, Desktop Users, EA_win10, and EA_win7]
Use Case
Use Case – Purple Team

**Sector:** Financial

**Scope:** Hired Mandiant to perform a Purple Team Assessment to assess and enhance Security Operation Center prevention, detection, & response capabilities

**Length:** 2 weeks with 1 red teamer and 1 incident response consultant

**Deployment:** Preferred Verodin Implementation (60 actions)
- 1 cloud network actor, 2 on-prem network actor, 2 on-prem endpoint actors, and SIEM integration
## Use Case – Specific Category Score

<table>
<thead>
<tr>
<th>Persistence Type</th>
<th>Letter Grade</th>
<th>Numeric Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Scripts</td>
<td>C</td>
<td>75</td>
</tr>
<tr>
<td>New Service</td>
<td>A</td>
<td>95</td>
</tr>
<tr>
<td>Scheduled Task</td>
<td>A</td>
<td>95</td>
</tr>
<tr>
<td>Startup Folder</td>
<td>C</td>
<td>75</td>
</tr>
<tr>
<td>Registry Run Key</td>
<td>F</td>
<td>65</td>
</tr>
<tr>
<td>Overall Score</td>
<td>B</td>
<td>81</td>
</tr>
</tbody>
</table>
## Use Case – Overall Score

<table>
<thead>
<tr>
<th>Category</th>
<th>Initial Compromise</th>
<th>Establish Foothold</th>
<th>Escalate Privileges</th>
<th>Internal Recon</th>
<th>Lateral Movement</th>
<th>Maintain Presence</th>
<th>Complete Mission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Scores</td>
<td>B</td>
<td>B</td>
<td>A</td>
<td>F</td>
<td>C</td>
<td>B</td>
<td>F</td>
</tr>
<tr>
<td><strong>Overall Score</strong></td>
<td><strong>C+</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>79.28</strong></td>
</tr>
</tbody>
</table>
Use Case – Continuous Purple Team

**Sector:** Health Care

**Scope:** Hired Mandiant to perform a Purple Team Assessment to assess and enhance Security Operation Center prevention, detection, & response capabilities

**Length:** 3 months – 2 Purple Teams, re-ran failed actions weekly, monthly scores

**Deployment:** Advanced Verodin Implementation (75 actions)
1 cloud network actor, 3 on-prem network actor, 2 on-prem endpoint actors, EDR & SIEM integration
Use Case – Continuous Purple Team

Monthly scores to track progress against the attacker lifecycle

Effectiveness Trend Over Time

- Initial Compromise
- Establish Foothold
- Escalate Privileges
- Internal Recon
- Lateral Movement
- Persistence
- Complete Mission

<table>
<thead>
<tr>
<th></th>
<th>July</th>
<th>August</th>
<th>September</th>
<th>October</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Compromise</td>
<td>68</td>
<td>71</td>
<td>76</td>
<td>80</td>
</tr>
<tr>
<td>Establish Foothold</td>
<td>69</td>
<td>71</td>
<td>78</td>
<td>80</td>
</tr>
<tr>
<td>Escalate Privileges</td>
<td>68</td>
<td>78</td>
<td>78</td>
<td>82</td>
</tr>
<tr>
<td>Internal Recon</td>
<td>72</td>
<td>82</td>
<td>87</td>
<td>90</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>72</td>
<td>84</td>
<td>87</td>
<td>86</td>
</tr>
<tr>
<td>Persistence</td>
<td>71</td>
<td>84</td>
<td>87</td>
<td>86</td>
</tr>
<tr>
<td>Complete Mission</td>
<td>76</td>
<td>80</td>
<td>87</td>
<td>86</td>
</tr>
</tbody>
</table>
Thank you.