LEVEL UP
SKYLIGHT SUMMIT 2023

Unifying the Network

It’s a New NetSecOps World

John Cardani-Trollinger
Senior Director, Cybersecurity
Solutions Marketing, Accedian

ACCEDIAN

Agenda

1 Digital Transformation is Driving Change

2 The Network is Evolving

3 NetSecOps

4 NDR

Digital Transformation is Creating New Complexities

- Accelerated move to the cloud
- Adoption of multi-cloud
- Perimeter-less security
- Hybrid work
- Move to SD-WAN

As a Result, the Network is Evolving

Traditional way	New way
1 Speeds & feeds	2 User experience & optimization
3 Performance centric	4 Performance & security centric
5 Basic monitoring and detection	6 Intelligent insights
7 Basic troubleshooting	8 Complex troubleshooting

Companies are Forced Into Multiple Solutions That Don’t Play Well Together…

1. Performance monitoring solutions
2. End user experience monitoring
3. Testing and validation of network
4. Advanced threat protection
5. Intrusion detection prevention (IDS/IPS)
6. Web security
7. Email security
8. Forensics analysis
9. Data loss prevention (DLP)
10. Network generation firewalls
11. Application security
12. MDR, EDR, XDR, NDR, SIEM, SOAR

In 2021, **80% of organizations ran as many as ten solutions simultaneously for data protection and cybersecurity** - yet more than half of them suffered downtime because of data loss.

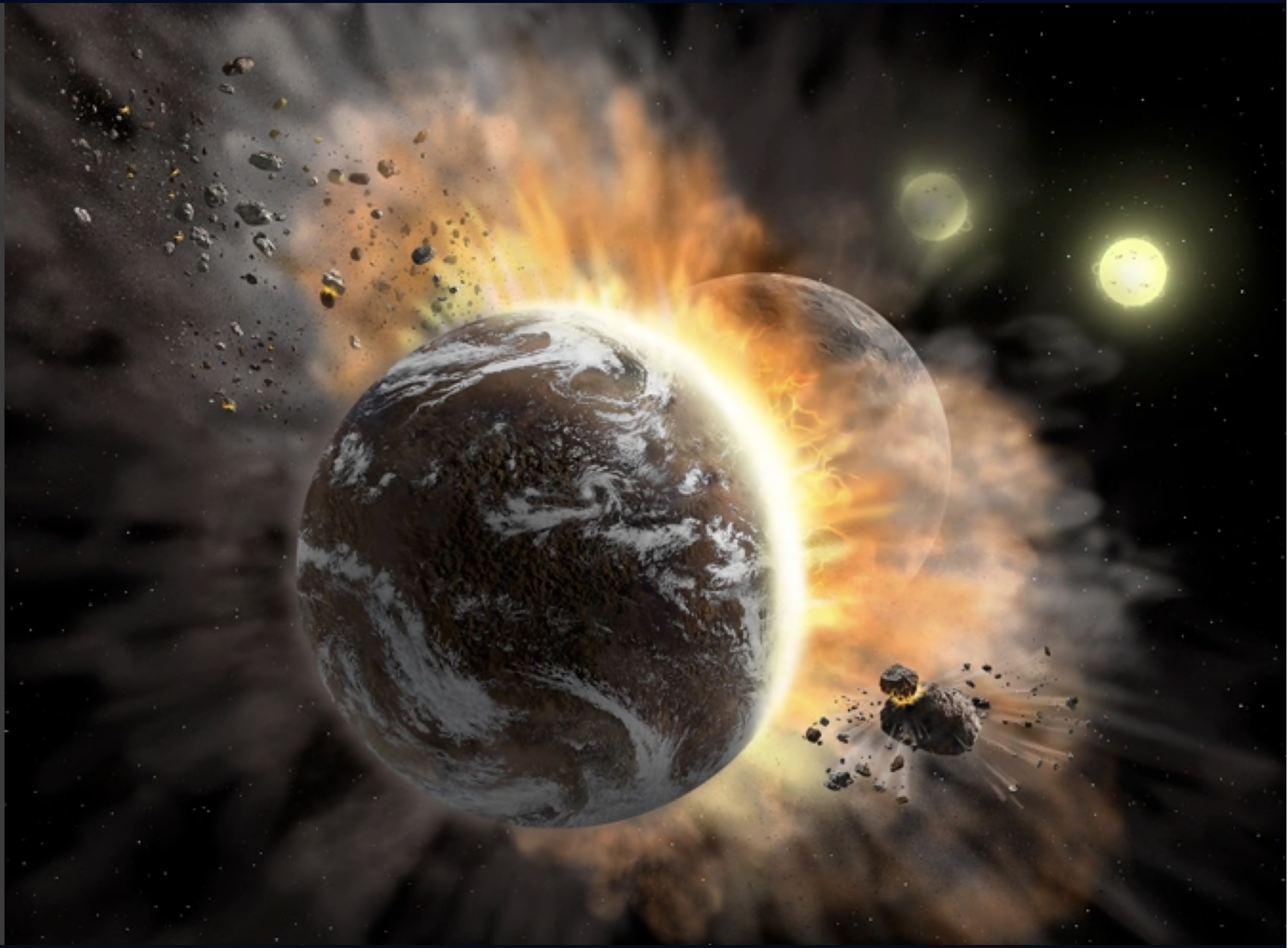
Clearly, more solutions do not translate into more protection.

