STELLAR CYBER®

Supply Chain Risk Demands XDR

Nov. 2023

Aimei Wei
CTO, Founder of Stellar Cyber

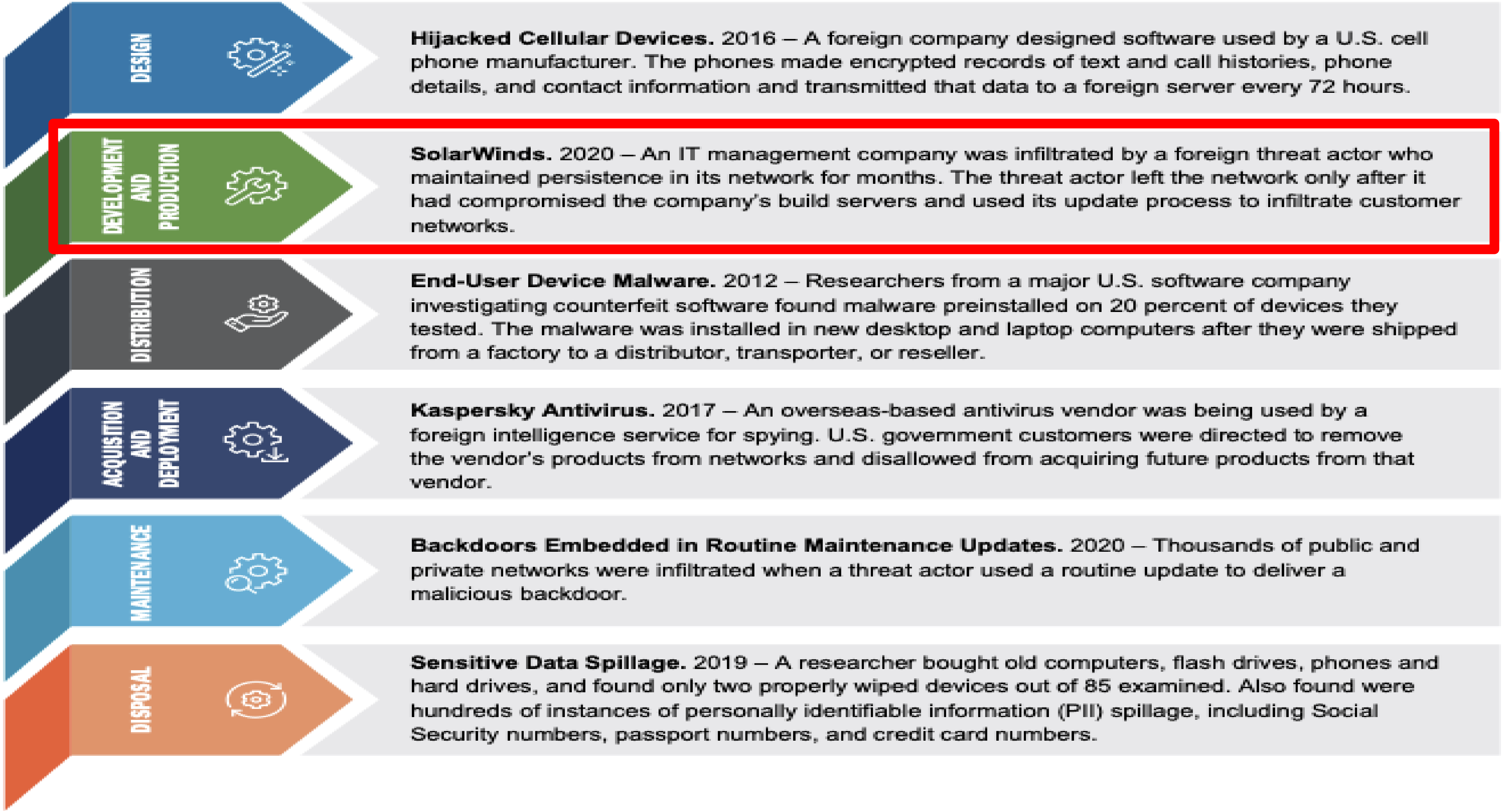
A 20 Year Journey

Two sides of one coin: Improved productivity/more exposed

What Is Supply Chain Risk?

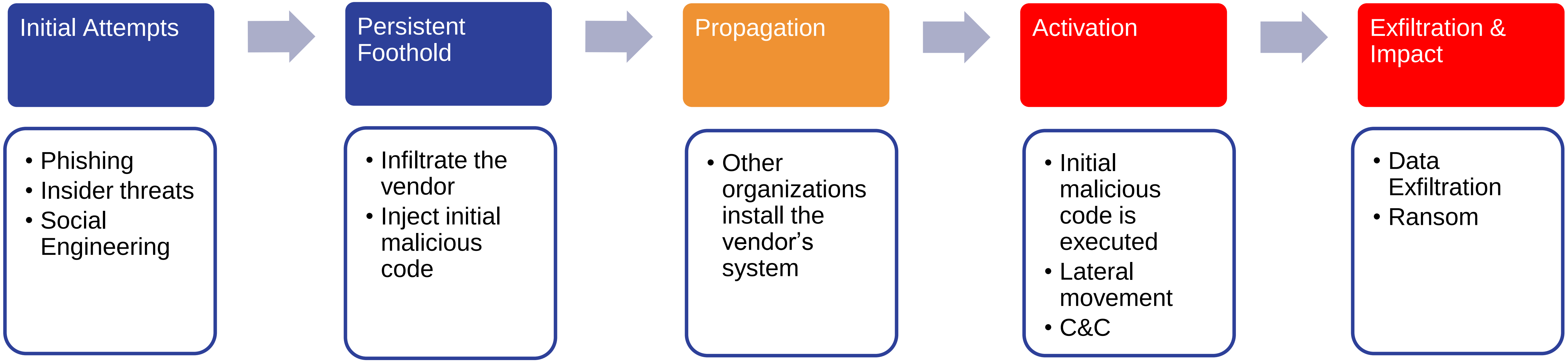
- A cyber threat actor infiltrates a software vendor’s network and employs malicious code to compromise the software **before** the vendor sends it to their customers.
- The compromised software then compromises the customer’s data or system.
- These types of attacks affect **all** users of the compromised software and can have **widespread consequences** for government, critical infrastructure, and private sector software customers

Table 1: ICT Supply Chain Lifecycle and Examples of Threats



DESIGN	**Hijacked Cellular Devices.** 2016 – A foreign company designed software used by a U.S. cell phone manufacturer. The phones made encrypted records of text and call histories, phone details, and contact information and transmitted that data to a foreign server every 72 hours.
DEVELOPMENT AND PRODUCTION	**SolarWinds.** 2020 – An IT management company was infiltrated by a foreign threat actor who maintained persistence in its network for months. The threat actor left the network only after it had compromised the company's build servers and used its update process to infiltrate customer networks.
DISTRIBUTION	**End-User Device Malware.** 2012 – Researchers from a major U.S. software company investigating counterfeit software found malware preinstalled on 20 percent of devices they tested. The malware was installed in new desktop and laptop computers after they were shipped from a factory to a distributor, transporter, or reseller.
ACQUISTION AND DEPLOYMENT	**Kaspersky Antivirus.** 2017 – An overseas-based antivirus vendor was being used by a foreign intelligence service for spying. U.S. government customers were directed to remove the vendor's products from networks and disallowed from acquiring future products from that vendor.
MAINTENANCE	**Backdoors Embedded in Routine Maintenance Updates.** 2020 – Thousands of public and private networks were infiltrated when a threat actor used a routine update to deliver a malicious backdoor.
DISPOSAL	**Sensitive Data Spillage.** 2019 – A researcher bought old computers, flash drives, phones and hard drives, and found only two properly wiped devices out of 85 examined. Also found were hundreds of instances of personally identifiable information (PII) spillage, including Social Security numbers, passport numbers, and credit card numbers.

How Does It Happen?



