SECURITY EFFECTIVENESS REPORT

FOCUS:

TECHNOLOGY

Over the last year, the Verodin Security Instrumentation Platform (SIP) has continued to be POC'd and deployed across every major industry vertical. The goal of this report is to highlight the trends and common problems that Verodin SIP is consistently uncovering.

A LOT HAS TO GO RIGHT FOR SECURITY TO WORK

Infrastructure complexity, continuously changing environments and lack of consistent validation are clearly **undercutting the efforts** of teams everywhere.

The challenges outlined in this report are consistent across every vertical. Based on this, Verodin estimates that every organization is likely experiencing several of the following issues.

SECURITY EFFORT ≠ SECURITY EFFECTIVENESS

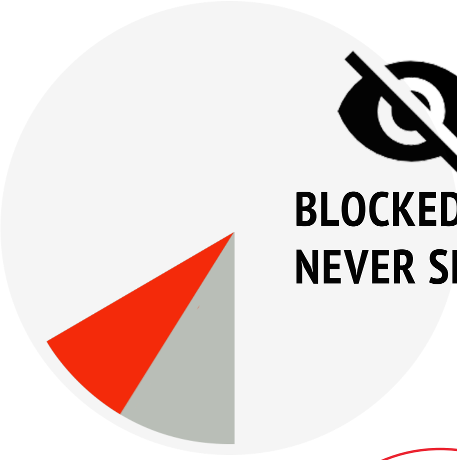
PREVENTION

PREVENTION… WHAT PREVENTION?

On average,

15-25%

of executed attack patterns are actually blocked (prevented)



BLOCKED BUT NEVER SEEN

LESS THAN 40%

of the attacks that are blocked (prevented) have corresponding events that make it to the SIEM

WHERE ARE THE LOGS?

DETECTION

Of the attack patterns that are **NOT** blocked… only

25-45%

have relatable detection alerts that make it to the SIEM

CRITICAL: The moment an attack is not blocked, *100% of your ability to defend* is dependent on a clear alert being generated and seen by an analyst who knows how to respond to it.

SIEMS & CUSTOM ANALYTICS

ONLY 0-45%

of correlation rules fire

As a result, critical alerts never bubble up to analysts

MOST COMMON CAUSES:

DEAD ON ARRIVAL

- Analyst did not validate the rule at the time of creation

RULES WENT STALE

- A signature upgrade or configuration change impacted what events will be generated (Defensive Regression)

EVENTS ARE NEVER MAKING IT TO THE SIEM

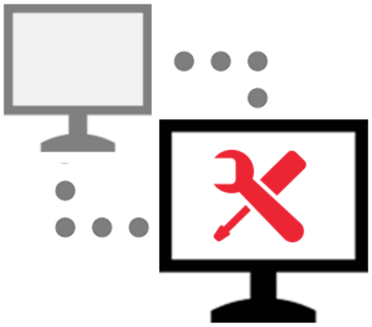
- Firewall rules blocking syslog
- Misconfigurations at the data sources (e.g. incorrect destination IP)
- Misconfigured or broken devices (e.g. load balancers) dropping events

EVENTS THAT MAKE IT ARE MISCONFIGURED

- Missing data (e.g. blank source IP, blank destination port, missing username)
- Wrong data type in fields (e.g. URL data in an IP field)

NTP IS STILL A BIG PROBLEM WITH DATA SOURCES

- Wrong timestamps on events (e.g. minutes, hours and even days off)



BASIC NETWORKING

Still undercutting security effectiveness

20 yrs later...

SPAN PORTS CHANGES **STILL** **wreak havoc on visibility**

Q: More than 3 proxies deployed in your environment?

If so...

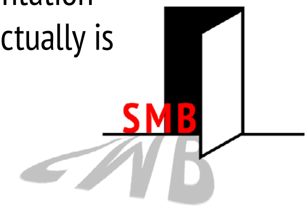
AT LEAST 1 proxy is likely to be **MISCONFIGURED**

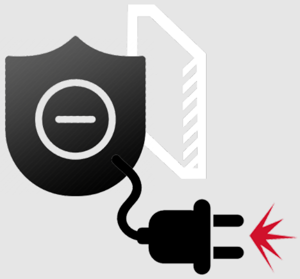
MISCONFIGURED ROUTING & FORWARDING CAUSING SERIOUS ISSUES:

Critical zones bypassing malware inspection and other defenses

Segmentation that actually ISN'T...

Organizations **ASSUME** there is more segmentation than there actually is





"NEXT-GEN" SOLUTIONS

Lots of promise / capability, but lacking value out-of-the-box

ENDPOINT

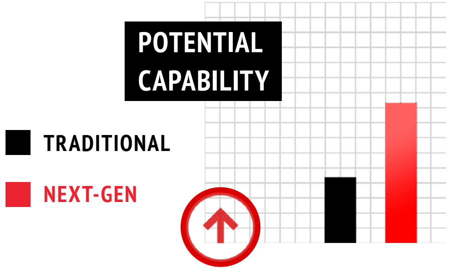
NETWORK

NEXT-GEN has a lot of promise

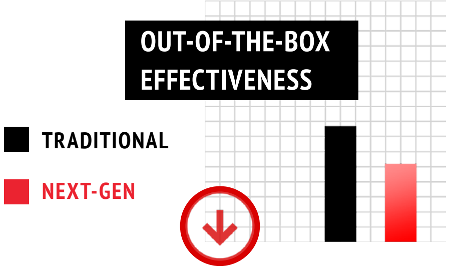
BUT requires significant calibration and tuning...