Source: Global News Wire

Two Worlds are Colliding…
Network Operations and Security

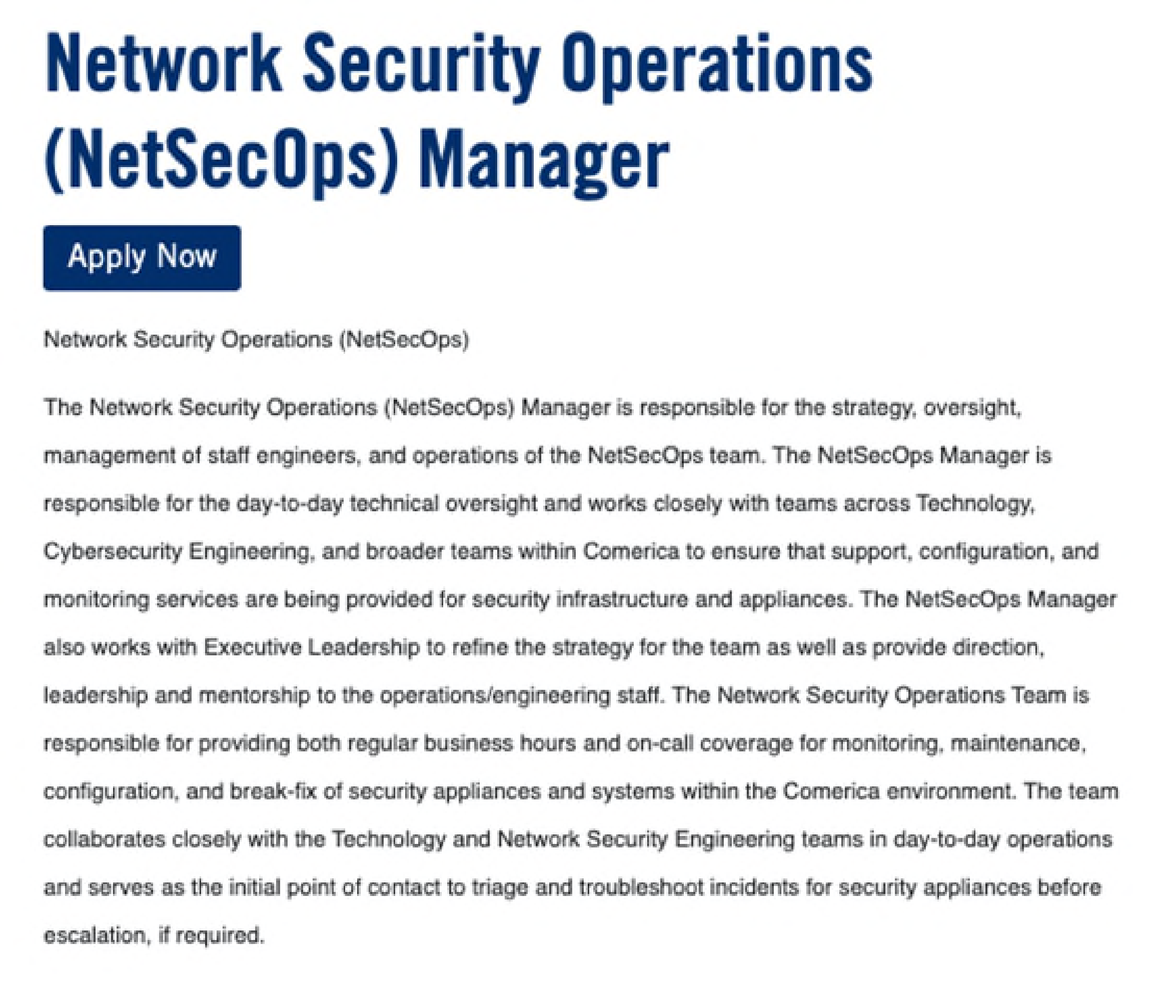
97% of organizations are trying to consolidate network packet capture infrastructure that will be shared by networking and security.