Initial Attempts

- Phishing
- Insider threats
- Social Engineering

Persistent Foothold

- Infiltrate the vendor
- Inject initial malicious code

Propagation

- Other organizations install the vendor’s system

Activation

- Initial malicious code is executed
- Lateral movement
- C&C

Exfiltration & Impact

- Data Exfiltration
- Ransom

Suppliers ***Organizations***

“Supply Chain Kill Chain”

Three Common Attack Techniques

Hijacking updates

1

- Routine updates to address bugs and security issues, or release new features
- Software vendors typically distribute updates from centralized servers
- Threat actors can hijack an update by infiltrating the vendor’s network and either inserting malware into the outgoing update or altering the update to grant the threat actor control over the software’s normal functionality

Three Common Attack Techniques

Undermining code signing

- Code signing is used to validate the identity of the code's author and the integrity of the code.
- Attackers undermine code signing by self-signing certificates, breaking signing systems, or exploiting misconfigured account access controls.
- hijack software updates by impersonating a trusted vendor and inserting malicious code into an update

2

Three Common Attack Techniques

Compromising open-source code

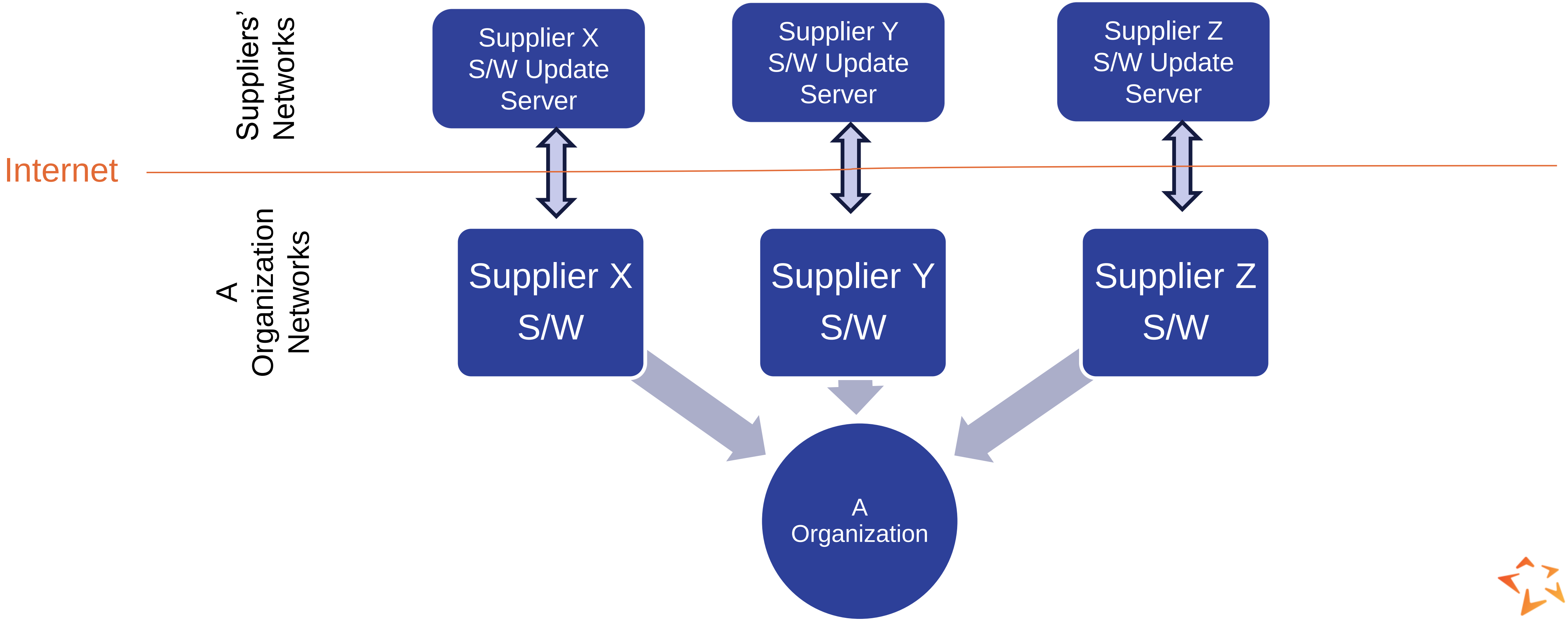
- Threat actors insert malicious code into publicly accessible code libraries, which unsuspecting developers—looking for free blocks of code to perform specific functions—then add into their own third-party code

- For example, in 2018, researchers discovered 12 malicious Python libraries uploaded on the official Python Package Index (PyPI)

3

Organizations Are Vulnerable To Supply Chain Attacks

- Many third-party software products require **privileged** access
- Many third-party software products require **frequent** communication between a vendor’s network and the vendor’s software product located on customer networks.

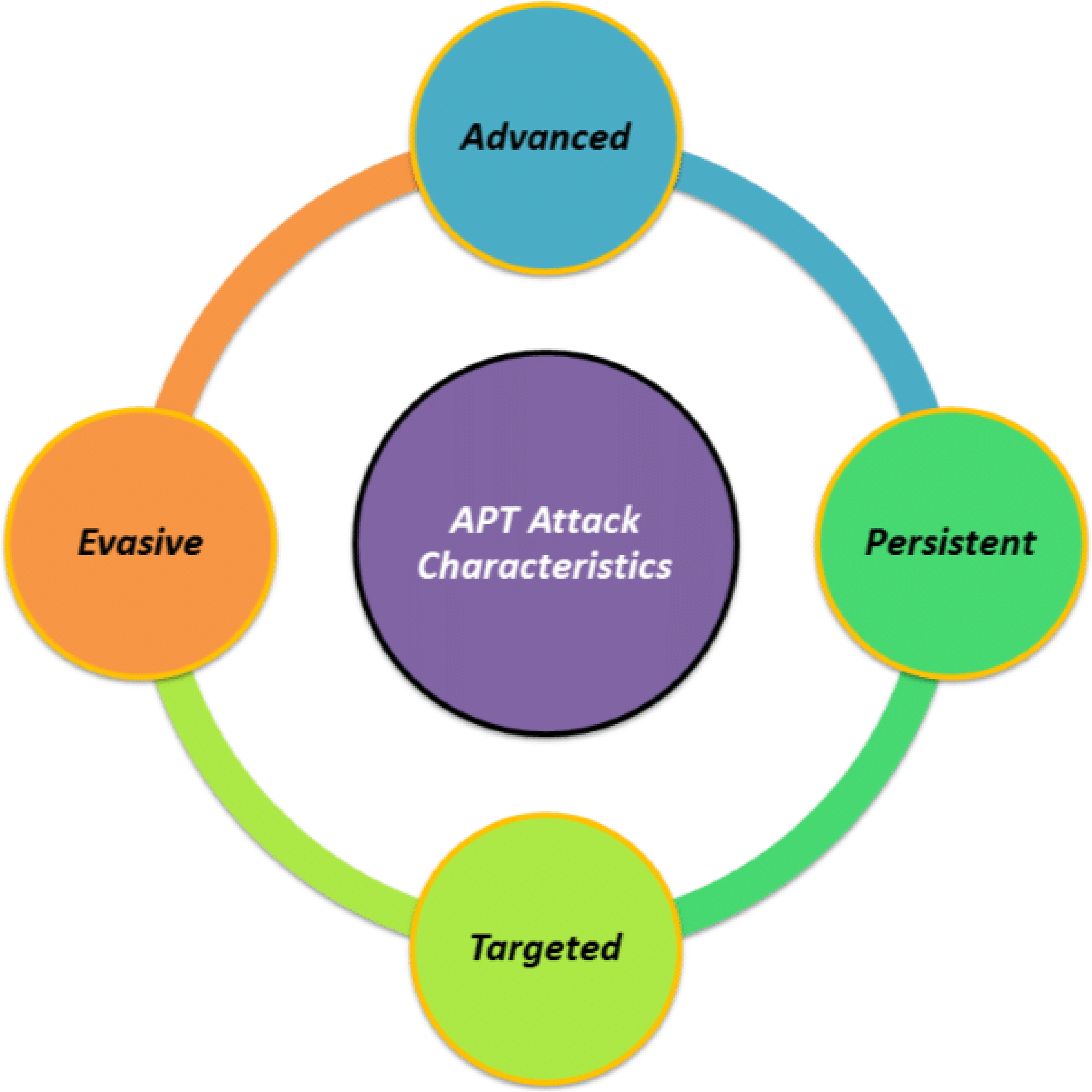


Characteristics of Supply Chain Attacks

Essentially APT attacks

Common characteristics:

- Well-planned, **targeted**
- **Multi-staged** with diverse attack vectors, evasive
- Advanced **techniques**
- Prolonged, **low and slow**, long-term persistent



Consequences of Supply Chain Attacks

Gain initial persistent access to an organization	**Lateral movement**	**Conduct malicious activities**
Bypass perimeter security measures like firewalls, web security gateways, email security gateways, etc.	Gain access to key assets like servers or databases Inject additional tailored malware on a chosen target	Data, IP, or financial theft Monitoring organizations' or individuals' behaviors Ransomware attack etc.