In fact: Out-of-the-box, some **traditional tools** are actually **OUTPERFORMING** "next-gen" solutions.

EXAMPLE: Known hacker tools (commonly used for lateral movement) are identified with "threat scores" of 100, but are not actually being blocked or quarantined



POTENTIAL CAPABILITY

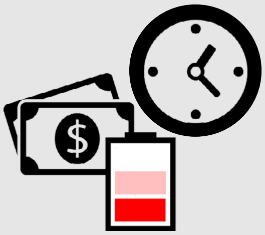


OUT-OF-THE-BOX EFFECTIVENESS

TOO MANY PRODUCTS

FEAR OF RETIRING LEGACY PRODUCTS

Without the ability to quantify impact, there is unease in removing legacy products, resulting in wasted money and unnecessary infrastructure complexity.



Fortune 1000 companies and large government agencies have **50+** different security products deployed, making their environment overly complex and more susceptible to misconfigurations.

THE POINT:

A LOT HAS TO GO RIGHT FOR SECURITY TO WORK

In security, we've been somewhat trained to think that the ABSENCE of an alert implies things are GOOD. No notification of an attack means there is no attack... right? WRONG ✗

As laid out in this report, the lack of an event or alert often indicates **something is broken** along the chain.

Let's look at the components that go into the prevention or detection of a single threat.

01

ENDPOINT
NETWORK
CLOUD

The defensive stack has to be properly calibrated and configured to detect the malicious behavior.

02

An event has to be generated that is properly formatted, accurately timestamped and channeled to the correct destination.

03

The event navigates a maze of routers, proxies, load balancers, ACLs and firewall rules to arrive at its final destination - typically a SIEM, log manager or custom analytics engine.

04

At its final destination, the event has to be correctly parsed and saved. Then, a correlation rule or analytics model has to be properly tuned.

05

ALERT

Ultimately, the alert needs to "bubble up" to notify analysts that an attack may be taking place.

For security technology to be effective, there are a lot of moving parts that need to work, and stay working, within a constantly shifting enterprise.

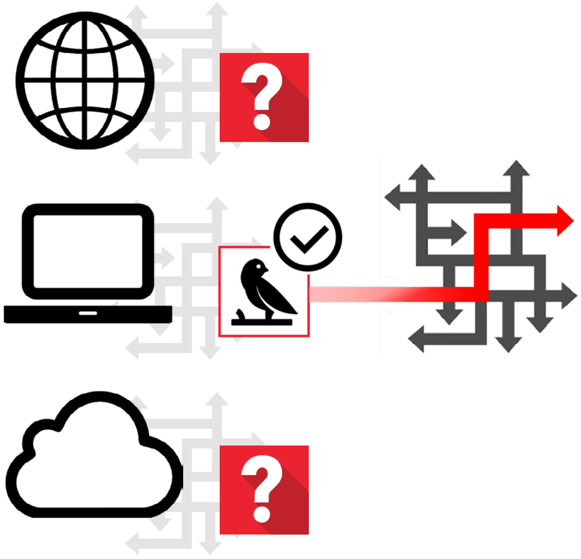
CONCLUSION:

Without a positive signal proving layered defenses are performing as assumed, most environments unknowingly suffer from Defensive Regression. Yes, the network and applications are "up", and core IT systems are performing normally. However, without continuous validation, there is no implicit warning when critical layers of prevention, detection and visibility become ineffective due to misconfigurations or other changes in the environment.

Modern security infrastructures, across endpoint, network and cloud controls, are too complicated and dynamic to understand their effectiveness with manual, point-in-time assessments.

The Verodin Security Instrumentation Platform (SIP) is the **SIGNAL THAT CONTINUOUSLY VALIDATES** the layered defenses in your infrastructure are optimally configured and working as expected.

Verodin SIP empowers customers to execute evidence-based, assumption-free security in day-to-day processes. With Verodin SIP, validation and proof become essential to every aspect of defense.



Verodin SIP is the proverbial canary in the coal mine. Its "chirps" are letting you know that your defenses remain effective as the environment around you is constantly changing.

ABOUT VERODIN

The **Verodin Security Instrumentation Platform (SIP)** empowers enterprises to remove assumptions and prove their security effectiveness with quantifiable, evidence-based data. With Verodin SIP, you can observe and adjust real responses to real attacks without ever putting production systems in danger. Verodin customers dramatically increase the ROI of their existing security investments, achieve maximum value from future spending and measurably mature their cyber prevention, detection and response capabilities.

☎ (571) 418-8684

✉ general@verodin.com