61% of global orgs' IT teams now report a preference for integrated solutions that replace their complicated stacks of cybersecurity and data protection tools with a single, unified console.



Source: Global News Wire

Real World Job - The (R)Evolution is NOW

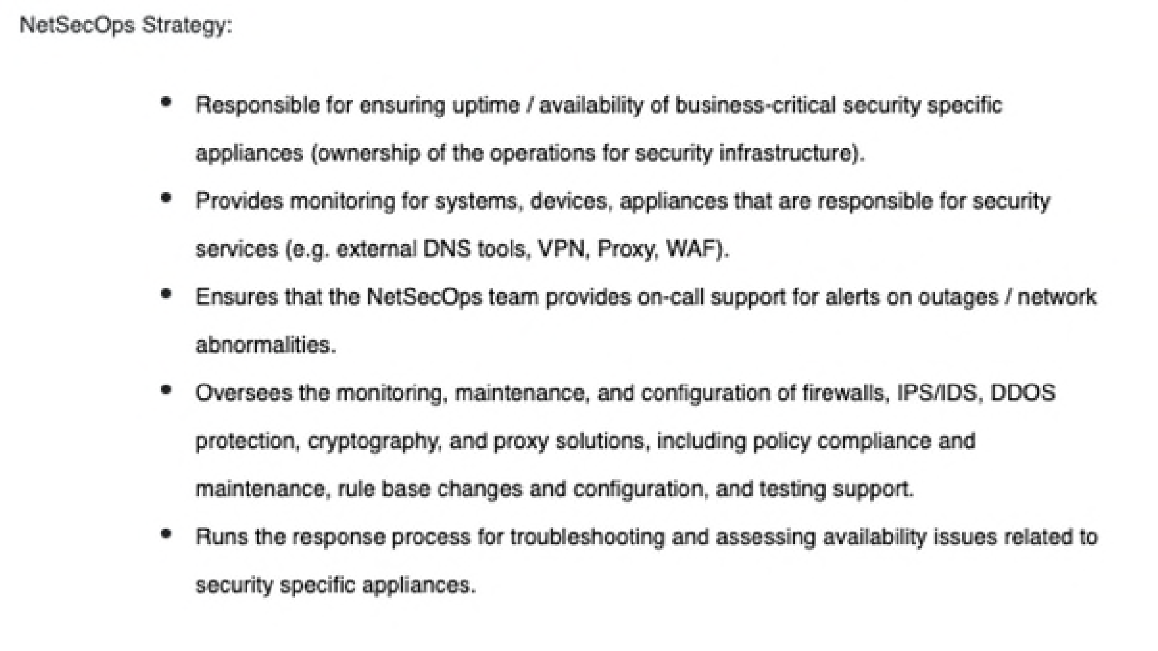


Network Security Operations (NetSecOps) Manager

Network Security Operations (NetSecOps)