Risk Management Program

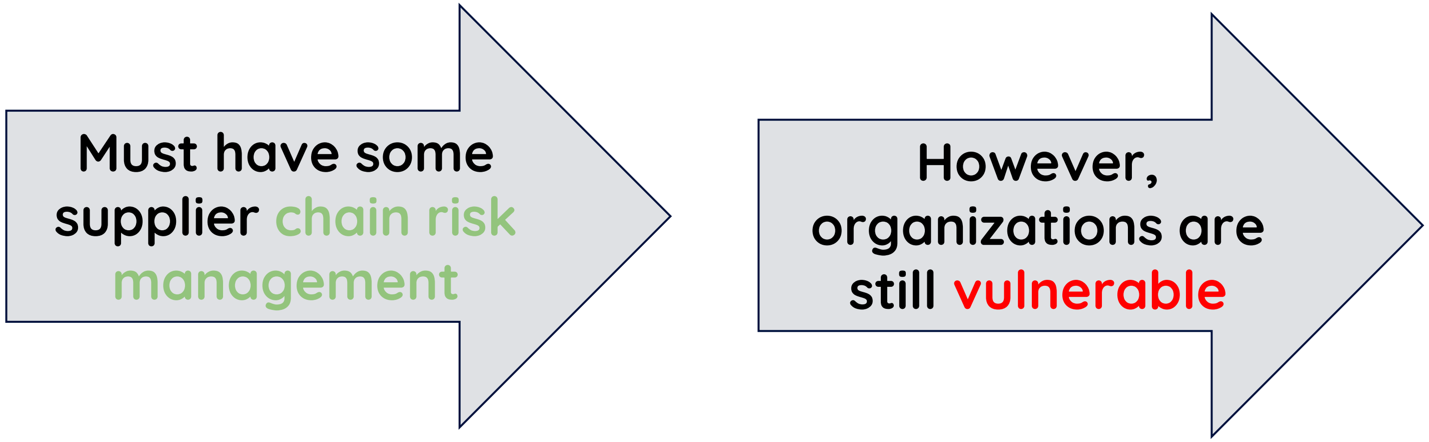
UPDATE

NIST

Cybersecurity Guidance for Supply Chain Risk Management

NIST – C-SCRM

- Identify key mission-critical business processes
- Maintain an inventory of your organization’s current and future software licenses
- Research and document how each software license is supported by its supplier
- Understand how your software supports or otherwise relates to your key processes
- Document how you would plan to address software when a vulnerability is disclosed



Must have some supplier chain risk management

However, organizations are still vulnerable

- **Can greatly reduce the chance of being attacked by supply chain software**

- As long as there is **single** one that evades you

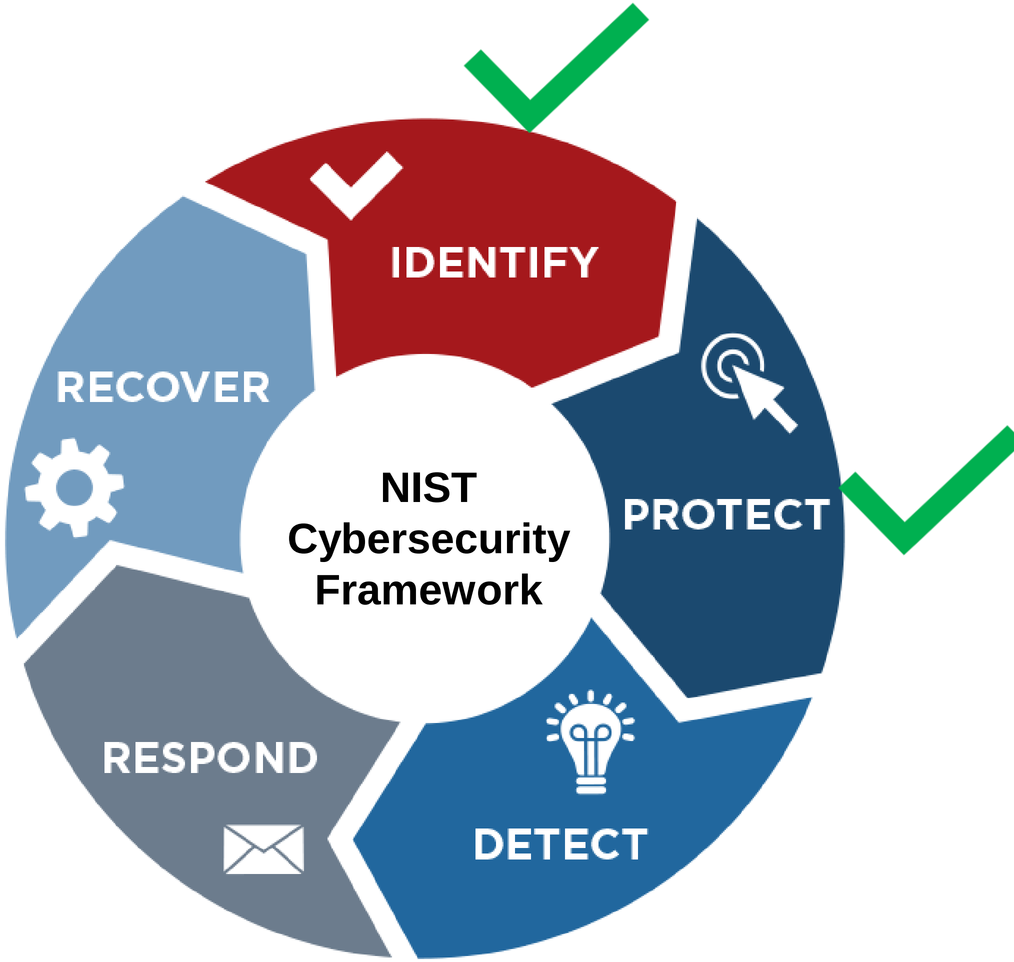
What Else?

NIST – C_SCRM

- Identify
- Protect

Supplier Chain Attacks

- Pervasive – everywhere
- Dynamic – not a one-time deal
- Evasive – bypass your parameter defense

