Brian Contos
CISO, Verodin

brian.contos@verodin.com
+1 (408) 834.5815
@BrianContos

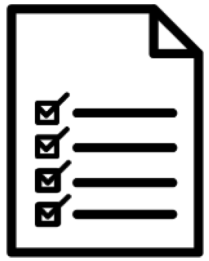
VERODIN™
Security. Instrumented.

CONFIDENTIAL - NOT FOR DISTRIBUTION
© 2019 VERODIN INC. ALL RIGHTS RESERVED

CBYERSECURITY HAS A BROKEN FORUMLA

SECURITY
INVESTMENTS

+



SECURITY
EFFORT

≠

SECURITY
EFFECTIVENESS

CONFIDENTIAL - NOT FOR DISTRIBUTION
© 2019 VERODIN INC. ALL RIGHTS RESERVED

FUNDAMENTAL CHALLENGE

Cybersecurity today is based on ASSUMPTIONS
We simply haven't had a way to MEASURE & generate EVIDENCE

WE ASSUME:
Technologies work as vendors claim

WE ASSUME:
Products are deployed and configured correctly

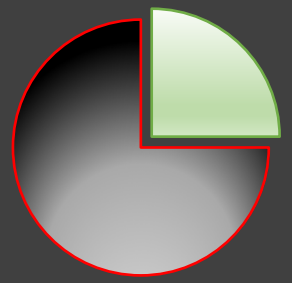
WE ASSUME:
People are correctly handling events and processes are effective

WE ASSUME:
Changes to the environment are properly understood, communicated and implemented

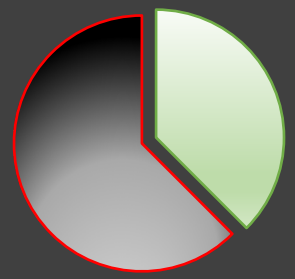
CONFIDENTIAL - NOT FOR DISTRIBUTION
© 2019 VERODIN INC. ALL RIGHTS RESERVED

ASSUMPTION-BASED, NOT EVIDENCE-BASED SECURITY

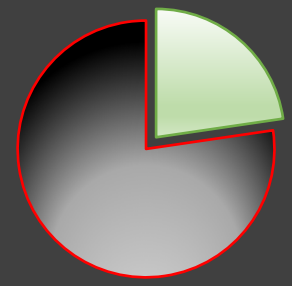
~25% of prevention works



~45% of detection works



~22% of correlation alerts work



Resulting in

- Poor rationalization: validation, prioritization, investment, and retirement
- Limited security value with time, money, and resource waste
- Leadership decisions based on inaccurate and incomplete measures

CONFIDENTIAL - NOT FOR DISTRIBUTION
© 2019 VERODIN INC. ALL RIGHTS RESERVED

VERODIN SIP. NOT JUST BETTER. DIFFERENT.