The Network Security Operations (NetSecOps) Manager is responsible for the strategy, oversight, management of staff engineers, and operations of the NetSecOps team. The NetSecOps Manager is responsible for the day-to-day technical oversight and works closely with teams across Technology, Cybersecurity Engineering, and broader teams within Comerica to ensure that support, configuration, and monitoring services are being provided for security infrastructure and appliances. The NetSecOps Manager also works with Executive Leadership to refine the strategy for the team as well as provide direction, leadership and mentorship to the operations/engineering staff. The Network Security Operations Team is responsible for providing both regular business hours and on-call coverage for monitoring, maintenance, configuration, and break-fix of security appliances and systems within the Comerica environment. The team collaborates closely with the Technology and Network Security Engineering teams in day-to-day operations and serves as the initial point of contact to triage and troubleshoot incidents for security appliances before escalation, if required.

Large national financial institution - US



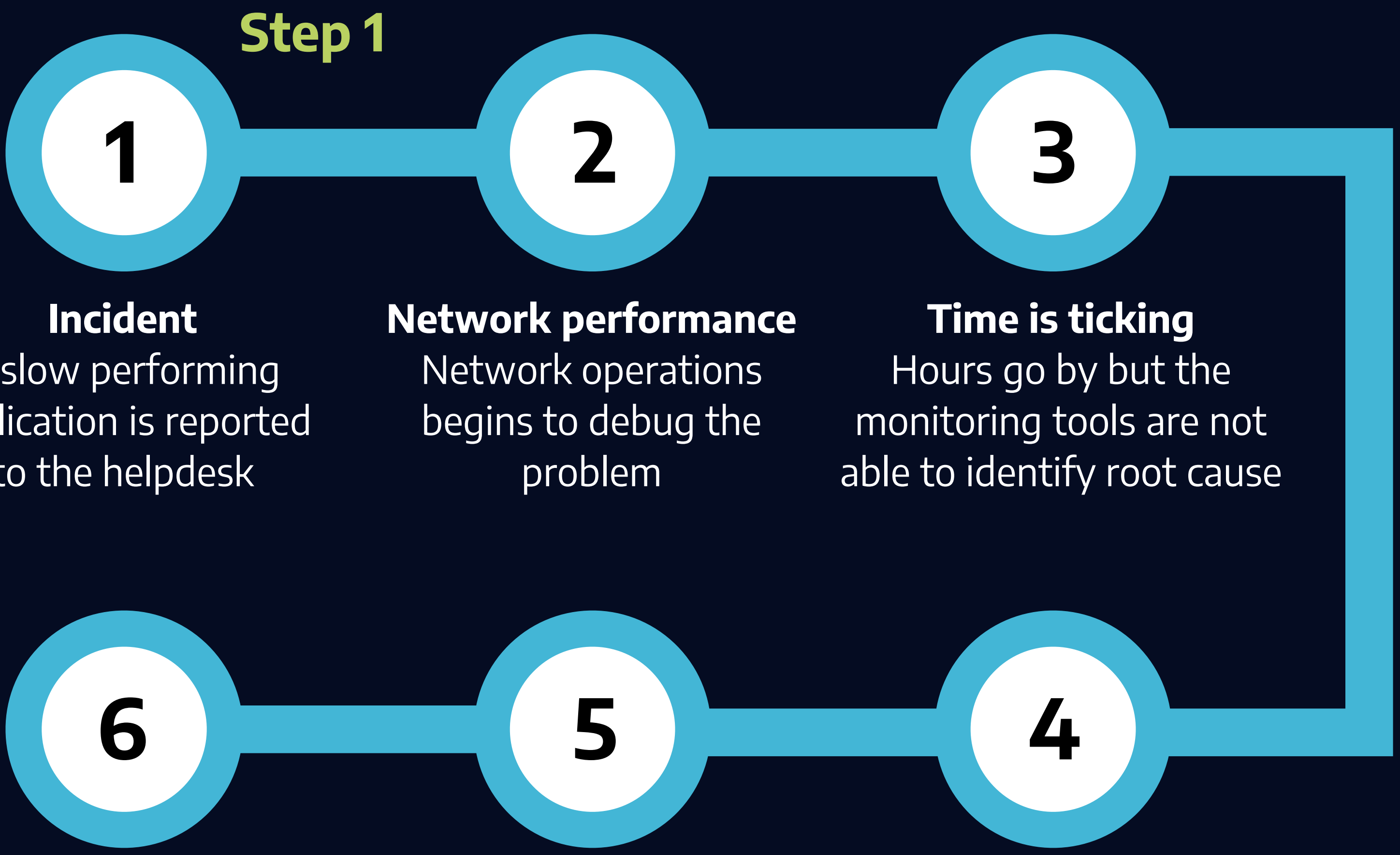
NetSecOps Strategy:

- Responsible for ensuring uptime / availability of business-critical security specific appliances (ownership of the operations for security infrastructure).
- Provides monitoring for systems, devices, appliances that are responsible for security services (e.g. external DNS tools, VPN, Proxy, WAF).
- Ensures that the NetSecOps team provides on-call support for alerts on outages / network abnormalities.
- Oversees the monitoring, maintenance, and configuration of firewalls, IPS/IDS, DDOS protection, cryptography, and proxy solutions, including policy compliance and maintenance, rule base changes and configuration, and testing support.
- Runs the response process for troubleshooting and assessing availability issues related to security specific appliances.

NetSecOps – A Recent Use Case

Customer use case testimonial by a CIO recently interviewed.

- A breach occurred in the network, but instead of recognizing it was a security related event, it was treated as a performance issue
- Three days later – the problem was finally identified



Incident
A slow performing application is reported to the helpdesk

Network performance
Network operations begins to debug the problem

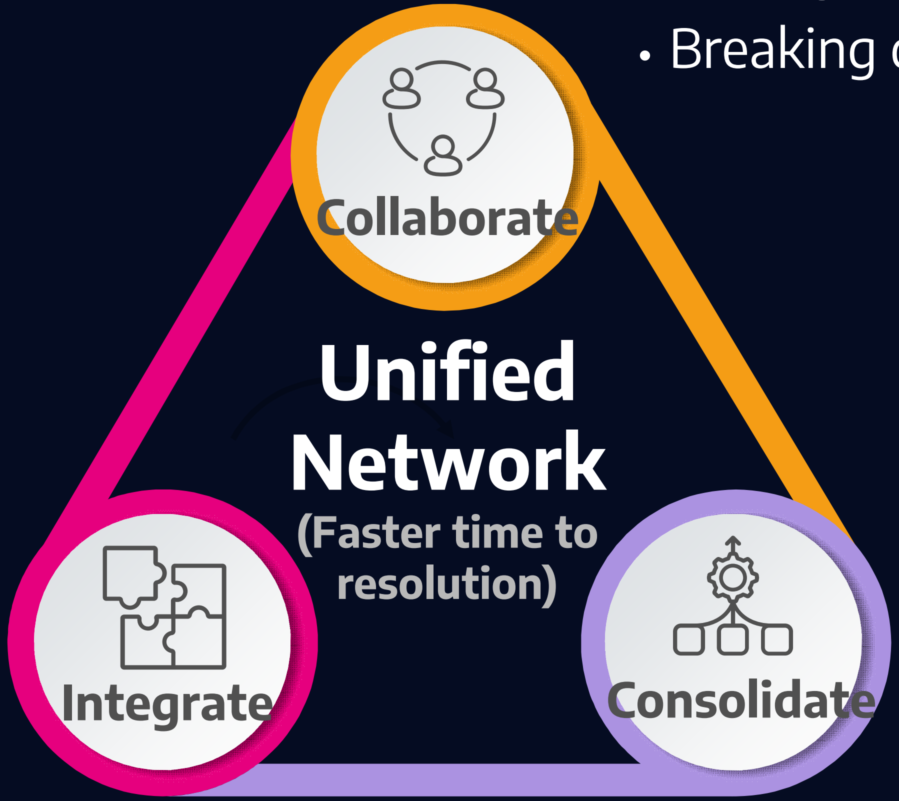
Time is ticking
Hours go by but the monitoring tools are not able to identify root cause

All hands on deck
Resources pulled off revenue generating tasks to chase the problem