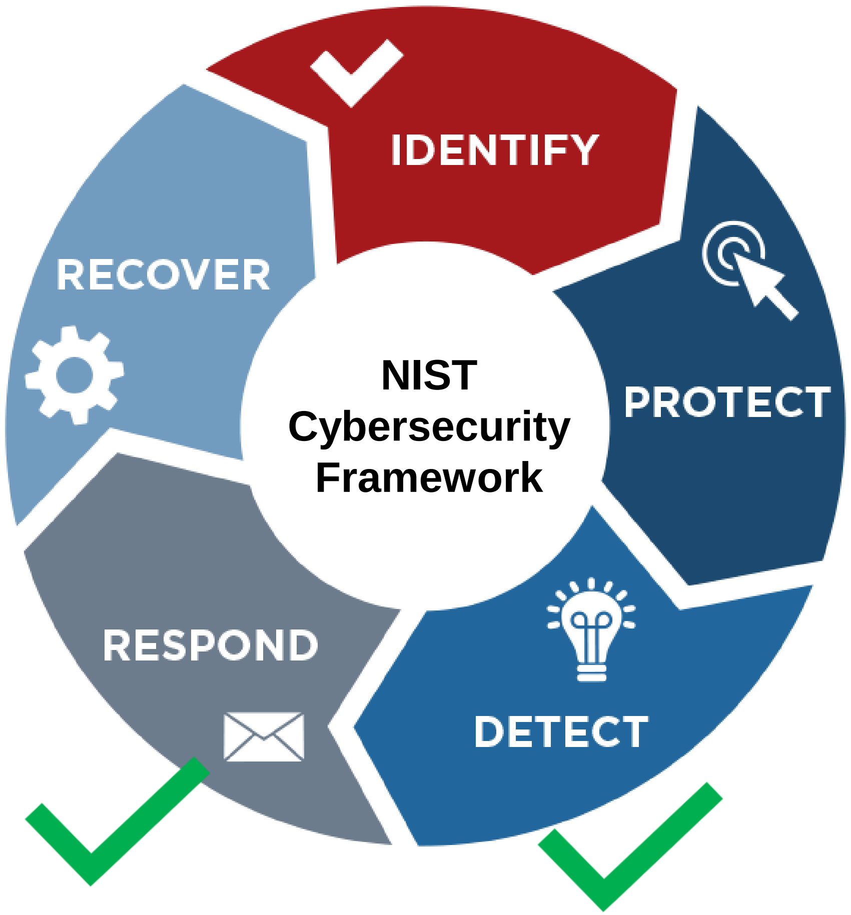


Additional Strategy

Detect and Stop Early

&

Respond and Act Fast



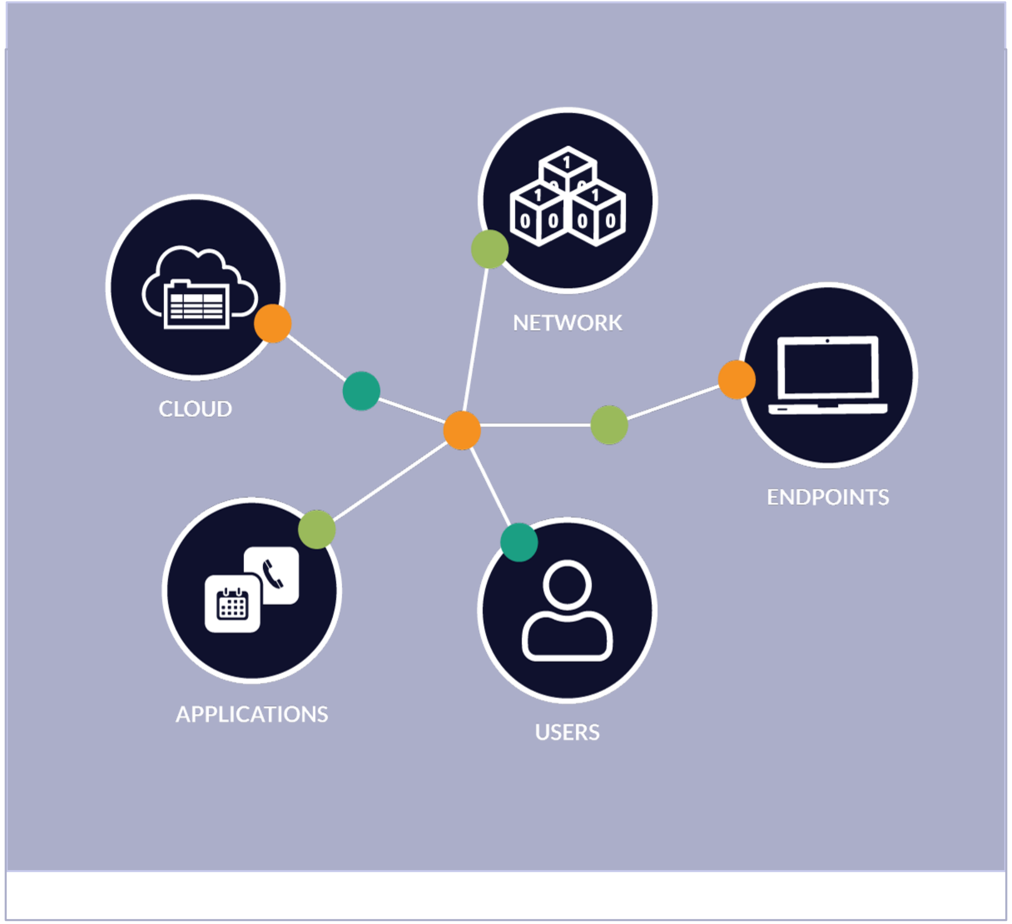
STELLAR CYBER®

How Extended Detection & Response (XDR) Helps

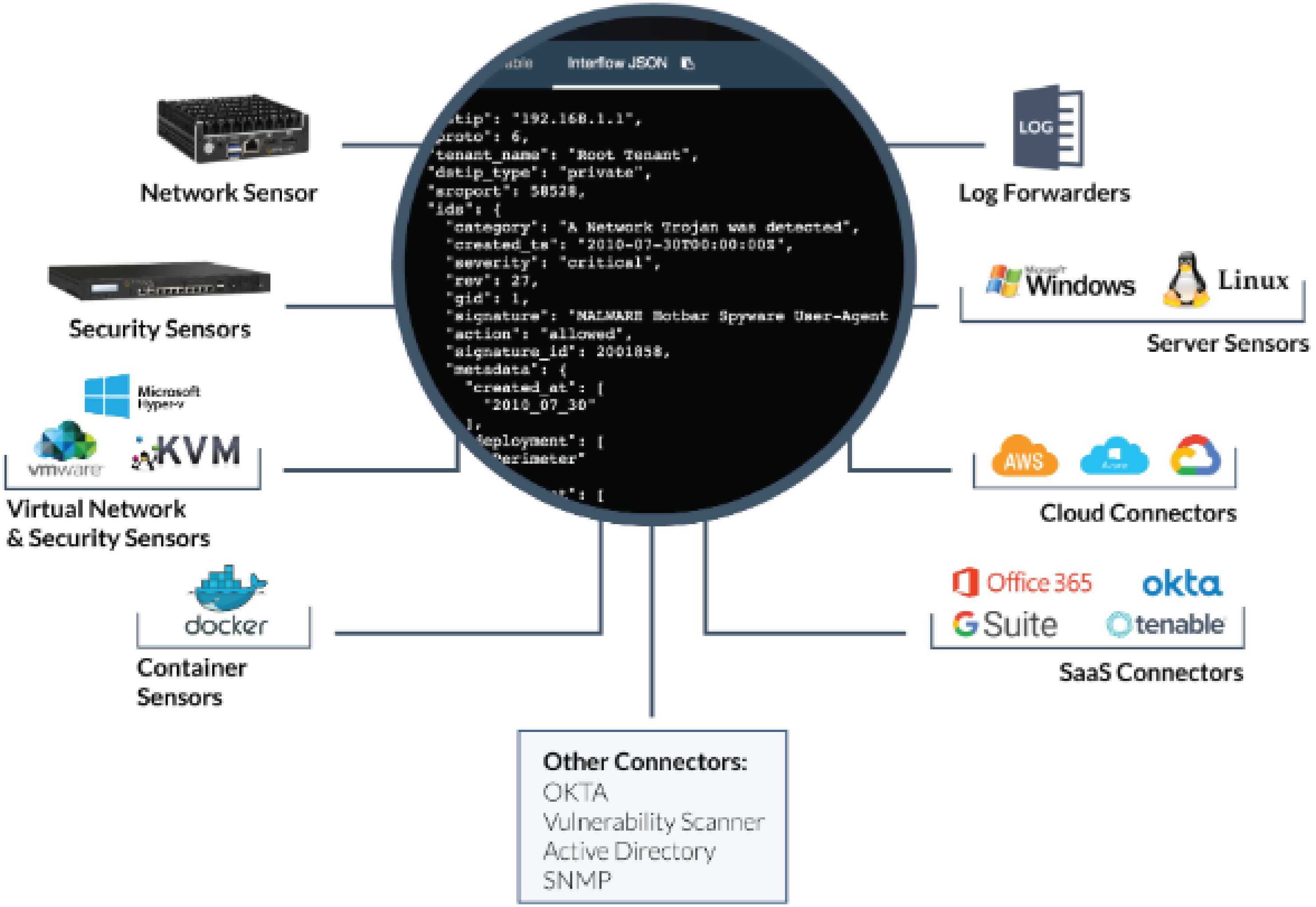
- **Full visibility** in your environment
- **Detect** suspicious signals leveraging AI/ML
- **Correlate** weak signals into stronger signals – connecting the dots
- **Response** capability, so you can stop the attack early before it progresses and cause damage

Full Visibility – See Everything, Anytime

- You can't detect what you can't see - **blind spots**
- Cover entire attack surface: **network, endpoint, cloud, email, identity**
- A family of sensors that can live In **any environment and collect any data**



360-Degree Visibility - Physical & Virtual Sensors



```
tip": "192.168.1.1",
proto": 6,
"tenant_name": "Root Tenant",
"dstip_type": "private",
"srcport": 58528,
"ids": {
  "category": "A Network Trojan was detected",
  "created_ts": "2010-07-30T00:00:00Z",
  "severity": "critical",
  "rev": 27,
  "gid": 1,
  "signature": "MALWARE Hotbar Spyware User-Agent
  "action": "allowed",
  "signature_id": 2001858,
  "metadata": {
    "created_at": [
      "2010_07_30"
    ],
    "deployment": [
      "Perimeter"

           ": [
```