Controls Effectiveness Validation: Identifying Gaps

Optimization, Mapping & Assurance: Tuning Prescriptively

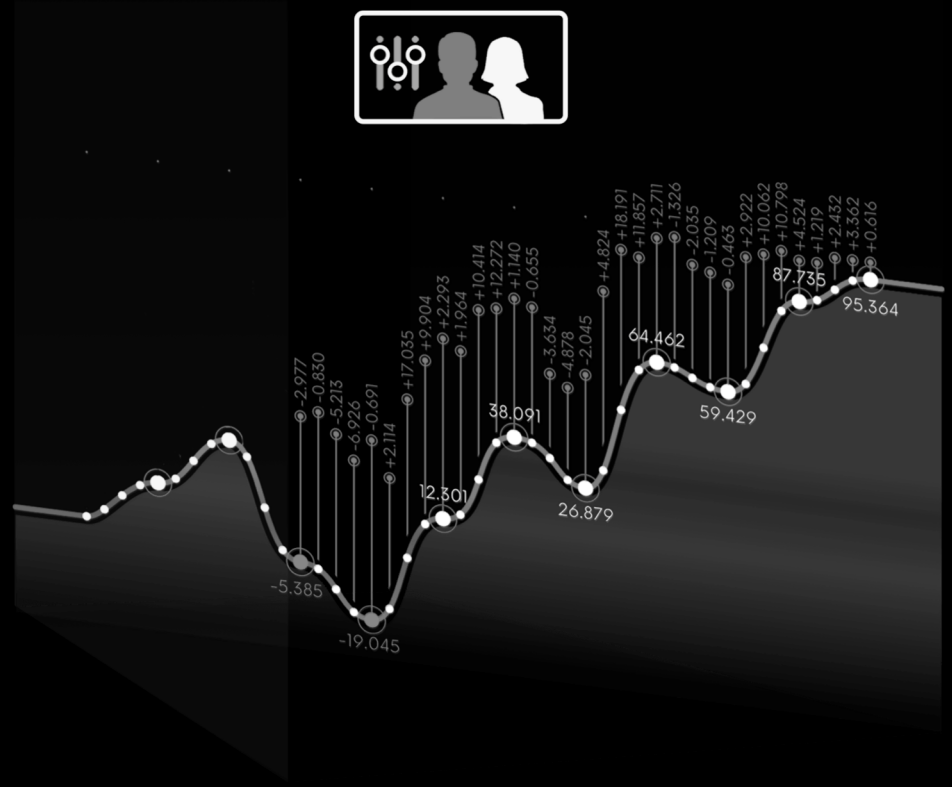
Rationalization: Value, Investment Prioritization & Retirement

Known Good Baseline: Environmental Drift Automation

Reporting & Communicating Security Effectiveness: Proof

CONFIDENTIAL - NOT FOR DISTRIBUTION
© 2019 VERODIN INC. ALL RIGHTS RESERVED

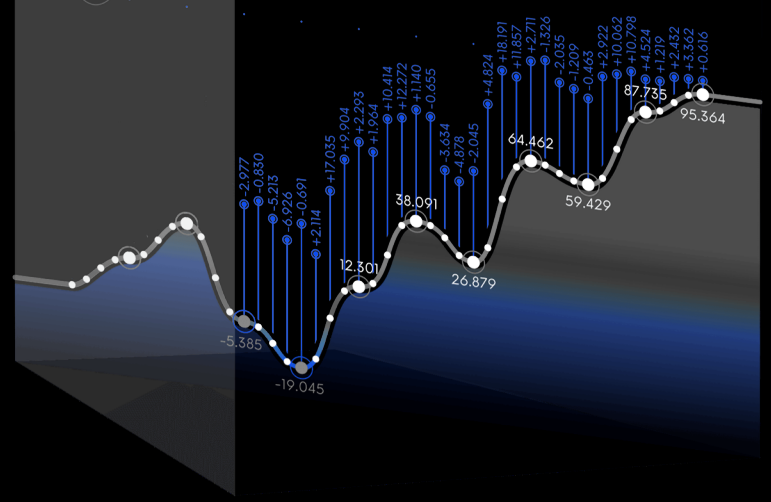
DIRECTOR


-2.977
-0.830
-5.213
-6.926
-0.691
+2.114
+17.035
+9.904
+2.293
+1.964
+10.414
+12.272
+1.140
-0.655
-3.634
-4.878
-2.045
+4.824
+18.191
+11.857
+2.711
-1.326
-2.035
-1.209
-0.463
+2.922
+10.062
+10.798
+4.524
+1.219
+2.432
+3.362
+0.616
-5.385
-19.045
12.301
38.091
26.879
64.462
59.429
87.735
95.364