Security team
Meanwhile, the security team detects a threat in the network

Business is impacted
No one realizes the two incidents are one in the same

People, Processes and Tools



People

- Cross training
- Driving collaboration
- Breaking down silos

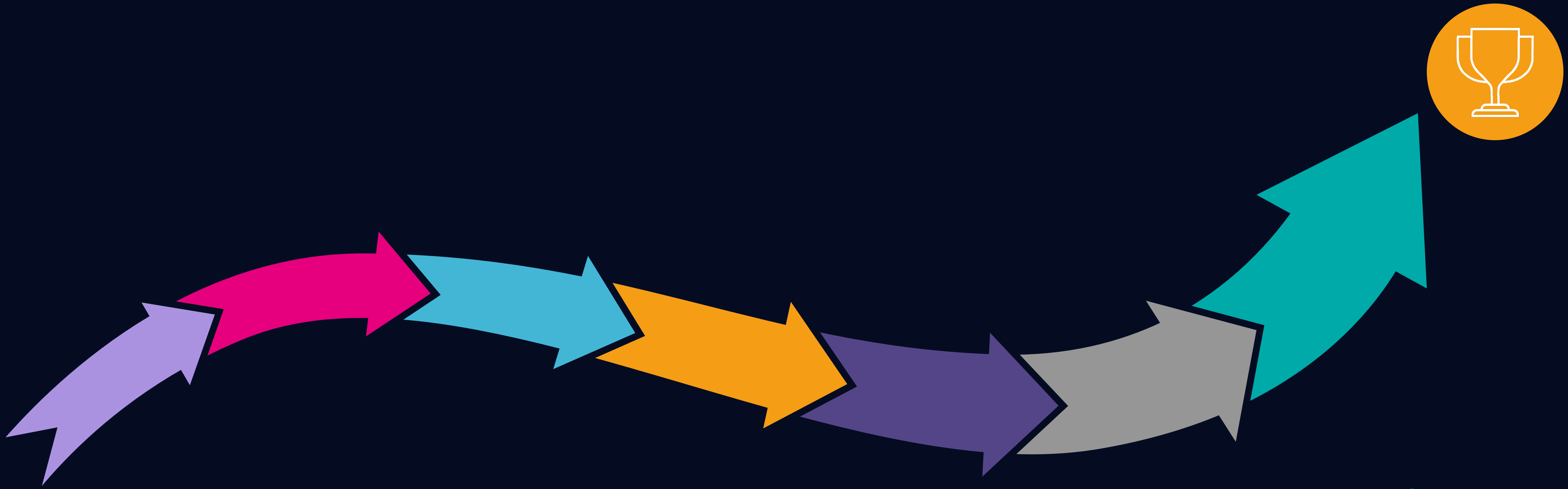
Processes

- Removing duplication
- Improving efficiencies
- Eliminating blindspots

Tools

- Integrated monitoring
- Built-in intelligence
- Tool reduction

Operationalizing NetSecOps



Unify

Unify work cultures

Assess

Assess budgets, teams, and toolsets

Integrate

Consolidation or integration of tools

Skills

Address skill gaps & create training plans.

Process

Define best practices and processes.