Network Sensor

Security Sensors

Virtual Network & Security Sensors

Container Sensors

Log Forwarders

Server Sensors

Cloud Connectors

SaaS Connectors

Other Connectors:
OKTA
Vulnerability Scanner
Active Directory
SNMP

STELLAR CYBER®

High-Level Stellar Cyber Architecture for Modular Sensors

Stellar Cyber Modular Sensor Features

Security Features

- IDS (60K+ Rules)
- Malware Sandbox
- Tenable.io (Nessus)

Network Features

- Network Traffic Analysis (NTA)
- Log Forwarder
  - Log Parsing
  - Log Normalization
- Data Buffering
- Local Connectors
- Aggregator

High-Level Stellar Cyber Architecture for Modular Sensors

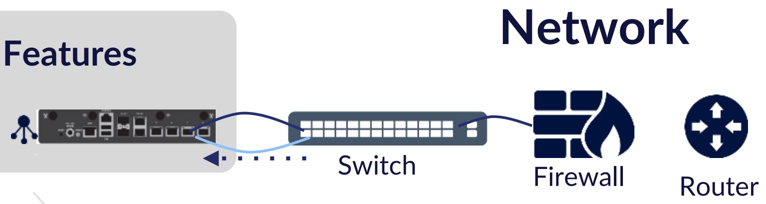
Stellar Cyber Modular Sensor Features

Security Features

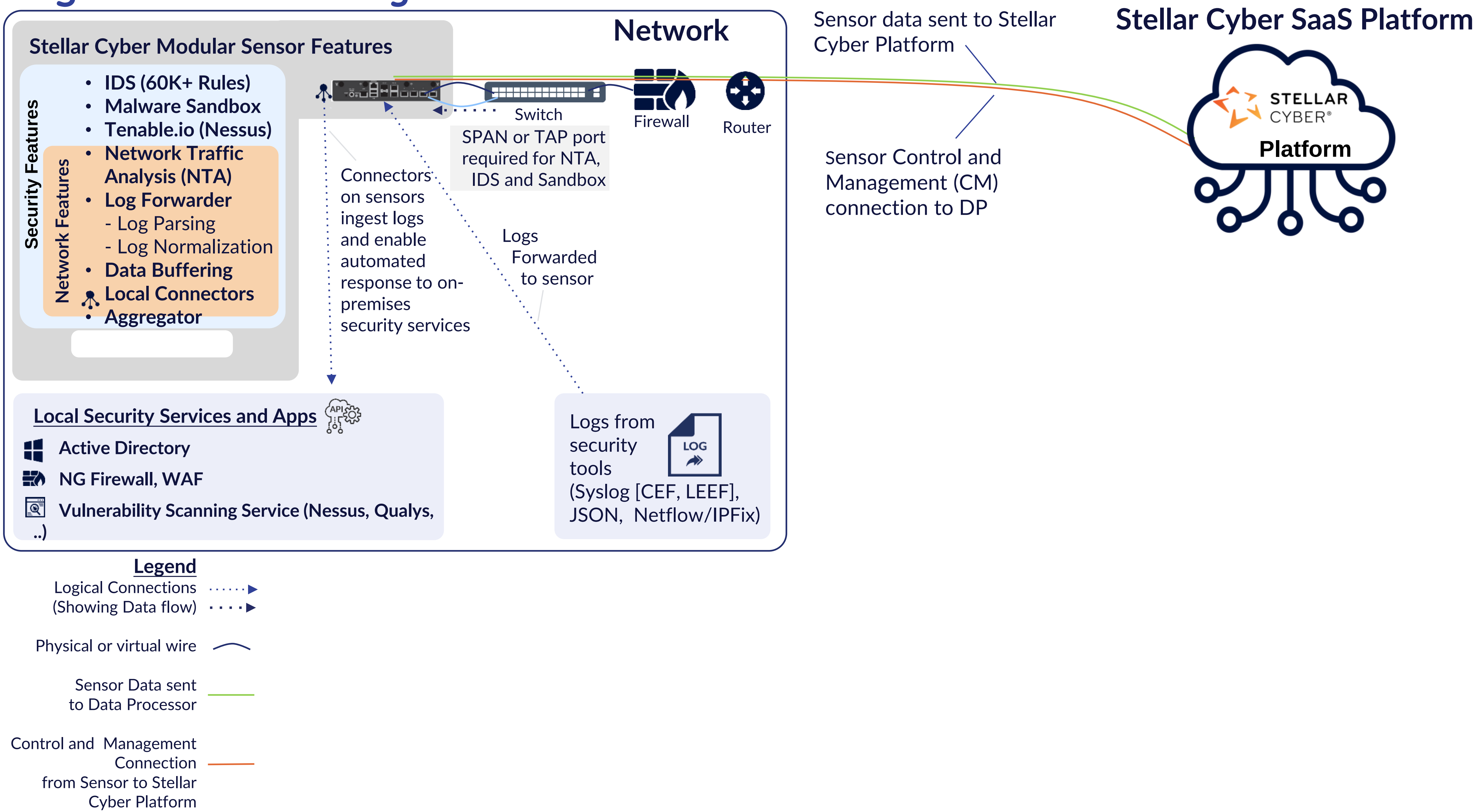
- IDS (60K+ Rules)
- Malware Sandbox
- Tenable.io (Nessus)

Network Features

- Network Traffic Analysis (NTA)
- Log Forwarder
  - Log Parsing
  - Log Normalization
- Data Buffering
- Local Connectors
- Aggregator



High-Level Stellar Cyber Architecture for Modular Sensors



Network

Stellar Cyber Modular Sensor Features

Security Features

- IDS (60K+ Rules)
- Malware Sandbox
- Tenable.io (Nessus)

Network Features

- Network Traffic Analysis (NTA)
- Log Forwarder
  - Log Parsing
  - Log Normalization
- Data Buffering
- Local Connectors
- Aggregator

Switch

SPAN or TAP port required for NTA, IDS and Sandbox

Firewall

Router

Connectors on sensors ingest logs and enable automated response to on-premises security services

Logs Forwarded to sensor

Local Security Services and Apps

- Active Directory
- NG Firewall, WAF
- Vulnerability Scanning Service (Nessus, Qualys, ..)

Logs from security tools (Syslog [CEF, LEEF], JSON, Netflow/IPFix)

Sensor data sent to Stellar Cyber Platform

Sensor Control and Management (CM) connection to DP

Stellar Cyber SaaS Platform

Legend

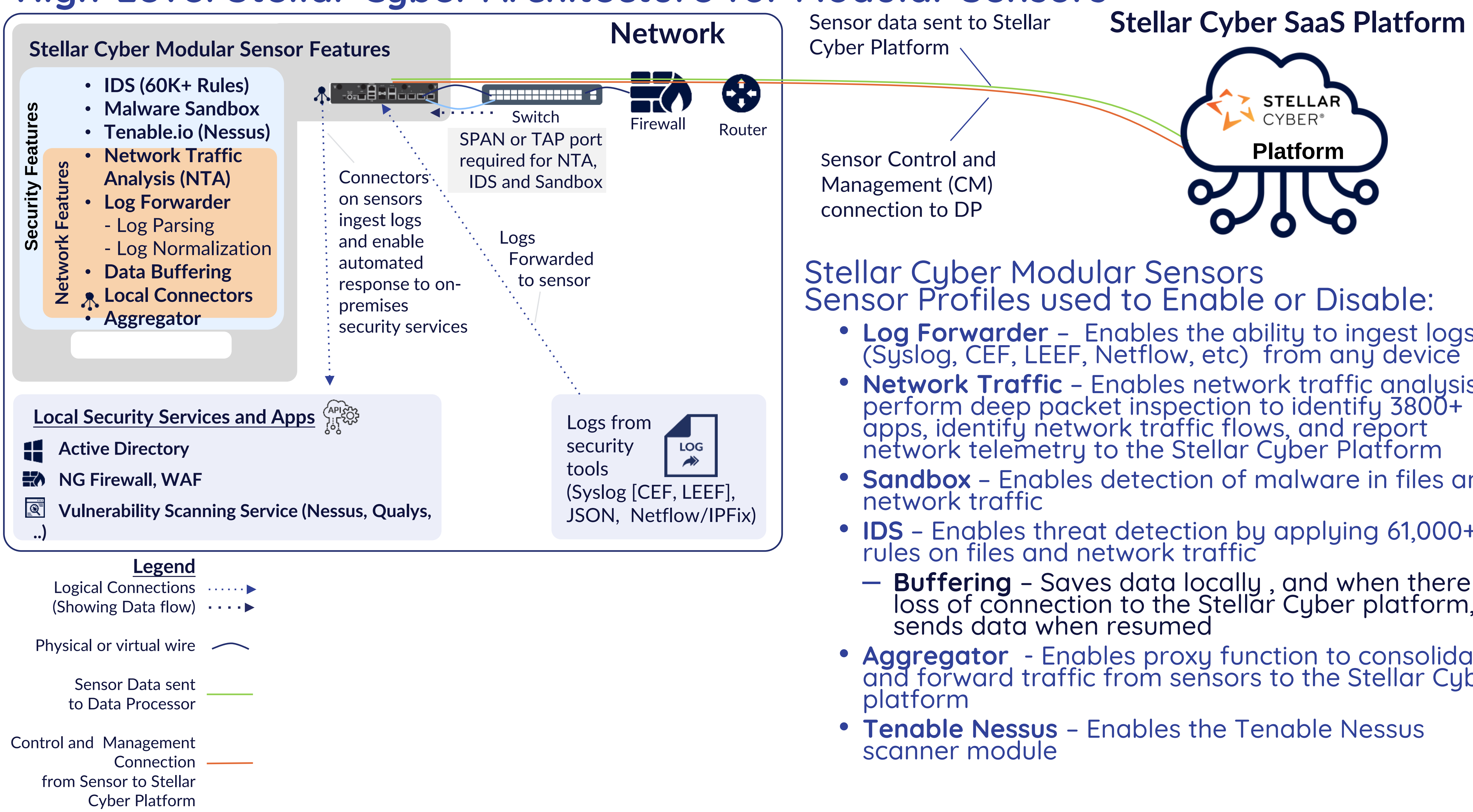
Logical Connections (Showing Data flow)