Integrations

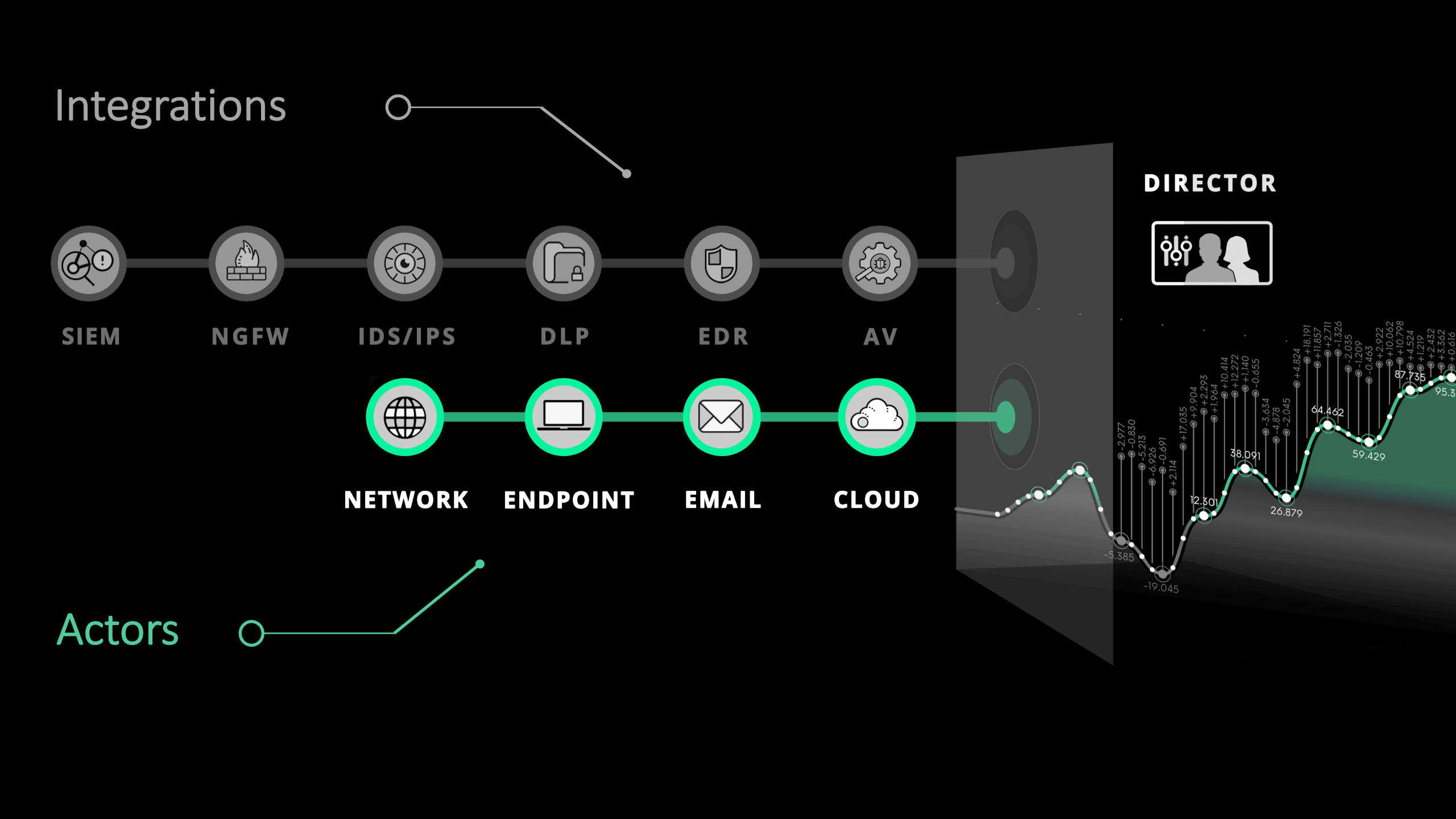
SIEM NGFW IDS/IPS DLP EDR AV

DIRECTOR

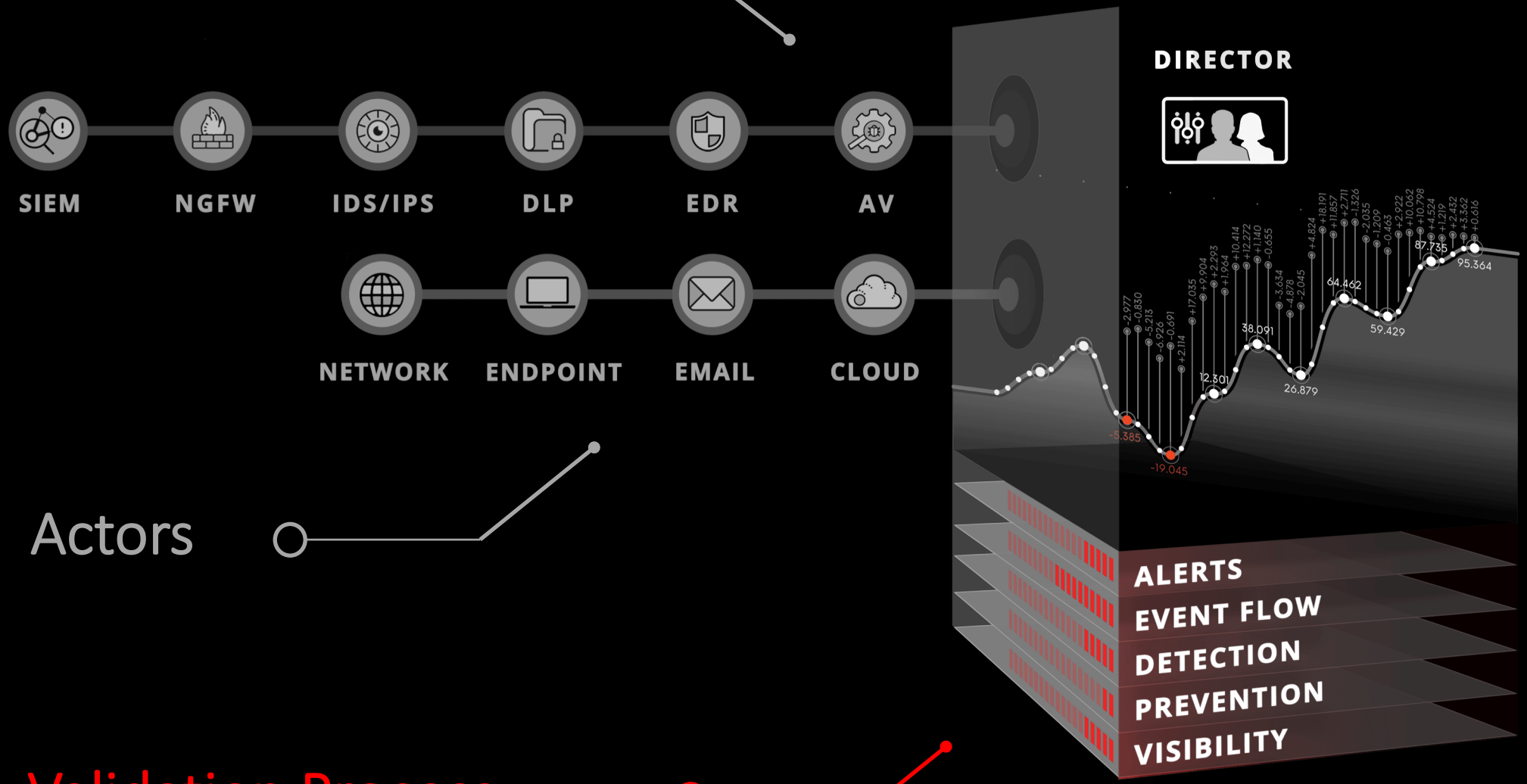


ArcSight · AlienVault · Carbon Black · Check Point Software Technologies Ltd. · Cisco
CrowdStrike · Cylance · cybereason · FireEye · Forcepoint
elastic · LogRhythm · McAfee · Microsoft · mimecast
paloalto Networks · proofpoint · Qradar · RSA · SentinelOne
SOURCEfire · splunk> · sumologic · Symantec · TippingPoint

Hundreds of technology integrations


Integrations
SIEM
NGFW
IDS/IPS
DLP
EDR
AV
NETWORK
ENDPOINT
EMAIL
CLOUD
DIRECTOR
Actors