Focus

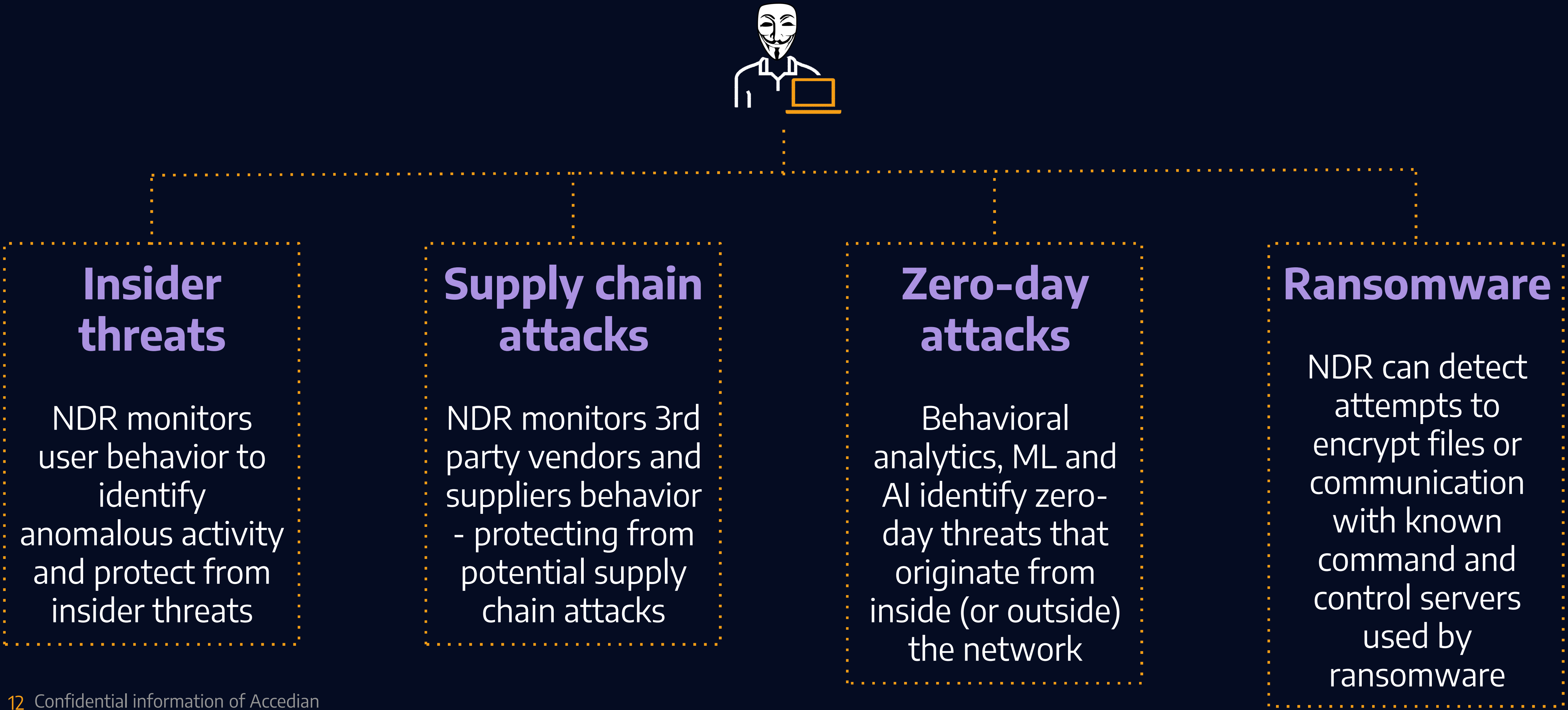
Focus on the future

Patience

Stay the course and measure results.

The “Sec” in NetSecOps

The Essential Role of NDR for Stopping Modern Threats



Insider threats

NDR monitors user behavior to identify anomalous activity and protect from insider threats

Supply chain attacks

NDR monitors 3rd party vendors and suppliers behavior - protecting from potential supply chain attacks

Zero-day attacks

Behavioral analytics, ML and AI identify zero-day threats that originate from inside (or outside) the network