Physical or virtual wire

Sensor Data sent to Data Processor

Control and Management Connection from Sensor to Stellar Cyber Platform

High-Level Stellar Cyber Architecture for Modular Sensors



Network

Stellar Cyber Modular Sensor Features

Security Features

- IDS (60K+ Rules)
- Malware Sandbox
- Tenable.io (Nessus)

Network Features

- Network Traffic Analysis (NTA)
- Log Forwarder
  - Log Parsing
  - Log Normalization
- Data Buffering
- Local Connectors
- Aggregator

Switch

SPAN or TAP port required for NTA, IDS and Sandbox

Firewall

Router

Connectors on sensors ingest logs and enable automated response to on-premises security services

Logs Forwarded to sensor

Local Security Services and Apps

- Active Directory
- NG Firewall, WAF
- Vulnerability Scanning Service (Nessus, Qualys, ..)

Logs from security tools (Syslog [CEF, LEEF], JSON, Netflow/IPFix)

Sensor data sent to Stellar Cyber Platform

Sensor Control and Management (CM) connection to DP

Stellar Cyber SaaS Platform

STELLAR CYBER® Platform

Legend

Logical Connections (Showing Data flow)

Physical or virtual wire

Sensor Data sent to Data Processor

Control and Management Connection from Sensor to Stellar Cyber Platform

Stellar Cyber Modular Sensors Sensor Profiles used to Enable or Disable:

- **Log Forwarder** – Enables the ability to ingest logs (Syslog, CEF, LEEF, Netflow, etc) from any device
- **Network Traffic** – Enables network traffic analysis, perform deep packet inspection to identify 3800+ apps, identify network traffic flows, and report network telemetry to the Stellar Cyber Platform
- **Sandbox** – Enables detection of malware in files and network traffic
- **IDS** – Enables threat detection by applying 61,000+ rules on files and network traffic
  - **Buffering** – Saves data locally , and when there a loss of connection to the Stellar Cyber platform, sends data when resumed
- **Aggregator** - Enables proxy function to consolidate and forward traffic from sensors to the Stellar Cyber platform
- **Tenable Nessus** – Enables the Tenable Nessus scanner module

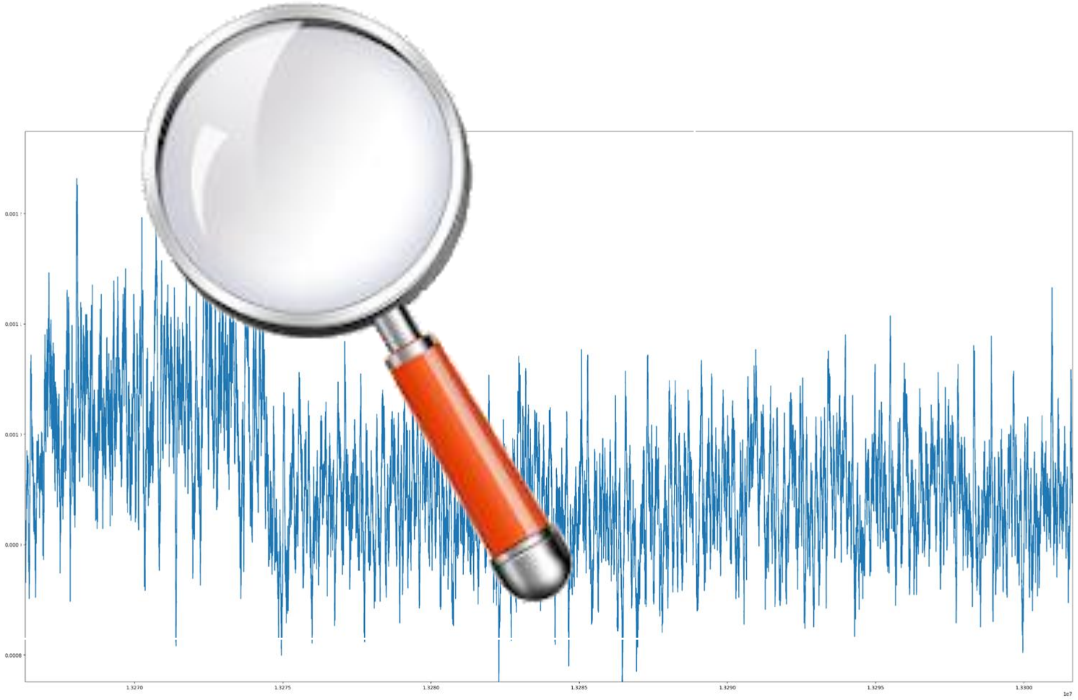
Detect Suspicious Signs of Being Compromised

Stay low and slow, do not trigger strong signals

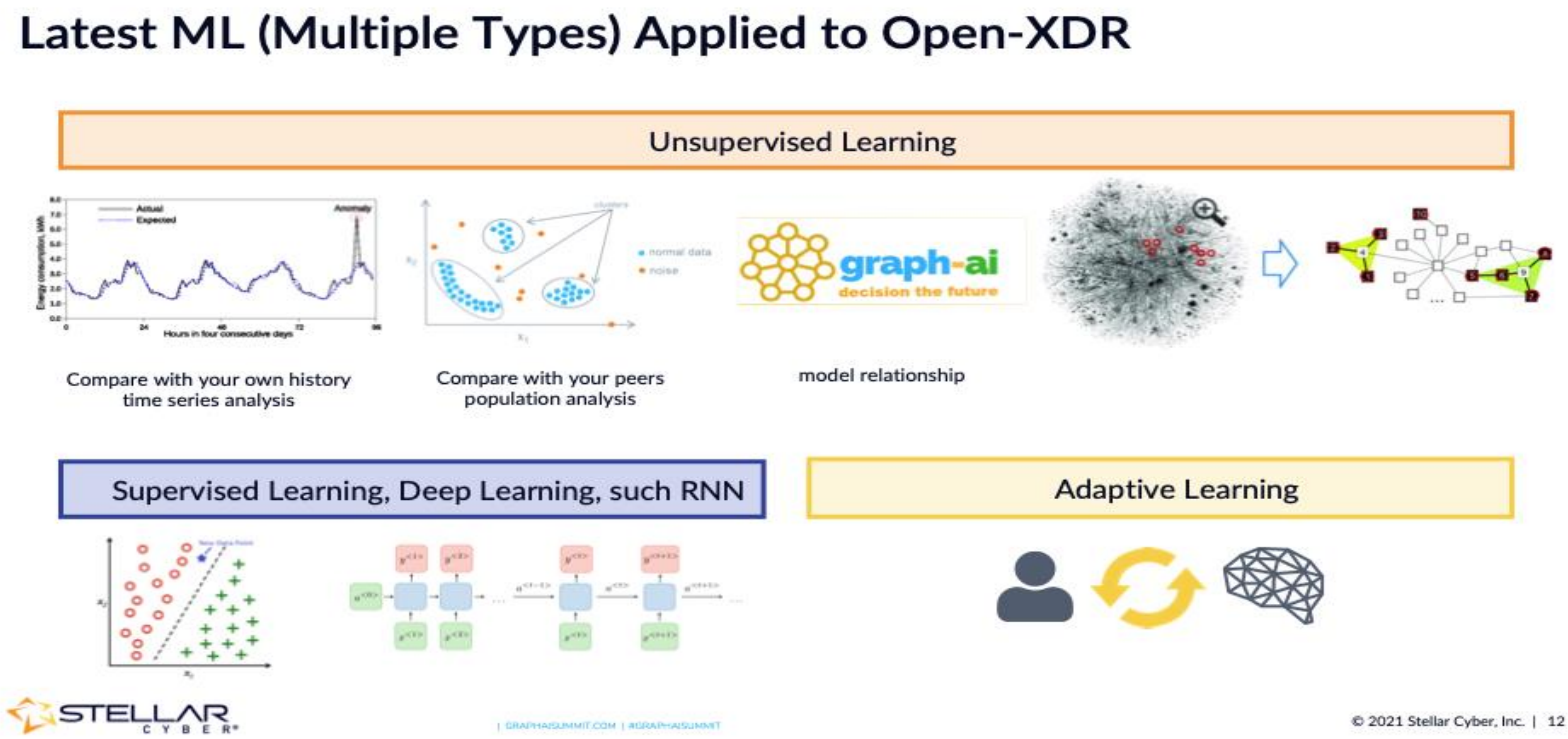
No matter how low it stays, the attack **will leave some traits**, for example, a new communication pattern, activity at different time of the day, access to assets that never happened before