Integrations

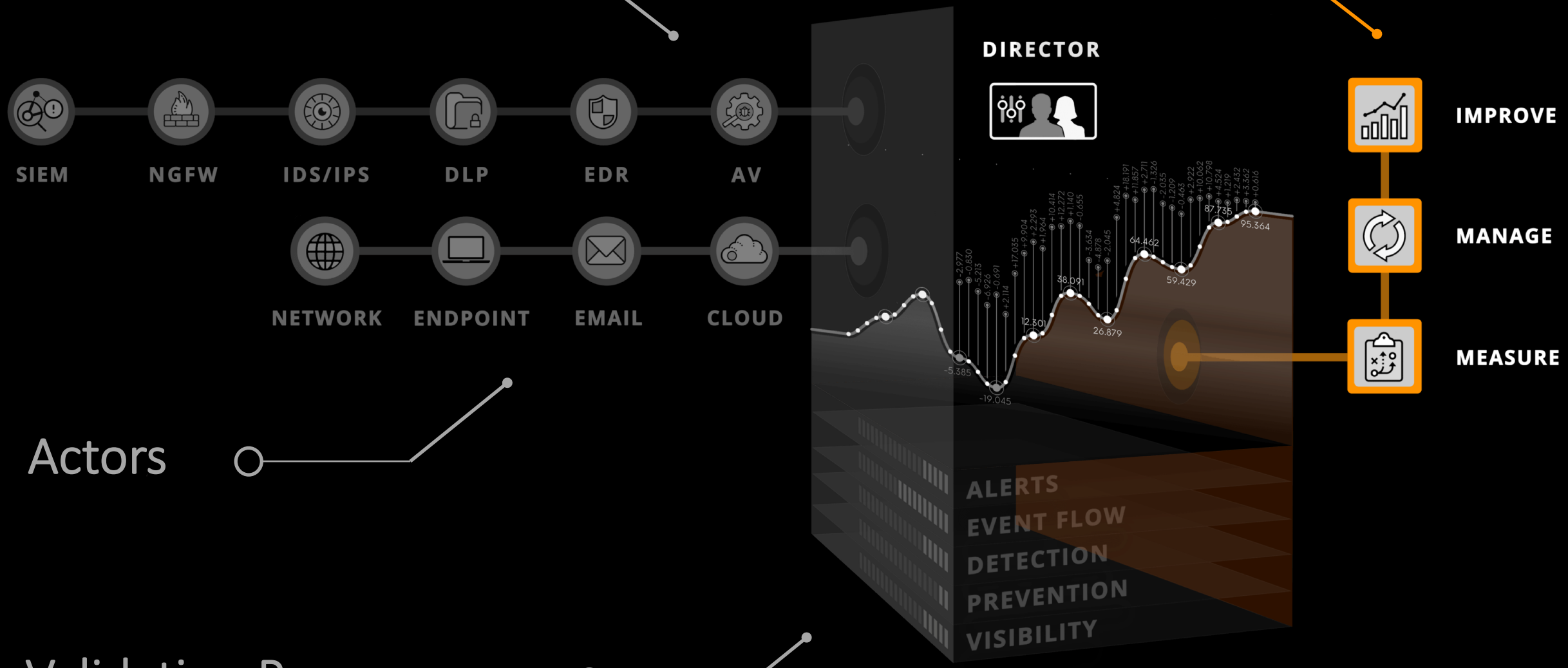


Actors

Validation Process

Integrations

Effectiveness



Actors

Validation Process

BENEFITS

- Maximize the value of your security investment & mitigate environmental drift
- Retire what doesn't provide value & prioritize future investments based on evidence
- Validate vendor & service provider claims, SLAs…
- Enable and align security with business initiatives
- Measure, communicate, and make decisions like other strategic business units
- Align with industry frameworks: NIST, MITRE ATT&CK, SANS, OWASP…
- Help hire and train security staff and continuously improve processes

CONFIDENTIAL - NOT FOR DISTRIBUTION
© 2019 VERODIN INC. ALL RIGHTS RESERVED

Brian Contos
CISO, Verodin

brian.contos@verodin.com
+1 (408) 834.5815
@BrianContos

VERODIN™
Security. Instrumented.

CONFIDENTIAL - NOT FOR DISTRIBUTION
© 2019 VERODIN INC. ALL RIGHTS RESERVED