Ransomware

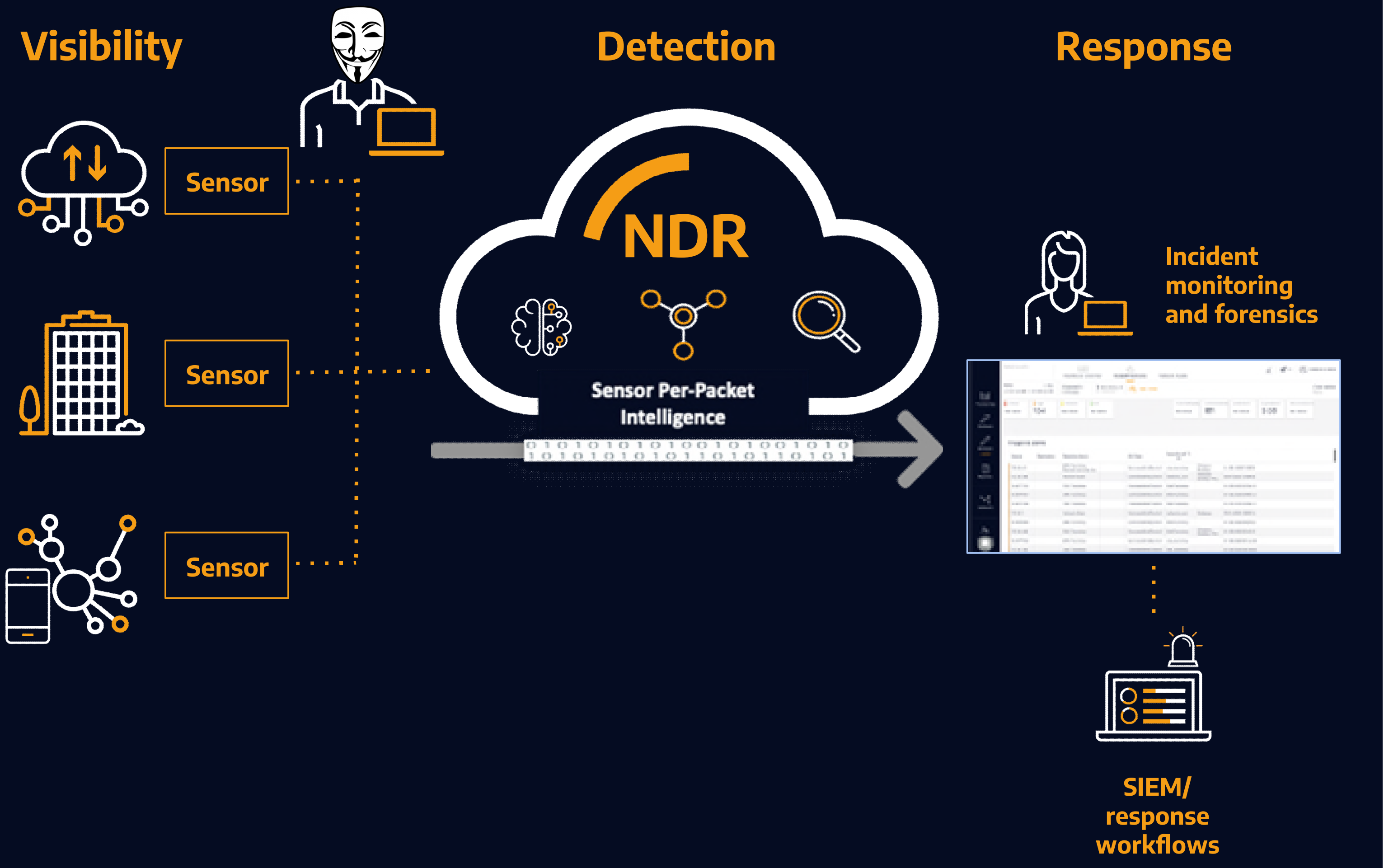
NDR can detect attempts to encrypt files or communication with known command and control servers used by ransomware

NDR – Catching Threats that Evade the Perimeter

- Delivers rapid investigation, internal visibility, intelligent response, and enhanced threat detection across cloud, on-premises, and remote environments.

- Detects attacks at the network layer so that it's extremely difficult for threat actors to hide their activity.

- Unlike EDR or XDR solutions, NDR focuses on analyzing packet data in network traffic rather than endpoints or other data streams to detect potential cyber threats.



The Convergence of Performance and Security

Harmonizing your security and IT ops

NPM ← Single platform, single sensor → NDR

Network performance

- How is the network performing?
- Identify and isolate network issues
- Manage user experience

Unified network

- Unified to quickly identify root cause across performance and security
- Built-in intelligence across both performance and security
- Reduce costs & complexity, greater ROI and TCO

Network detection and response

- Reduce security risks within network
- Identify known threats
- Proactively hunt for zero day threats

The Time is Now for Unified Visibility

- The security resource problem is real
- The risks are greater than ever before
- Costs are rising
- Competition is fierce

Removing barriers to innovation

LEVEL UP SKYLIGHT SUMMIT 2023

Thank you!

John Cardani-Trollinger
Senior Director, Cybersecurity Solutions Marketing

jcardanitrollinger@accedian.com

ACCEDIAN