ML/AI to continuously profiling the baseline, and detect deviations from normal behaviors.

Combined with signature/rule-based detections for known bad



Detection ML: Use Multiple Models to Achieve the Best Data-Model Fit for Diverse Attack Types in Open-XDR



Latest ML (Multiple Types) Applied to Open-XDR

Unsupervised Learning

Compare with your own history
time series analysis

Compare with your peers
population analysis

model relationship

Supervised Learning, Deep Learning, such RNN

Adaptive Learning

You Have to Connect Many ‘dots’

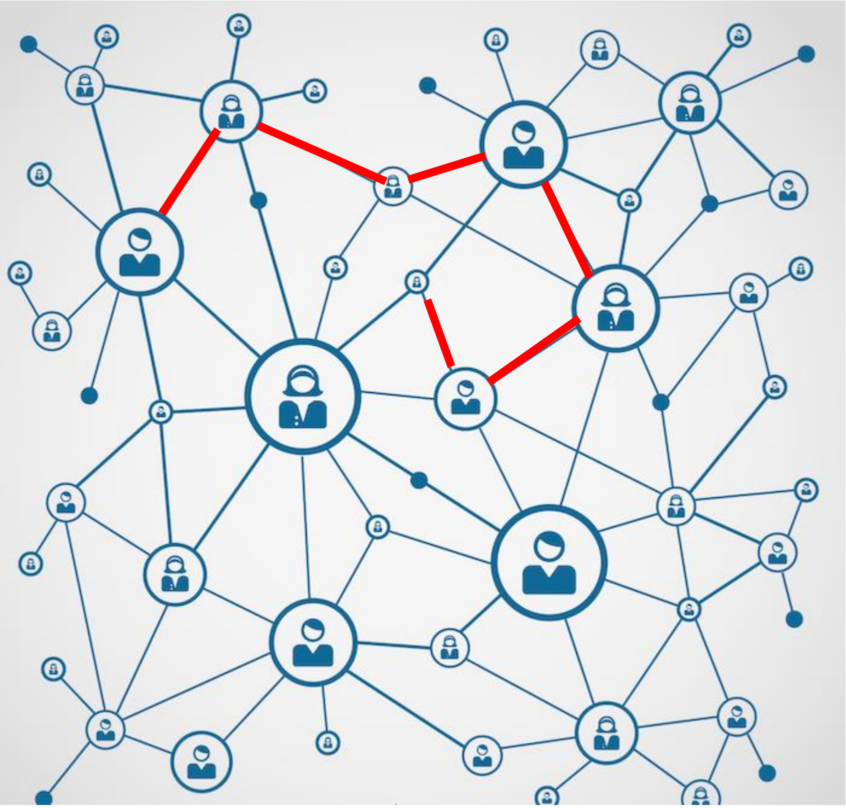
Each event is a ‘dot’

An abnormal ‘dot’ may not be malicious

- Alert fatigue if triage every single suspicious signal
- May miss the one that matters if you don’t

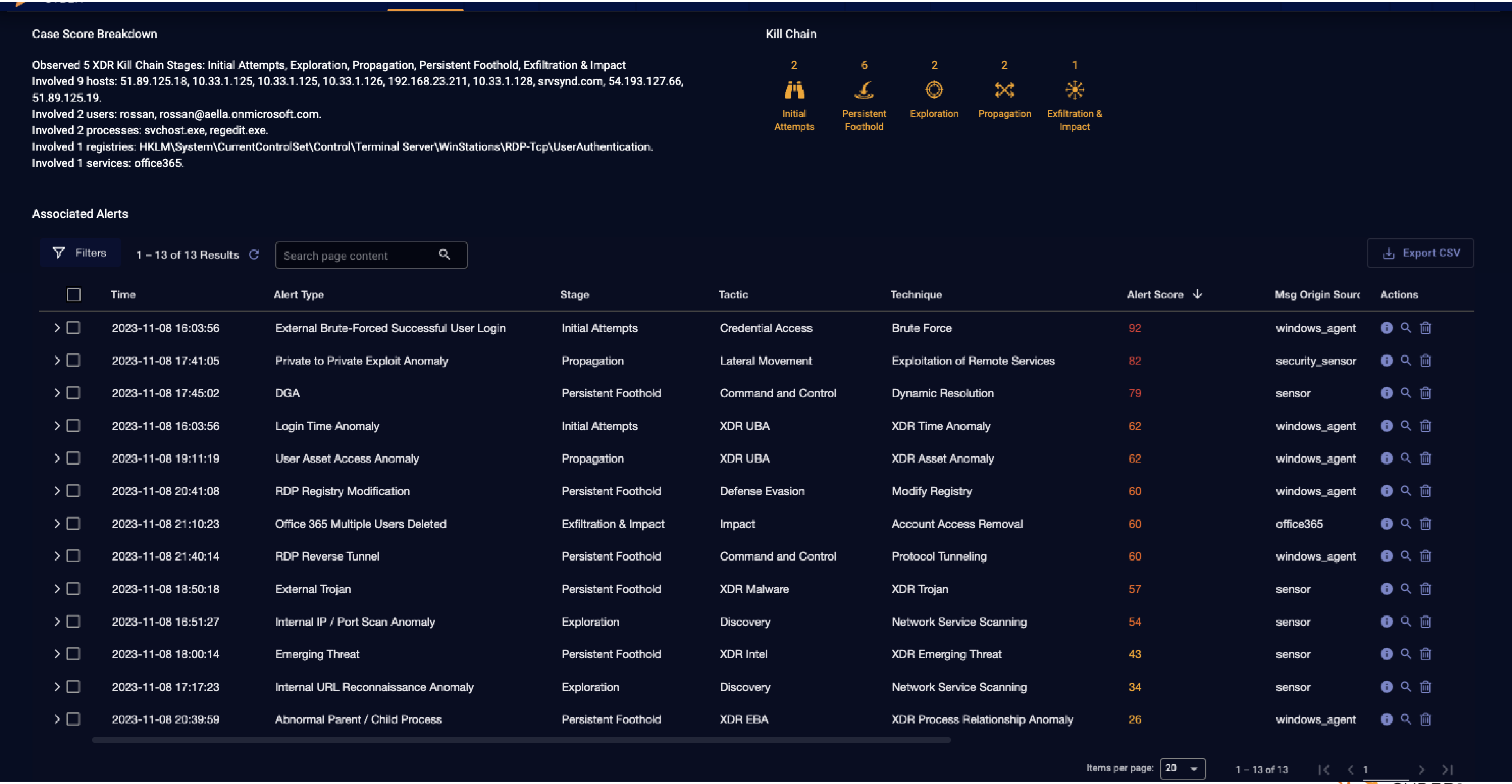
Building context in your data for meaningful correlation is the key

- Creating a storyline for better analysis of related alerts
- Providing visibility for the potential attack path



Response Capability – Stop It Early!

- **Manual** response if I see it
- **Automatic** response to stop it when I am sleeping
- **Block** IP from Firewall, contain a host, disable a user, trigger a slack message or email



Case Score Breakdown

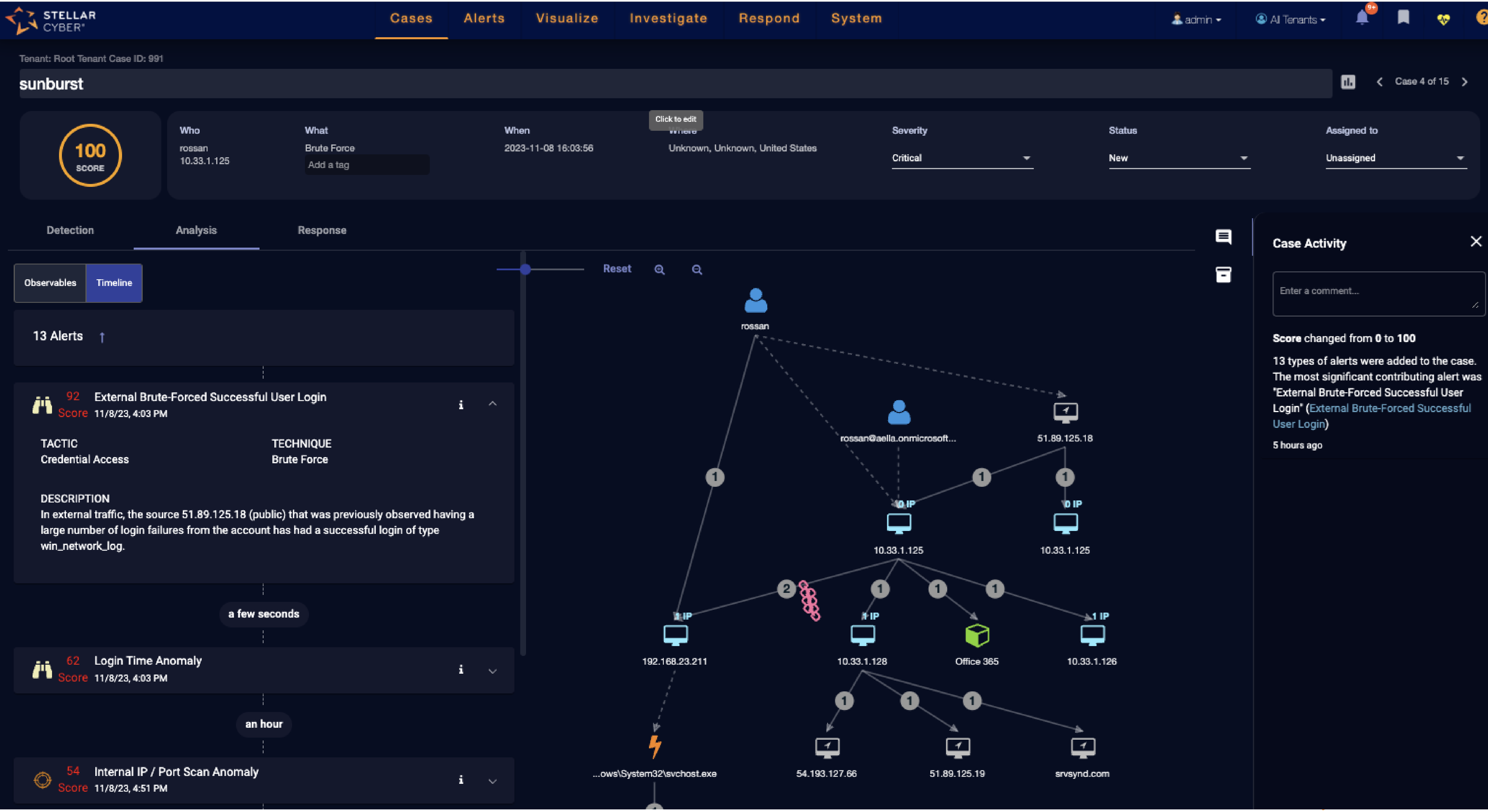
Observed 5 XDR Kill Chain Stages: Initial Attempts, Exploration, Propagation, Persistent Foothold, Exfiltration & Impact
Involved 9 hosts: 51.89.125.18, 10.33.1.125, 10.33.1.125, 10.33.1.126, 192.168.23.211, 10.33.1.128, srvsynd.com, 54.193.127.66, 51.89.125.19.
Involved 2 users: rossan, rossan@aella.onmicrosoft.com.
Involved 2 processes: svchost.exe, regedit.exe.
Involved 1 registries: HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\UserAuthentication.
Involved 1 services: office365.

Kill Chain

2	6	2	2	1
Initial Attempts	Persistent Foothold	Exploration	Propagation	Exfiltration & Impact

Associated Alerts

	Time	Alert Type	Stage	Tactic	Technique	Alert Score ↓	Msg Origin Sourc	Actions
> □	2023-11-08 16:03:56	External Brute-Forced Successful User Login	Initial Attempts	Credential Access	Brute Force	92	windows_agent	ⓘ 🔍 🗑
> □	2023-11-08 17:41:05	Private to Private Exploit Anomaly	Propagation	Lateral Movement	Exploitation of Remote Services	82	security_sensor	ⓘ 🔍 🗑
> □	2023-11-08 17:45:02	DGA	Persistent Foothold	Command and Control	Dynamic Resolution	79	sensor	ⓘ 🔍 🗑
> □	2023-11-08 16:03:56	Login Time Anomaly	Initial Attempts	XDR UBA	XDR Time Anomaly	62	windows_agent	ⓘ 🔍 🗑
> □	2023-11-08 19:11:19	User Asset Access Anomaly	Propagation	XDR UBA	XDR Asset Anomaly	62	windows_agent	ⓘ 🔍 🗑
> □	2023-11-08 20:41:08	RDP Registry Modification	Persistent Foothold	Defense Evasion	Modify Registry	60	windows_agent	ⓘ 🔍 🗑
> □	2023-11-08 21:10:23	Office 365 Multiple Users Deleted	Exfiltration & Impact	Impact	Account Access Removal	60	office365	ⓘ 🔍 🗑
> □	2023-11-08 21:40:14	RDP Reverse Tunnel	Persistent Foothold	Command and Control	Protocol Tunneling	60	windows_agent	ⓘ 🔍 🗑
> □	2023-11-08 18:50:18	External Trojan	Persistent Foothold	XDR Malware	XDR Trojan	57	sensor	ⓘ 🔍 🗑
> □	2023-11-08 16:51:27	Internal IP / Port Scan Anomaly	Exploration	Discovery	Network Service Scanning	54	sensor	ⓘ 🔍 🗑
> □	2023-11-08 18:00:14	Emerging Threat	Persistent Foothold	XDR Intel	XDR Emerging Threat	43	sensor	ⓘ 🔍 🗑
> □	2023-11-08 17:17:23	Internal URL Reconnaissance Anomaly	Exploration	Discovery	Network Service Scanning	34	sensor	ⓘ 🔍 🗑
> □	2023-11-08 20:39:59	Abnormal Parent / Child Process	Persistent Foothold	XDR EBA	XDR Process Relationship Anomaly	26	windows_agent	ⓘ 🔍 🗑



Tenant: Root Tenant Case ID: 991

sunburst

Case 4 of 15

100 SCORE

Who
rossan
10.33.1.125

What
Brute Force
Add a tag

When
2023-11-08 16:03:56

Where
Unknown, Unknown, United States

Severity
Critical

Status
New

Assigned to
Unassigned

13 Alerts

92 Score External Brute-Forced Successful User Login 11/8/23, 4:03 PM

TACTIC
Credential Access

TECHNIQUE
Brute Force

DESCRIPTION
In external traffic, the source 51.89.125.18 (public) that was previously observed having a large number of login failures from the account has had a successful login of type win_network_log.

a few seconds

62 Score Login Time Anomaly 11/8/23, 4:03 PM

an hour

54 Score Internal IP / Port Scan Anomaly 11/8/23, 4:51 PM

Case Activity

Enter a comment...

Score changed from **0** to **100**

13 types of alerts were added to the case. The most significant contributing alert was "External Brute-Forced Successful User Login" (External Brute-Forced Successful User Login)

5 hours ago

Thank You